PAYMENT & FRAUD

May 2013

an internet retailing special report

sponsored by:

Kount®

ogone
An ingenico company

ukash®
use your cash online

Editors' comment

Welcome to the latest in our regular series of *Internet Retailing* supplements. In this edition, we're going back to basics and putting payments and fraud under the microscope. It's a salutary reminder of an area of ecommerce that can easily be overlooked in the rush to focus on weightier issues, such as ecommerce platforms, or on whizz-bang areas such as flash websites and marketing campaigns. But, as we argue throughout this supplement, to do so would be a mistake, for payment and fraud are crucial to the well-functioning online retail business. No transaction can be complete without the ability to pay, and no business is safe without strong yet flexible fraud screening in place.

But although we talk of going back to basics, payments and fraud must today of necessity be viewed in the light of the increased sophistication that's permeating a now mature industry. Since we last looked at this area, the emphasis has shifted. Where previously merchants might have sought to keep fraud rates low, now payment processors are increasingly hearing that clients want something more: to make businesses as profitable as possible. That means increasing the number of 'good' transactions that happen on sites, and curtailing restrictive fraud screening in order not to frighten away potentially profitable customers.

And at a time when retailers are looking both to new sales channels and to new markets to boost the bottom line, payments and fraud concerns now reflect this. A few years ago, the emphasis was on getting payments right. Today it's on getting international payments right – and on rolling out fraud screening to suit an international audience. It's also on navigating these two areas amid the increasing complexity of multiple sales channels. Both for shoppers' convenience and their own protection, retailers are today looking to extend their payment and fraud systems across the store, the call centre, online and mobile commerce. That brings, of necessity, a great deal of added complication to the 'basic' task of enabling payment and managing the checkout.

Over the coming pages, therefore, we look at the key issues that internet traders need to consider when they consider this central part of their online commerce business.

We do that through the prism of our usual features: web interface, merchandising, cross-channel experience, logistics, strategy framework and customer engagement.

In our interface and design feature (page 8), we look anew at the idea of best practice in checkout design. How do the complexities of cross-channel sales and international commerce play in here?

Then our merchandising section (page 12) looks at ways that retailers can best promote their payment options to convince shoppers that the choices on offer are both relevant and attractive to them, while simultaneously reassuring them about the safety of using them. We also consider how that task of merchandising the payment process can translate to other markets, and cross sales channels.

In our cross-channel experience feature (page 16), we're prioritising joined-up thinking, examining the challenges of updating systems that link the store, the call centre and more besides.

Meanwhile, our logistics feature (page 20) considers the practical aspects of achieving balance in fraud screening systems. Much as reducing fraud is laudable aim, how can retailers work towards something different: the balance between tough and flexible screening, which enables merchants to keep taking orders from loyal customers while ensuring they do not become a target for fraudsters.

We focus on strategy framework in our piece on page 25, examining some of the upcoming issues that merchants must consider in order to keep their multichannel business ahead of the curve. "Mobile money," says WeDo Technologies' Ana Cunha, "should be on the radar for all retailers." But in this feature we're also looking at the payment and fraud priorities when considering emerging markets, and consider the gradual rise of the digital wallet – and what it means for retail boards.

Finally, our customer engagement feature (page 28) looks at the need for merchants to inspire trust in existing and potential shoppers. We look at key practical steps they can take in order to achieve that, both on and beyond the website, and in both the UK market and in the crucial international markets beyond our shores. It's a serious issue, as Jean-Marc Noel of Trusted Shops reminds us in the feature when he says: "Without trust there is no trade... and the payment is eventually the result of the trust in the transaction."

Throughout, the What's New boxout tells you how the market has changed since we last covered payment and fraud, in May 2012.

We hope you find this supplement useful. If you have comments, questions or suggestions for future supplements, do contact us. We can be reached at chloe@internetretailing.net or jonathan@internetretailing.net.

INTRODUCING OUR EDITORS
Chloe Rigby has been writing about business issues for more than a decade. A former business editor of the *Bristol Evening Post,* she has written for a wide variety of online and offline publications. chloe@internetretailing.net

Jonathan Wright earned his e-stripes on the UK launch of *Business 2.0,* which rode the crest of the dot.com wave back at the turn of the millennium. Since then he's been writing about subjects from entertainment to alternative investment for a variety of print and online audiences. jonathan@internetretailing.net

CONTENTS

THE ADVENT OF TRUE CROSS-CHANNEL AND THE GROWTH IN INTERNATIONAL SALES ARE POWERFUL DRIVERS IN RETAIL. WHAT NEW DEMANDS DOES THIS PUT UPON RETAILERS IN THE ARENAS OF PAYMENTS AND FRAUD?

With ecommerce and m-commerce (mobile commerce) growing at astronomical rates worldwide, retailers are faced with new problems from increased fraud risk to payment security. As these elements of the online retail ecosystem rapidly expand and change, there are a few things every retailer needs to plan for and consider.

First, many tools and systems currently used by retailers are likely not enough to fully protect them or their customers, much less meet the shopping experience expectations of today's online consumer. Cross-channel retailers have a different level of complexity to navigate to ensure their environment is equally secure for customers who buy online and ship to a location as those who make online purchases and pick items up at their local branch.

Store operations and logistical systems need to work together seamlessly to provide a singular experience for the customer. Many retailers we've spoken with claim that their online and in-store systems are too different to work well together. Inventory management, payment acceptance, return policies and determining who gets credit for the sale – store or website – are just some of the challenges that undermine the level of integration necessary for success.

However they engage with the retailer, the customer only wants a simple shopping experience. They don't care what backend systems are used or their limitations until their expectations aren't met. That's when they look for a new place to shop.

Second, in terms of fraud and risk exposure, international sales are much more complicated for retailers currently selling just in one country. Recent studies indicate that international transactions are three to four times more likely to be fraudulent than in-country purchases. That's quite a leap in a retailer's risk profile if they aren't protected. Before expanding internationally, there are a number of elements retailers need to review and consider.

As a first step, retailers should contact their payment service provider (PSP) to review what fraud detection and mitigation features they offer. In my experience, most PSPs do not have sufficient fraud detection options that keep up with evolving threats. Often they will provide a few basic tools that can help identify fraud or suspicious activities, but these tools use techniques that fraudsters have already bypassed or beaten outright.

Today, tools for detecting fraud must use dynamic, real-time data to detect fraudulent transactions. Using dated lists, simple address verification or credit card approvals are not enough to keep fraudsters from getting into and thwarting the payment system.

Fraudsters today are very sophisticated in technique and technology. They work fast and can coordinate with like-minded individuals worldwide to become very large and powerful networks. Retailers should regularly review their own fraud management policies, systems and tools to keep current on the latest methods to reduce fraud exposure without impacting online sales. Many retailers lower fraud attempts by implementing very broad rules that may reduce some fraud but also have a dramatically negative effect on revenue and sales opportunities. There is definitely a balance needed.

A complete fraud strategy should take into consideration three main areas of focus. Fraud detection and prevention, business rules for managing fraudulent attempts in real-time and complete integration with with operational and logistical systems such as accounting and shipping systems are all critical. These components are the only way to enable a comprehensive, closed loop system that detects and manages fraud across the entire organisation. Fraudsters are getting smarter and more numerous while growing at a rate faster than ecommerce. Only a solution integrated across the retailers organisation will be sufficient to detect and alleviate fraud in both the short and long term.

Another area often lacking in fraud solutions is reporting how effective these systems are. As a management tool, good reports or on-screen dashboards can provide vital information about the effectiveness and efficiency of the payments and fraud rules. A good reporting tool should provide a real-time view of operations, with trends and analysis to inform ongoing system updates and maintenance.

It's a daunting task when expanding cross-channel or cross-border. Retailers can alleviate these challenges by establishing a fraud solution that aligns with company strategies and integrates with existing systems. This critical step can mean the difference between growing customers and revenue or giving the fraudster an opportunity neither of you will forget.

www.kount.com

The growth of online shopping opens innumerable opportunities for traditional, online and cross-channel retailers. Online retail showed an annual increase of almost 13 per cent in 2012, and that figure is likely to rise again by the end of 2013 with increasing retail opportunities.

However, there are new challenges and cultural considerations when selling internationally. For example, when trading in countries less reliant than the UK on credit and debits cards, are consumers who prefer to pay in cash simply unattainable?

Consumers who prefer to pay in cash represent a huge number of potential customers, and therefore revenue, which retailers are missing out on. But cash payment schemes like Ukash can help convert these valuable customers. Ukash codes can be purchased using cash in retail outlets such as local convenience stores, petrol stations and kiosks in more than 50 countries around the world, on six continents. Customers then spend the voucher online, meaning they are able to continue using cash as their preferred payment method both online and offline.

Not only does this provide convenience for the customer by allowing them to use their preferred payment method, but it also protects against the risk of fraud as no card details are provided.

Tight payment security is vital to fight against increasing levels of fraud, which could affect retailers' profits, reputation and customer relationships. So the challenge is to create a safe and secure online purchasing process that doesn't risk asking consumers so many questions that they feel interrogated or lose patience and drop out of the payment process.

Our research has revealed that nearly half (46 per cent) of online shoppers are frustrated by security questions when making purchases online, and over a third (39 per cent) have actually abandoned an online transaction because they were being asked for too much information. E-money enables cash consumers to shop online and protect their personal identity and financial information when making online transactions – thereby reducing the threat of credit and debit card fraud for consumers.

As online retail continues to increase in popularity, consumers should be given as many payment options as possible to allow them to shop in the way they feel most protected and comfortable. This, in turn, encourages return custom and brand loyalty, thus increasing sales and profits.

Miranda McLean, marketing director
www.ukash.com

The payments sector is rapidly evolving. Consumers want to pay where and when they wish, and new technologies are enabling them to do so. However, as well as providing the opportunity for merchants to generate new revenues from new channels, there are challenges that need to be considered. For any payment mechanism, it is essential to ensure security without compromising the customer relationship, as this can result in preventing repeat business.

The increasing variety of sales channels is improving service levels and the way we pay is changing, whether it is at a retail outlet using self-service, an internet purchase or a mobile payment made on the go. There are card-swipe payments, payments secured by chip and PIN, closed-loop payments, payments made using an e-wallet, contactless and NFC payments. Retailers need consumer and merchant-friendly terminals that are optimised to present the relevant information in the most efficient way in order to accept as many payments as possible.

It is no secret that a growing number of payments take place online and in 2012 the UK saw an increase of 18 per cent in spending (reaching £63 billion) by UK cardholders. This presents a number of challenges. Consumers must believe the payment mechanism is secure and reliable and be confident to make payments in this way. For merchants selling in foreign markets, there is a need to be flexible. In some instances consumers may prefer to use their traditional local payment solution and merchants wishing to sell effectively in these countries must be in a position to offer this option.

Transactions where the card is not present (telephone, internet and mail order) present particular challenges and indeed accounted for more than 62 per cent of UK card fraud in 2012. In addition to CVS and AVS checks, and the use of 3DS security that enables a liability shift, retailers can work with their acquirer and card service provider to introduce device fingerprint technology and business rules that will identify fraudulent transactions while allowing any genuine transactions to be processed without delay.

Merchants trading in an international environment need solutions that are quick, reliable and have security measures that counter the threat of fraud. They must also anticipate changes in the way people wish to pay in an increasingly mobile environment. Whether it is in-store, online or via a mobile or tablet, there is now a one-stop shop for multichannel payments. In an environment where consumers are confident in using different payment mechanisms for different transaction types this enables easy secure payments and analysis via common fraud prevention tools and associated profiling. For consumers the result is greater choice and convenience, and for the retailer more control and increased sales opportunities.

www.ogone.co.uk

BEATING FRAUD WHILE BOOSTING SALES IS NO GAME

THE SITUATION

For more than a decade, Jagex has been a leading online game developer with a global reputation for creating hugely popular, free-to-play games. The company has developed and self-published online titles, including *RuneScape*, the Guinness World Record-holding "Most Popular Free Multiplayer Online Game". With more than 480 staff, Jagex currently stands as the largest independent games developer and publisher in the UK.

In 2009, the company started using an internally developed fraud prevention solution. But fast-changing fraud tactics, high rejection rates and increasing competition for in-house development resources caused Dave Parrott, fraud manager at Jagex, to seek a solution that would allow him to rapidly respond to fraud, while reducing decline rates.

"In 2009, we were hit with a round of fraud attacks," says Dave. "Fraudsters would use stolen credit cards to buy paid memberships – which let them earn virtual currency at a much faster rate – so they could then sell this virtual currency for real money. It's called Gold Farming. We implemented new rules to stop the fraud, but it left us with a high rejection rate. Then in 2011, the Gold Farmers attacked us with everything they had.

" Kount offered us something other companies couldn't: the ability to write our own custom rules that apply to our unique situation. I didn't have to buy someone else's pre-packaged sets. Further, the Kount system is easy to integrate and set up, so I could use what I already had in place... quickly and intelligently. "

Dave Parrott,
fraud manager, Jagex

This took a lot of effort to combat, diverting time and programming resources that we wanted to devote to our games." Dave became convinced the company needed help from outside fraud prevention experts. "We realised our internal system was not the long-term solution. Our rejection rate was too high and implementing changes to respond to new attacks was too awkward."

THE SOLUTION

Dave began with a Google search, and came up with a substantial list of candidates. After interviewing multiple local companies and viewing demos from five finalists, Jagex chose Kount. "One of the deciding factors was how easy Kount makes it to rapidly write and implement custom rules to defeat new fraud tactics."

"Integration took about two weeks," recalls Dave. "It was quite simple, really. At first, we had the Kount system merely replicating the old system. But then we started using Kount's easy rule writing to make fine-grained modifications to quickly stop new fraud attacks. Next, we put Kount to work reducing our rejection rate. All the data I was seeing suggested we were missing out on sales... that our rejection rate was too high."

Leveraging the Kount Score functionality, Dave was able quickly and easily to write additional rules that cut their rejection rate by 50 per cent with no increase in fraudulent charges. In fact, even with the lower rejection rate, Jagex was still able to hold its chargeback rate at around 0.2 per cent. "Altogether, that's equals almost one per cent more net credit card revenue each year," notes Dave.

Kount also helped Jagex improve revenues in other areas. "After we implemented Kount, our conversion rate on longer-term membership subscriptions increased three per cent to four per cent," notes Dave. What's more, with Kount protecting the company's back end, Jagex was able to discontinue front-end screening measures that were previously necessary. "We turned off 3D Secure and we saw no increase in fraud," says Dave. "That will save us hundreds of thousands of pounds in expense each year."

In the coming months, Jagex plans on rewriting many of the rules in the Kount system to take full advantage of all of Kount's capabilities (instead of just having it mimic the old system). "I expect that update will cut the rejection rate in half again," says Dave.

ABOUT KOUNT

Kount helps businesses boost sales by reducing fraud. Our all-in-one, SaaS platform is designed for merchants operating in customer-not-present environments looking to simplify fraud detection and dramatically improve bottom line profitability. For each transaction, Kount's "decisioning" engine analyses hundreds of relevant variables and activity across the globe in real-time. Kount applies a multitude of proven and proprietary technologies based on the specific needs of each customer, including Multi-layered Device Fingerprinting®, Proxy Piercer® geolocation tools, statistical scoring, rules-based fraud detection, cross-merchant linking, and Persona™ behavioral modeling. The result is a highly predictive fraud assessment delivered in an average of just 350 milliseconds. Kount provides a single, turnkey fraud solution that is easy to implement and easy to use. Kount's proprietary technology has reviewed hundreds of millions of transactions and provides maximum protection for some of the world's best-known brands. For more information about Kount, please visit www.kount.com

THE OUTCOME

• Approximately four per cent increase in net credit card income annually.
• Rejection rate reduced 50 per cent, with another 50 per cent reduction projected.
• Conversion rate increased three per cent to four per cent on membership subscriptions.

Dave sums up: "With Kount, we didn't have to buy someone else's pre-packaged rules and then try to make them work for our situation. Kount lets me quickly and easily implement custom rules specific to our transactions. For example, if I detect a new kind of fraud attack, I can respond with new rules within minutes. Part of the reason for that is Kount's support team. They have been brilliant. I feel like they're listening to me as a merchant, that they want to solve my problems, not just sell me a product." ■

NEW WAYS TO GET
BACK TO BASICS

THE CHECKOUT PROCESS NEEDS TO BE AS SIMPLE AS POSSIBLE FOR CUSTOMERS TO USE. HOWEVER, THAT SHOULDN'T BE AN EXCUSE FOR RETAILERS TO BE COMPLACENT AND NOT TO TRY NEW DESIGN APPROACHES, ADVISES **JONATHAN WRIGHT**

If there's just one subject that just about everyone involved ecommerce can agree upon, it's that the checkout process needs to be as smooth and easy for consumers as possible. Once a customer has decided to buy an item and he or she is headed for the digital till, trying to prolong the conversation may only result in the customer abandoning a shopping cart in frustration. Keep it simple (stupid) and sales will surely follow.

"Every single one of your customers has to complete the checkout to pay," points out Mo Syed, head of user experience at ecommerce technology company Amplience. "That's not true for every part of your site, for your home page or certain [product] categories, but it is true absolutely for every single part of your logged-in or guest checkout."

Despite this, it's surprising how many retailers appear to think little about the design of the checkout process. In the worst cases, even as the rest of the website is revamped, going to pay can be like suddenly visiting an earlier iteration of a site.

"It's often hard for designers to snap themselves out of just sleepwalking through a design because there's such an accepted format for the checkout," continues Mo Syed. "They're so similar that you rarely see an unusually different checkout. And that's a really big missed opportunity because it is one of the areas where innovating or rethinking or experimenting through A/B testing or otherwise could potentially yield you massive returns."

So how should retailers go about getting these returns? It's a more difficult question than it might first appear. On the one hand, the elegantly

> **"The elegantly straightforward Amazon sales funnel has been widely copied for a good reason, it works"**

straightforward Amazon sales funnel has been widely copied for a good reason, it works. Moreover, customers have become familiar with this way of doing

SPEAKING
FROM
EXPERIENCE

COMMUNICATING SECURITY

"I would be very transparent about what [a site's] security requirements are. A lot of legitimate customers will try and deliver to a work address, or try and deliver to a relative's address. They might expect to be able to do that because a form doesn't implicitly say something otherwise. And they'll trip a fraud constraint, and the transaction will either get stuck in limbo, where it'll need to be manually authorised, which is a really bad experience, or it'll just be marked off as fraud.
Mo Syed, head of usability, Amplience

LONG-TERM PROJECT

"We have a checkout model which we've spent years and years developing now. It's not something you can do on a project, you have to spend quite a lot of time doing it, and you end up far more with a standardised model where you can swap different payment methods, payment devices, or delivery methods and delivery devices, subject to what the geography is you're trying to target."
Leigh Whitney, managing director, Design UK

JUST OVER THE HORIZON

"I think the most exciting methods of payment for cross-channel are still out there a ways. When we start talking about near-field communication and payment by phone, and things of that nature, things really become dynamic. We haven't quite got there yet."
Jamus Driscoll, senior VP of marketing, Demandware

things. Against this, there may be gains to be made from being innovative, but how do you guard against getting ahead of what consumers expect of the checkout process?

If that weren't tricky enough in itself, retailers need to consider other developments too. Will the rise of cross-channel retail lead to changes in the way checkouts look and work? How will the adoption of new kinds of devices, from smartphones to smart TVs, affect things? What about the myriad delivery options that many retailers now offer – and indeed have to offer? How should retailers tackle new markets where, for example, consumers expect to see different payment options?

These aren't abstract questions for designers, they're live issues. As Jamus Driscoll, senior VP of marketing with ecommerce technology company Demandware notes as he explains why "responsiveness and adaptability" are key attributes for successful cross-channel retailers: "Opportunity is everywhere. Whether a retailer can take advantage is directly correlated to how fast they can move."

FORWARD MOMENTUM

Before moving on to look at the questions posed above in more detail, it's worth pausing to emphasise that the basics really do matter here. "The simpler and easier the checkout process is for consumers, whatever the format of that checkout, the greater probability and propensity that they're going to complete that checkout, and therefore that the purchase or sale is made," advises Leigh Whitney, managing director of digital agency Design UK. "Any obstacles along that journey, or anything that distracts them or takes them away from that forward momentum in the checkout can lead to an exit and therefore a lost sale. A large part of getting checkouts right is about building and maintaining that forward momentum."

Of course, this was far simpler in an age when those shopping online could be relied upon to be using a PC. These days, customers jump between devices, doing research on a smartphone, for example, before buying via a PC and arranging to pick up goods from the store – and that's a simple example of a cross-channel journey. Once you start to

ogone
An *ingenico* company
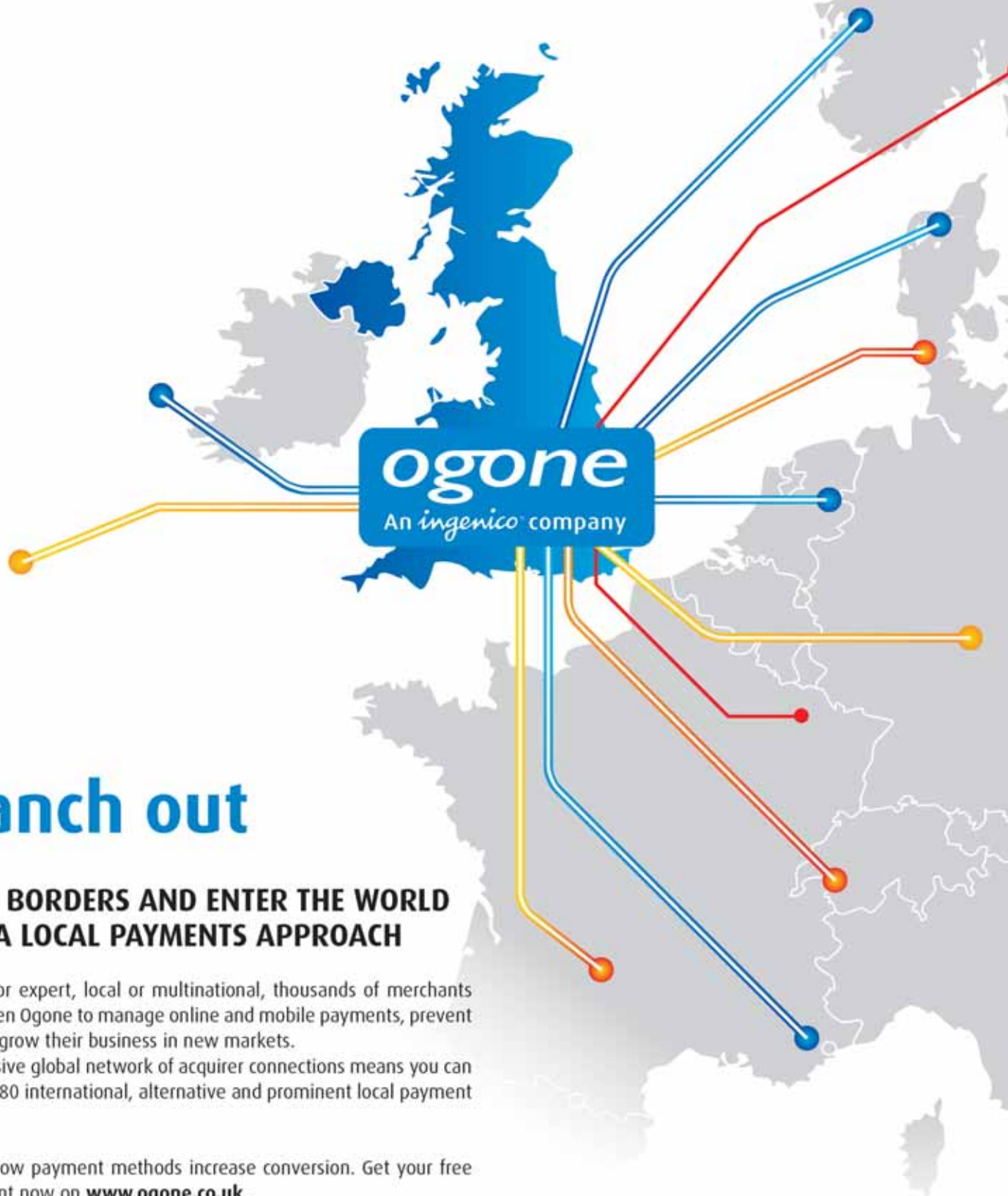
Branch out

CROSS BORDERS AND ENTER THE WORLD WITH A LOCAL PAYMENTS APPROACH

Beginner or expert, local or multinational, thousands of merchants have chosen Ogone to manage online and mobile payments, prevent fraud and grow their business in new markets.

Our extensive global network of acquirer connections means you can offer over 80 international, alternative and prominent local payment methods.

Discover how payment methods increase conversion. Get your free trial account now on **www.ogone.co.uk**.

Did you know you can already group most local payment methods in one single contract?

A W O R L D O F L O C A L P A Y M E N T S — J U S T O N E C L I C K A W A Y

introduce these kinds of steps, it's all too easy to loose that crucial momentum.

One way to tackle this problem is to think of the shopping basket as a kind of intermediate stage between browsing and committing to buying. At least where it's possible to identify customers, retailers need to make it as easy as possible for customers to access items saved for later, something Amazon do well.

"It's the kind of temporary holding place that would work well across channels, so if I go in and I speak to someone and my identity with that retailer is visible within an in-store kiosk, I can add it to my basket, save [an item] for later, and then come back and buy it a month later from my desktop PC," says Mo Syed.

This also helps to get around the problem of customers using devices where it's fiddly to key in details, something that's only going to become more of an issue as smartphones and tablets increasingly supersede the PC as the devices of choice for ecommerce. "Because of mobile and tablet people are much more acutely aware of how painful it is to input stuff," says Mo Syed. "Of course, it was *always* painful to input stuff…"

In great part because of this, designers at the very least need to be aware of the way payment technology is developing, to be keeping up with the plethora of e-wallets and new ideas that get around the keyboard problem – while at the same time recognising that not all of these will succeed.

"We don't know yet how the new payment types are going to be working," says Jamus Driscoll. "PayPal, certainly, is making a great push on stores: but how well will that be absorbed? We don't know yet, but we know that it's not unlikely change is going to happen very, very quickly. We think everyone needs to be thinking with highly responsive architectures in mind."

PRESENTING DELIVERY OPTIONS
Driscoll's emphasis on reacting quickly to change is pertinent here because it captures the tension between a design imperative towards simplicity and the complexities introduced by new kinds of customer behaviour. This isn't just down to the burgeoning cross-channel world. Even the question of how to present delivery options can trip up unwary retailers. "You can have store delivery, you can have [goods] delivered

to the post office, you can have delivered to the local newsagent in the form of a Collect+ delivery," points out Leigh Whitney. "You've got am, pm, same day, avoid school run, next-day delivery, three-days delivery, Saturday delivery, man-on-a-running-bike delivery, same-day-within-the-M25 delivery. All those delivery options and electronic delivery as well, and all of those delivery options require different information or certain sets of information to be provided in order to deliver that fulfilment."

None of this exactly encourages simplicity within the checkout process. "As soon as you want to offer this breadth of delivery options to the consumer, you need space within the design to do it," adds Whitney.

> 66 **Designing checkouts and payment routes that are specific to different territories can be an expensive business** 99

LOOKING OVERSEAS
These kinds of design problems only multiply when companies look overseas. While the UK and US checkout model is even now based primarily around credit and debit cards, that's not necessarily the case even elsewhere within the developed world. In Germany, for example, many customers prefer to pay by cheque or bank transfer.

Designing checkouts and payment routes that are specific to different territories can be an expensive business. However, cost considerations need to be balanced against the fact that customers presented with unfamiliar payment options will often become suspicious, a sure route to shopping cart abandonment.

"What we see in the minds of retailers who are looking at running in lots of different countries is how do they manage the complexity of having lots of different payment options and having countries, and having country-specific and/or cultural-specific payments without really inflating the cost of operating and running the business?"

WHAT'S CHANGED

Not enough. Even as ecommerce and old-fashioned shopping evolve into cross-channel retail, and we enter a world where all kinds of different devices will be connected to the internet, too many designers still don't take the checkout process seriously enough. A key message from the usability experts we interviewed for this feature is clear: innovate and test, and then innovate and test again.

says Jamus Driscoll. "Historically, payments have been a very big challenge and create a lot of complexity when you're trying to go into five, 10, 15 different markets.

"We're seeing a lot of emphasis from our retailers on how do they adopt 'right' in-market payments in a way that is a lot more flexible, a lot more agile than historically has been the norm."

Again, it's a remark that might be applied more generally to the design of digital checkouts because, while the idea of the slick, easy-to-use sales funnel hasn't gone away, it's increasingly clear that it's not enough in itself simply to rely on received wisdom around best practice here.

If that sounds an obvious point to make – it's hardly rocket science to suggest that companies need to monitor business practices as a guard against complacency – it's worth returning to the first point we made here, that too often retailers don't focus enough on the checkout process. One of the reasons this feature doesn't focus more on the brave new world of service design, e-wallets, smartphones and how to present alternative payment options is because of this.

"The checkout is not about communicating the quality of your products, the checkout is about one thing and one thing alone, and that's reducing the interaction costs of completing the payment, completing the transaction process," says Mo Syed. "That's what the checkout is for, and that type of deign, where you're just ruthlessly squeezing, and refining and refining and refining, and removing interaction costs and friction in that process, that's something that people in ecommerce don't really do that much." ■

CLEAR AND
PRESENT PAYMENT

HOW PAYMENT OPTIONS ARE PRESENTED CAN HAVE A DIRECT EFFECT ON CONVERSION RATES, WRITES CHLOE RIGBY

R etailers sell products online most effectively when they present their wares clearly and to the most relevant website visitors. By using strong imagery and by offering thorough information, they give customers the detail they need and the confidence to buy. But merchants who apply such merchandising techniques only to their products are missing a trick, for that same attention to detail is just as relevant on the payments page.

For far from being the afterthought of the site, savvy retailers regard the checkout as one of the most important single areas of a website. It's where shoppers make the final decision not only on the products they have chosen, but also on the payment methods available. Missing out one that matters could have a real effect on conversions and ultimately on the bottom line. It's worth taking time to consider in detail, for as Tom Waterfall of Webtrends says, the payment page is the "really critical" one when it comes to generating a return on investment into internet retailing and cross-channel commerce.

> **Savvy retailers regard the checkout as one of the most important single areas of a website**

MAKE IT CLEAR
If effective presentation of payment is about making it easier for customers to buy, that starts when retailers show clearly what type of payment options they accept. Clear and well-placed logos occupy little space but reassure customers that as and when they get to the shopping cart, they will be able to pay using the type of payment option that they want to use.

Don Bush, VP, marketing, at payment processing and fraud screening specialist Kount, says it's important to show the choice on offer as early as possible in the shopping process. After all, he says, no shopper wants to get to the point of payment only to find that their chosen method isn't accepted. "Where I've seen it merchandised well," says Bush, "is when it's even on the home page. Payment types may not be a sexy part of

BEST PRACTICE?
"It's really hard to say there's best practice in today's day and age. That's where A/B testing and multivariate testing come into play."
Tom Waterfall, optimisation solutions manager, EMEA, Webtrends

TIMESAVERS
"For me, if I see that at the home page, down at the bottom – here are the payment types we accept and these are the certifications that we have, I appreciate because then I haven't spent a bunch of time shopping, I haven't started the process. Some retailers might argue with that and say we want to get them all the way through the shopping cart – I think that's somewhat frustrating."
Don Bush, VP, marketing, Kount

WHAT WORKS
"Whatever is best practice doesn't always work for our retailers so we always test it. I think that's particularly applicable when you look across different regions. What happens in the UK may not happen in Germany or France or other regions where there are very different cultures. You'll find that when you test across different regions you get different results for exactly the same test."
Daniel Martin, managing consultant, Maxymiser

the web page, but down at the bottom [of the page] retailers can list the ones they accept." That effectively communicates a vital piece of information that can reduce wasted time on a site, something, argues Bush, that is better than frustrating the customer once they've arrived at the virtual till.

Taking a clear approach to presenting information goes beyond payment options. It's also important to show customers that the retailer will look after their financial information carefully. That's a message that can be given through the use of trustmarks or by judicious use of the padlock symbol. It's important to make sure that the symbol used is one that is recognised – and that may vary from market to market. We've more on trustmarks in our customer engagement feature (page 28).

WHAT'S NEW

With retailers increasingly realising the value of testing, the take up of related approaches to 'merchandising' key website areas, including the payments page is now taking off rapidly. Expect this to become the norm as online retail becomes ever more competitive and merchants seek to be sure that their sites are as efficient and effective as possible.

MAKE IT RELEVANT
Key to selling different markets is the understanding that shoppers in other parts of Europe and the world don't have the same expectations of payment as in the UK. Shoppers in the Netherlands, for example, expect to be able to pay using the Ideal bank transfer system – one that would be entirely foreign to customers paying in the UK. It's important, then to keep payment pages relevant to their visitors. Through website optimisation and personalisaton, retailers can ensure that the payment page each visitor sees is relevant to them, containing only the payment types that are available to them in the country from which they are shopping.

That idea of relevancy also extends to showing visitors different information about payment based on whether they are first-time visitors or if they have previously bought from the site." I think you do need to consider small differences that can make a bit of an impact on sales," says Tom Waterfall, optimisation solutions manager at Webtrends. "Some things work for some cultures and languages and some don't. Overall, the company needs to be consistent in terms of its brand, but small tweaks can make quite a difference. The journey is also quite

ukash®

use your cash online

Increase your conversion rates by 22% - accept cash on your website

Consumers want choice when spending online, research shows that every new payment added increases conversion rates.
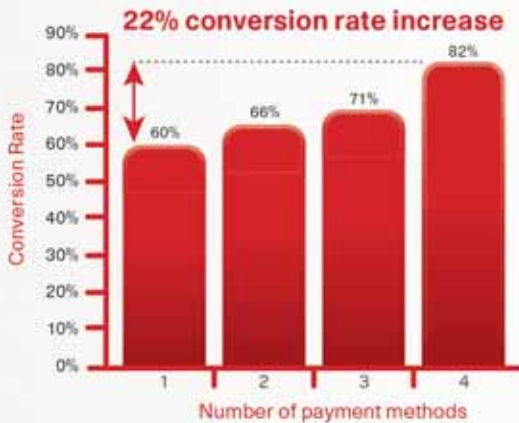
Source: Global Collect, merchant survey

I am new to online shopping and Ukash makes it simple

u 3 MONTHS COMMISSION FREE

Get 3 months commission free

We are offering all Internet Retailing subscribers a 3 month free trial, with no set up fee. Ukash is the ideal addition to your existing payments options.

Email us at retail@ukash.com and get started today.

What is Ukash?

Ukash enables consumers to use cash to pay online by exchanging notes and coins for a voucher. This caters for the growing number of consumers who want to purchase quickly without the hassle of security questions, those that are worried about having their card details stolen or don't have a card to pay for goods online.

What are the benefits?

✔ Attract new customers and generate new business

✔ Beat your competition by driving online sales growth and expanding into new countries

✔ No monthly/annual fees or chargebacks

✔ Save time with hassle free integration

Find out how Ukash can benefit your business
visit www.ukashbusiness.com | **email** retail@ukash.com | **call** +44 (0) 20 7939 0377

different if you're a new visitor checking out or the first time, or someone who is logged in. You have an opportunity to make that final critical page in the journey different – and that can make a big difference to sales."

Another driver of this kind of relevant optimisation is the device that a shopper visits from. As more people buy from mobile phones or tablets, it's important to make sure that the most relevant method of payment is available to those buying from different devices. "More and more visitors are buying on their mobiles, on tablets," says Waterfall, "but it's not always that easy to fill out a form on a touchscreen entering all those little digits on your credit card number. Facilitating the process for those other devices therefore becomes really important." This idea is explored further in the cross-channel feature (page 16).

Meanwhile, continuing to promote messages about the retailer's unique selling point – or why the retailer is relevant to the customer – up to and throughout the payment process can also have a marked effect. Waterfall suggests that messages such as 'you're qualifying for free delivery', or 'free returns' can help to 'seal the deal'.

But it can be hard to know for certain what works or doesn't work on any given site unless a retailer is measuring through testing.

CHECK WHAT WORKS
Best-practice advice may offer big-picture guidelines to tactics that work online. But individual retailers who want to be sure that they are backing the right approach can find out how it works on their unique site, with their unique set of customers, through A/B or multivariate testing. Payments, says Daniel Martin, managing consultant at Maxymiser, is "always an area that we test".

He adds: "There are always things we can be improving and there's always uplifts to be had in the payments area of every retail website." He points to "usual suspects" that retailers can explore through testing. They include presentation of information about delivery, security and terms and conditions. Meanwhile, the wording and positioning of reassuring messages can also be important.

Small changes in the way that each of these is presented can have a significant

CASE STUDY: HOW CLARKS USED TESTING TO IMPROVE ITS PAYMENT PROCESS AND LIFT CONVERSIONS

Shoe manufacturer and retailer Clarks found that small alterations to the presentation of its payment process had a significant effect on site conversions. The company teamed up with online testing experts Mayxmiser in a partnership that started in 2010 in order to find out how to adjust its site to give customers the best experience.

"Clarks has always been very customer-focused – it's a major part of our ethos. But having launched the website, we knew that we didn't yet have the 'voice' of our online customers," says Mark Carlock, web analytics manager, Clarks. "The site was how we wanted it – but we needed to establish whether it was how our customers wanted it.

Among the areas that it examined through the prism of multivariate testing, was the payment process. "We knew people were coming onto the site and viewing products, but we weren't clear on why people were leaving without purchasing," says Carlock. "What's more, we didn't understand whether changes we were making to the site were helping or hindering us."

Maxymiser and Clarks drew up a programme to analyse every part of the sales funnel, from the landing pages to the checkout. One checkout test looked at a simple change in wording about delivery charges. The minor change that was introduced as a result boosted conversion by 4.2 per cent. "This is huge," says Carlock. "The test showed that a small change in phraseology could provide the catalyst for real improvements in conversion. This highlights a major tenet of multivariate testing: little things can drive huge change."

Another checkout test questioned why Clarks was using a 'closed basket' that meant users could not longer see the items they had put in their basket. "They couldn't see what they were buying," says Carlock. "The subsequent test suggested an 'open basket' increased customers' propensity to purchase. It led to a 1.99 per cent increase in conversion. In financial terms, that's a massive uplift for us."

Carlock says the retailer's approach to testing has altered over time. "Not only do we test our site more than ever," says Carlock, "but the way we test continues to evolve too. If we want to build something new into the website, we can now test it pre-launch and it makes such a difference. Testing has become part of our culture. We couldn't do without it."

impact in the way that shoppers use the site. Highlighting returns, or using different payment options can inspire some shoppers to spend more, and retailers can get a clearer idea of what works for their customers by testing

> **Testing across different markets is critical because shoppers from different countries can and do respond differently to the same information**

different versions. The choice of payment methods, for example, can have a measurable effect on the number of payments that are made. One payment option might prove a winner for some retailers while having a negative impact on sales for others. Testing, says Martin, can thus give useful business insights. "I think it's

about enabling the business to understand the value of that payment option, how successful it is and also use that to go back and get better terms and conditions from them."

The same can be true of security messages. Webtrends' Waterfall points to a test that his company ran on an international travel company's payment page across a number of different markets. He says that while consumers in the UK responded well to the inclusion of a small padlock symbol, underlining the company's approach to security, "It didn't work at all with the Nordic countries."

Testing across different markets is critical, says Maxymiser's Martin, because shoppers from different countries can and do respond differently to the same information. What might seem like a small difference on the page can make a real difference to the bottom line, and advocates of testing swear by its ability to deliver business changing insights.

When it comes to merchandising payments, that might be just the kind of long view that is needed. ■

ANY WHICH WAY TO PAY

DELIVERING THE SAME PAYMENTS EXPERIENCE IN-STORE, BY MOBILE, CALL CENTRE OR ONLINE AND KEEPING AHEAD OF THE FRAUDSTERS AT THE SAME TIME CAN BE CHALLENGING – ESPECIALLY AS SHOPPERS ADOPT NEW PAYMENT METHODS, REPORTS PENELOPE ODY

Where payments and fraud are concerned, delivering a seamless cross-channel experience may seem in theory to present few technological challenges, but in practice contains a host of pitfalls for the unwary. Problems range from insecure wi-fi and poorly integrated fraud control systems to complex refund issues and PCI-compliance. At the same time, received wisdom suggests that customers want an identical payments experience whether they buy online, via mobile or call centre, or in-store – and this requires a significant process change for many retailers.

"Consumers today expect retailing to be multichannel," says Akif Khan, director for products and services at CyberSource, "and that is most obviously seen in the growth of mobile. Merchants provide payment options using mobile apps – but how do they screen for fraud across multiple channels?"

A fraudster with a stolen credit card, for example, may be deterred from using it on a website as they don't have the 3-D Secure password, but they could then try their luck via a mobile app or call centre, so retailers need to have some means of checking whether an attempt has been made to use the card in a different channel.

As Dr Khan also points out, many retailers use the same fraud detection tools across all digital channels that they apply to standard online purchases – such as tracking an IP address or looking for abnormal shopping behaviour.

But on a mobile these parameters are not 'standard' – shoppers buy at anytime not in the 'usual' daytime office hours and the IP address may vary depending on the geography in which the mobile shopper happens to be. Typically, when travelling it may appear to be that of the head office of the mobile network provider. Standard 3-D Secure systems can also be difficult to use on a mobile's small screen so are bypassed by the apps.

"Our research suggests that 78 per cent of merchants who have m-commerce operations are using existing ecommerce fraud tools to screen their mobile channel," says Dr Khan. "A single fraud platform is ideal – but you need to create specific rules to match the channel and consumer behaviour within that channel."

Justin Fraser, sales and marketing director for Europe at Secure Trading agrees: "Mobile shopping is 24 by seven as your phone is never more than a foot away, so robust fraud systems have to be adaptive as consumer behaviour is changing all the time. A mobile phone is not a secure device from a PCI perspective and consumers are also perhaps not so aware of security issues with mobiles. Maybe there needs to be an education programme to highlight the risks."

HOT SPOTS

Using a mobile to make payments in a wi-fi hot spot, where transmissions are open and at risk from hackers, is part of

> **Open wi-fi is like opening the office door. You need to be able to restrict what guests can and cannot do on your network**

the problem. Free wi-fi in-store can be another. "Some retailers have just been dipping a toe in the water when it comes to offering free wi-fi," says Paul Leybourne, head of sales at Vodat. "So they've just been putting in a basic router for wi-fi, which is very easy to hack into and also doesn't segment corporate and guest traffic. Open wi-fi is

JUMP TO THE REAL WORLD

"PayPal is being proactive in taking a leap from ecommerce into the physical world, but if large enough numbers of consumers ask for a particular payment option in-store then marketing directors will do something about it – especially if PayPal can demonstrate that it can increase footfall."
Justin Fraser, sales and marketing director Europe, Secure Trading

REFUND ISSUES

"Electronic wallet providers have an aspiration for their wallets to become cross-channel but making a refund to a wallet can be a challenge for retailers – to start with, they have to identify which wallet, of several possible ones, the holder might have used."
Dr Akif Khan, director for products and services, CyberSource

ALTERNATIVE PAYMENTS

"In some geographies, notably South America, local credit cards are restricted to use in the domestic market, so if customers want to buy from an overseas website they have to use an alternative payment. It's proving a growing market for us – and cash payments are increasing in the Eurozone too."
David Hunter, CEO, Ukash

like opening the office door. You need to be able to restrict what guests can and cannot do on your network."

Restrictions can range from limiting bandwidth to denying access to competing websites by restricting users to the corporate site or certain brands only. For payments processing the wi-fi system also needs to be PCI compliant – and that obviously applies both for shoppers using their own mobiles to pay in-store or for payments made via tablets used by staff.

While monitoring fraud and ensuring payment security consistently across channels has its problems, what about the payment systems themselves? Do shoppers really expect to use the same payment methods wherever they shop – or is it more to do with returns and refunds?

Launched in May 2012 with Oasis, PayPal now has nine retailers, with around 900 outlets, live in the UK accepting payments via the system in-store at point of sale. In the US PayPal is already up to 23 retailers and 18,000 outlets and similar growth plans are in the pipeline for this side of the pond. "We're having a very positive response from retailers," says sales manager Jason Batten. "Customers can pay online with PayPal and when they return items to a store they can now have the money refunded direct to their PayPal account."

Implementation for retailers is said to be easy with no need for investment in additional IT technology, while for shoppers it is simply a matter of presenting the PayPal barcode on their mobiles at point-of-sale. PayPal is currently also trialling a pre-payment system with McDonald's in France. Shoppers pay for their orders using PayPal when ordering via a mobile or online and specify a collection time; they can then bypass the queues and collect their order from a pick-up point when they arrive at the outlet.

Presenting a barcode on a mobiles is not a problem for most larger retailers, but not all independent shops use barcode readers so for these retailers accepting PayPal in-store would require some investment. It's a similar story with contactless payments – whether using a contactless payment card, stick-on system of the Barclays Pay Tag variety, or one of the growing number of mobile phones enabled for NFC – including versions of Blackberry and Samsung's Galaxy – retailers will generally need an NFC-enabled reader and cost justification for the investment may be questionable with contactless card payments typically limited to transactions of £20 or less. However, many newer EFTPoS devices come with integral NFC capability. Ingenico, for

INTERNET RETAILING AWARDS

InternetRetailing
Selling in the digital age

Sponsored by

venda

YOU ARE INVITED TO

RETAIL'S HIGHEST AWARDS (202M (663 FT) TO BE PRECISE)

The Internet Retailing Awards, established on the 18th Birthday of eCommerce in 2012, seek out and recognise achievement by today's leading, admired and emulated multichannel retailers.

Join our judges, nominees, winners and leading retail professionals to celebrate eCommerce and multichannel excellence at our glittering awards party.

Wednesday 26th June
SushiSamba, Heron Tower, London

BOOK YOUR TICKETS AT:
www.internetretailingawards.net
Or you can contact us on 020 7933 8999 or info@internetretailing.net

example, has the technology embedded in most of its current range of readers. "Take up of NFC is still quite low," says account manager Russell Masterton, "as the system isn't really fully mature yet."

The UK Cards Associations lists more than a dozen retail chains where contactless cards are accepted on its website. Almost all of them are either fast food outlets or retailers – such as Boots, Tesco or Marks & Spencer – with a significant takeaway food business, as clearly that £20 transaction limit restricts usage.

ELECTRONIC WALLETS
Despite the growth of PayPal, most other electronic wallet systems are also in their infancy with a growing choice of systems – from the likes of Google, MasterCard and Visa for consumers to choose from. Rohit Patni, European vice-president sales and marketing at YesPay, is an enthusiast for the technology but admits that take up is slow. "We're not yet seeing any major demand for using electronic wallets in-store via a mobile phone," he says. "It's very different for shop's using and taking mobile payment on tablets where transactions are certainly increasing. I would expect to see wallet apps becoming more popular by the end of this year."

> " There's increasing convergence between channels and that could also apply to payment types in future "

Whatever those future in-store payment options might be, they have to be both cost-effective for the merchant and convenient for the consumers. With ecommerce payment methods that can vary, depending on geography, from basic credit card to direct bank debit to electronic wallet to prepaid cash, offering these in-store could not only stretch the existing till systems but also staff skills.

"We're seeing increasing convergence between channels and that could also apply to payment types in future," says Phil McGriskin, chief product officer with WorldPay, "with more cash payments

online and electronic wallets or direct debit payments in-store. It's obviously important for retailers to choose a payment services provider who can offer as full a range of payment options as possible from a single contract."

McGriskin points to WorldPay's recent acquisition of YesPay – best known for its in-store payments processing and electronic wallet developments – as symptomatic of this convergence trend. "It's a significant development for us," he says, "taking us into new payment markets through point of sale."

"Ecommerce payment options can be complex," says Tony Bryant, head of business development at K3 Retail, "and even more so when you start looking at refunds. How will a retailer cope with refunding payment to an electronic wallet when an item bought via a mobile is returned to store? Many of them can't even get click and collect right so how are they going to manage multiple payment options. The technology is not a problem – it's staff and business processes that will need to change."

CROSS-CHANNEL RETAIL JOURNEYS
With consumers regularly channel hoping on their shopping journeys, electronic wallets are not the only payment method that can confuse the unwary sales assistant. Ukash, for example, is seeing increased use of cash payments via mobile while some users

want to put Ukash 'money' into their PayPal accounts or onto pre-payment cards. "It seems that basket abandonment rates increase on mobile if the user is re-directed to a payment page," says David Hunter, CEO at Ukash. "Our merchants tell us that that they therefore like our system for mobile as they can accept the 19-digit Ukash number without having to redirect the shopper and that reduces the risk of abandonment."

Ensuring that sales staff know how to handle all these various options clearly has to be on the training agenda. What happens, for example, when a Ukash customer returning online goods to a store demands real cash as their refund rather than a credit to wallet or prepayment card?

With a raft of alternative payments used across Europe – from direct bank transfers to cash on delivery – returning goods to stores could clearly present even more awkward scenarios for sales staff in future. ■

RISK AND REWARDS

RETAILERS WHO TAKE A PRACTICAL APPROACH TO FRAUD SCREENING WITH A VIEW TO ENABLING AS MANY TRANSACTIONS AS POSSIBLE ACROSS THEIR CHANNELS WILL BOOST THE BOTTOM LINE – AND RETAIN CUSTOMER LOYALTY, SAYS CHLOE RIGBY

Do you want to prevent all fraud in your online shop? Simple. Close it down. Since such an approach would also spell the end of the business, many retailers prefer to take a pragmatic view, balancing an acceptable level of fraud risk against the potentially greater risk of losing customers through over-stringent fraud prevention measures. It's a risk that's currently front of retailers' minds, according to a recent

CyberSource study which found that UK online merchants were missing out on £1.8 billion a year in potential income when, for fear of fraud, they rejected valid payments. The primary challenge, cited by some 51 per cent of those questioned for CyberSource's 2013 *UK eCommerce Fraud Report*, is the risk of losing good business as a result of turning away too many good customers while trying to detect fraud. The study also showed that while retailers taking

part in the study rejected an average of four per cent of orders on suspicion of fraud, only 0.5 per cent of orders actually proved to be fraudulent.

"A lot of merchants will be wanting to minimise fraud rates," says CyberSource's director, products and services, Akif Khan, "but increasingly we're seeing merchants becoming more sophisticated than just a few years ago. The focus is moving from minimising fraud to maximising

profitability – the two don't always go in hand."

The challenge then for retailers is to take a practical approach to putting into place strong-enough fraud systems that don't slow down sales.

HOW FRAUD SCREENING WORKS

When a shopper submits their payment details to an ecommerce website, fraud screening services running in the background assess the quality of the transaction in real time. In the past, such fraud screening would simply mean checking customer details and email addresses against a list of 'good' and 'bad' consumers. Today screening happens in real time. Governed by a variety of rules set by the retailer and/or fraud screening provider to assess the likely risk, each transaction is judged on rules such as the buying history of the card, previous use of the device from which the transaction is being made, previous suspicious transactions, the location of the device and the registered address of the cardholder. From these factors the transaction is given a score. Depending on the score, a transaction will be immediately be cleared against the set rules, declined, or fall into a grey area for manual checking by a fraud analyst. That fraud analyst might be a member of the retailer's staff, or part of a team run by an outsourced fraud-screening provider.

The aim is to reduce the number of manual screenings that take place. Not only does reviewing transactions cost time and money, it also slows the customer experience considerably.

> " A recent study found that UK online merchants were missing out on £1.8 billion a year in potential income by rejecting valid payments "

"You don't want a fraud solution in place that is so rigid that it turns away good business," says Belinda Robson, head of fraud and risk at DataCash. "The consumer experience is the most important thing for a merchant today – they spend so much money bringing consumers onto their websites, and

SPEAKING FROM EXPERIENCE

CHESS GAME
"Fraud is like a game of chess – you make one move as a provider, fraudsters try and figure that out and make another move."
Belinda Robson, head of fraud and risk, DataCash

MAXIMISE 'GOOD' CUSTOMERS
"The price, typically, of having very low fraud rates is that you reject very good customers. We've seen a shift in merchants' activities to make sure they maximise the number of good customers."
Akif Khan, director, products and services, CyberSource

FRAUD MIGRATION
"We have noted that the fraudsters are migrating to the call centre and especially, mobile payments. Retailers need to prepare as transactions continue to grow to experience a lot of fraud unless they have the right strategy in place."
Ronan LeMestre, head of risk, ReD

NEW THREATS
"Retailers need to make sure they understand the risks that any new technology, device or system introduces to their business so they can ask the right questions and make sure they're working with right business partners and service providers who will help them do so securely.
Jeremy King, European director, PCI Council

competition is so strong so that if a fraud score rejects [a shopper] they'll just go to the next site. They're not going to retry and retry – they'll just go somewhere where it can be accepted."

So how do merchants balance that consumer experience with strong-enough fraud screening? Robson says the answer lies in analysing, evaluating and refining the fraud rules. "You can't implement the solution today, leave it running in the background and see in six months from now that it will still provide the same results, because fraudsters change," she says. "You need to keep refining in order to have pinpoint accuracy." Robson suggests that retailers should be aiming to flag between two and five per cent of transactions for manual review.

As the volume of sales continues to grow, manual checks on two per cent of all transactions will develop into a steadily larger, and more expensive, workload. However, Cybersource's recent study suggests that merchants are on average currently reviewing about 25 per cent of the transactions that they process. "That's a huge overhead in

terms of the headcount required and the impact on the customer experience," says Khan. "Decisions are being delayed about whether the transaction will be fulfilled or not."

BUYING INTO EXPERTISE

Many merchants decide to outsource their fraud screening systems, even if they choose to integrate different payments methods directly themselves. Doing so means that they can buy into the latest screening technologies and also benefit from the insights that fraud systems vendors gain when they work with large numbers of different retailers trading across the world.

But at the least, says Jeremy King, European director of the PCI Council, the organisation behind the PCI Standards that were developed in order to protect against card-related fraud, it's important that retailers act to make sure that new payment methods or other systems are integrated safely into their website systems. That's particularly important, he says, given that ecommerce was, according to Trustwave research of

WHAT'S NEW

Fraudsters have increasingly gone cross-channel as the way that we shop changes. That means retailers now need to think not only of online protection but also of channels such as their call centres and, most especially, of mobile commerce, now growing fast as a payment channel.

this year, the most targeted area for fraud in 2012. The organisation has developed a list of qualified integrators and resellers, the QIR programme, that retailers can safely use to integrate new software.

At a practical level, retailers can integrate with outsourced screening providers in one of two ways. First, they can integrate with screening technology at the back end of the website, with the practical effect that the consumer always stays on the merchant's website and doesn't feel they are moving to a third-party website. That approach carries the consideration that sensitive payment data is being entered directly on their website and means that they need to be compliant with the credit cards' verification programmes through the PCI Council's Data Security Standards (PCI DSS).

The second option for retailers is to integrate and the front end, opting for the payment and screening to happen on the provider's website. While this might be preferred from a data point of view, many merchants see that feeling of moving to a third-party website as a downside.

CROSS-CHANNEL FRAUD PREVENTION

Just as genuine customers and fraudsters move across sales channels, merchants increasingly need to adapt to multichannel screening. If a transaction fails on the website, it's possible that a fraudster or a genuine, frustrated, shopper might ring the call centre to try to buy again. Cross-channel fraud systems allow call centre operatives to see what happened on the website. "If a consumer has been rejected, do customer services' teams have visibility to look at the results from the fraud screening system and use that to help steer the conversation with the consumer?" asks CyberSource's Akif Khan. "If a consumer is rejected by the fraud screening because their address appears to be invalid, the customer service operator may then be able to elicit

the correct information from the consumer in order to turn that into a good purchase."

This comes with the caveat that customer service teams need to be well trained so they don't inadvertently give away information about the fraud-screening processes. "That's why it's critically important," says Khan, "that things like fraud screening and payment aren't really left as an afterthought but are an integral part of setting up any online or multichannel business so that the data can be integrated into all aspects of a modern multichannel retailer's environment."

Mobile is a key part of this multichannel challenge, warns Ronan Le Mestre, head of risk at fraud prevention specialists ReD, who detects an increase in fraudsters targeting new sales channels that they perceive to be less well protected. The fast-emerging mobile sales channel is a particular challenge for fraud screening because verification procedures that work well online, such as 3D Secure, do not currently operate on mobile. Equally, fraud-screening approaches such as checking the IP address of the device from which an order is placed do not apply to mobile devices.

Nonetheless, says the PCI Council's Jeremy King, while fraud may be adapting to new sales channels, the fundamental safeguards remain the same.

"Regardless of whether you're accepting a payment on a traditional POS device or using a phone, it comes back to the basics," he says. "You need to know what data you have and where it is, and then understand the risks associated and how to address them. From there it's about making sure you have the pieces in place to secure the data – including the people, process and technology. Remember, security is not just a technology choice, it's a business decision."

SETTING RULES

ReD's Le Mestre suggests that retailers can remove doubt presented as sales opportunities widen by learning to recognise 'good' customers. That means taking into account shopper history in the rules that retailers set, such as how many successful purchases a shopper has previously made. "If you know your good customers it's much easier to identify the fraudsters among the population," he says.

Meanwhile, it can also be easier to identify likely fraudsters by introducing screening rules around certain products, such as consumer electronics. "If you are

a big retailer maybe you don't want someone buying socks to end up in a queue for one of your agents to review," says Le Mestre. "If you are selling laptops or iPads that's the kind of order that you want for the verification so you need a system that allows you to get that granularity at a product level."

By setting rules retailers can also recognise common approaches to fraud. Account takeover, for example, sees a fraudster start to use an existing account at a retailer, entering user names and passwords that they already know. From there, it's a simple step to change email addresses and shipping addresses. Equally, these can be changes that take place perfectly innocently. "Any change of account, such as email address, shipping delivery, is not necessarily suspicious but you have to be careful," says Le Mestre.

Another approach to targeting fraud, Le Mestre suggests, is to put in place 'safer' delivery alternatives. Introduced correctly, he argues, click and collect should be safer because the shopper can be asked to show the card that they used to make the purchase when coming to collect an item.

An emerging trend most often spotted in the USA, as yet, is the move towards reshipment fraud. Here the fraudster places an order for shipment to a genuine

> **An emerging trend most often spotted in the USA is the move towards reshipment fraud**

address, on a genuine account. But after the order has been placed they will later contact the retailer's customer service to say that the item needs to be shipped to a different address. A further step, also more familiar in the US, is that the fraudster contacts the delivery company to make the change. The solution here, says Le Mestre, lies in the agreement that the retailer makes with their shipping company not to allow subsequent changes to the delivery address.

It's easy to be daunted by ecommerce fraud, currently running at high levels, but there are practical, and often simple, steps that retailers can take in order to avoid becoming a target." ■

PLANNING FOR TOMORROW

WHETHER IT IS CONTACTLESS CARDS, ALTERNATIVE PAYMENTS, INTERNATIONAL FRAUDSTERS OR EVER MORE EMPHASIS ON MOBILE THERE ARE PLENTY OF PAYMENTS AND FRAUD ISSUES FOR THE BOARD AGENDA, SAYS PENELOPE ODY

Ask many vendors and analysts working in the payment space about key upcoming issues and the vast majority will include mobile on their lists. Extend your survey beyond the UK or Europe and mobile could become even more significant.

As Ana Cunha, business development senior manager, UK, with WeDo Technologies puts it: "Mobile money should be on the radar for all retailers. There are more than three billion mobile phones worldwide, which is three times the number of bank accounts. We can expect to see a range of devices and end-to-end services emerge."

For developing markets, mobiles already outnumber landlines by a significant amount: Brazil, for example, has around 34 million landlines in use and around one million public telephones, while the country boasts almost 162 million mobile devices for a population of around 194 million. In China, there are 183 million landline subscribers but more than one billion mobiles in use for a population of 1.3 billion.

As has frequently happened in the past, emerging markets tend to leapfrog established systems when new technologies appear: it was much the same with the growth of payment cards in southern Europe in the 1980s as consumers opted to bypass cheques.

What form those mobile payments will take remains to be seen, with digital wallet schemes still largely in their infancy in many geographies and concerns – recently highlighted in the media – about the security risks of wi-fi systems. "Wireless hot spots generally have no control mechanism for restricting access," says Paul Leybourne head of sales at Vodat, "so all traffic is open to everybody."

Hacking such traffic is comparatively straightforward for the fraudsters and while reports of such challenges may be rare, the possibility can be enough to deter consumers.

FINDING NEW PARTNERS

For retailers, the growth of digital wallets could also mean working with new payment processing partners. "Retailers could see an increased reliance on new third-party providers specialising on mobile with multiple entities who will be 'partnering' for the first time," suggests Ana Cunha. "Retailers must consider the implications and requirements to enable them to minimise their exposure to fraud and security risks."

While take-up of digital wallets in the UK is still comparatively new, elsewhere they are more established. In Japan, wallets have

been in use since NTT Docomo launched its Osaifu-Keitai system for its mobile phones in 2004. The Osaifu services are now supported by all Japan's mobile phone carriers and so far, the country has six main competing cashless payment systems, many of them embedded into mobile phones. Osaifu services include electronic money, identity card, loyalty card, and even fare collection. However, usage rates both for e-wallets and contactless cards remain low with many consumers doubting the security of such systems.

Elsewhere, traditional card providers – such as Visa, MasterCard, and American Express – are actively promoting wallets while payment processors and systems providers, such as Neteller, Skrill, and YesPay (now owned by WorldPay) also have wallet offerings. In various parts of the world so too do the likes of Google, Lemon or Isis. Add systems for transferring money between friends or using on specific social media sites – including PingIt, Venmo, or Chirpify – and the options for consumers are many and confusing.

If, as the futurists suggest, consumers will eventually want to pay for purchases in-store using these various mobile wallets, then retailers will not only need systems that can accept such payments at their till-points, but also the ability to make refunds to these various wallets and, as Cunha suggests, a raft of new payment processing agreements to cover the various options. Those little stickers on shop doors declaring that Visa MasterCard *et alia* are "accepted here" may proliferate significantly.

BY TUBE TO THE FUTURE

While digital wallets may still be of interest to a minority of consumers, many now have a contactless payment card in their pockets. According to the UK Cards Association as at September 2012 some 30.3 million contactless cards had been issued in the UK. Despite the maximum transaction value increasing from £15 to £20 in June, usage rates are still low with

> **Emerging markets tend to leapfrog established systems when new technologies appear**

takeaway food still dominating. However, London buses started accepting the cards last December and what the Cards Association describes as the 'killer application' – the London Underground – is expected to start accepting the cards later this year.

Increasing user familiarity might encourage more retailers to install contactless card readers which, in turn, might encourage more use of NFC. That would also enable digital wallets at point of sale using NFC rather than wi-fi – perceived as potentially more risky; but there a great many 'mights' in the prospect, and if the Japanese experience is any guide it could be several years before such payments become widely accepted and mainstream. So for retail boards in the UK while mobile payments must certainly be 'on the radar' they are not yet at the top of the agenda: for those multichannel operations looking for growth in the BRIC countries it could, however, prove to be a very different story.

A more immediate concern for retailers looking for international growth is the proliferation of alternative payment systems used in various geographies. In much of the world real time bank transfers, direct debits or cash on delivery, can be preferred to the online credit card payments that dominate in the UK. "There are more than 230 alternative payment schemes in operation across the globe," says Phil McGriskin, chief product officer at WorldPay, "so even knowing where to start can be hard. Companies of all kinds can use alternative payments to their benefit, but to do that they need to understand which schemes are right for them – for their customers, their industry and their business model."

Julian Wallis, head of sales, UK & Ireland at Ogone agrees: "Local payment method acceptance should be on e-tailers' radar screens. When asked 'If you had to choose between two websites that offered the same product at the same price, which of the reasons below would influence your choice of where to buy?' 55 per cent of respondents in a study by Mindwave answered that they would choose the website which accepts the payment method they prefer to use."

LOCAL OPTIONS

Although some retailers do appear to trade successfully internationally while continuing to offer only familiar UK payment options, the consensus view argues that a wider range of alternative payments is essential – and that can apply to various channels and consumer behaviours not just in-store or online.

"Cash is one of those things that people tend not to think about in a multichannel market," says David Hunter, CEO at Ukash, "but its use is increasing. We find that some customers use Ukash for the first two or three times that they buy from a particular site and then, when their confidence in the site's reliability is assured, they switch to credit card payments. In Canada, we're also working with companies that take payments by telephone using interactive voice response and customers are happy to read out a Ukash code over the phone rather than give card details. We've not really promoted this option to merchants here but there is no reason why it couldn't work."

International aspects of fraud prevention also need to be on the agenda as retailers focus on overseas growth. Applying the same approach as in the UK can be effective in certain geographies. Fashion retailer River Island, for example, launched its international operation in September 2011. "What's the difference between overseas fraud and UK fraud?" Steve Frame, head of safety and loss told a recent retail fraud conference. "We talked to other retailers already trading overseas and had good feedback from them and it seemed that third party providers and suppliers exaggerated the risks. We continued with 3D-Secure for overseas sales although we had to relax our address verification strategy."

> " Longer term, biometric security is a likely development, potentially linked to mobile devices "

River Island divided its target markets into low-, medium- or high-risk countries and split the efforts of the fraud prevention team accordingly, so that expensive manual checks were focussed on areas of highest perceived risk. "You can't trade somewhere where you've not traded before without thinking about the risks and developing some sort of strategy," he says.

REDUCING CHARGEBACKS

Frame argues that each fraud investigator should be able to add up to £3 million in extra sales each year by approving transactions in manual checks that had been challenged by automated systems. The result is that 90 per cent of transactions that the systems highlights are ultimately approved and the company has a chargeback rate of less than 0.5 per cent.

Fraudsters are notorious for always finding new ways to outwit fraud-prevention systems so among newer technologies that the anti-fraud systems providers hope will help keep retailers ahead of the game are greater use of behavioural analysis, device fingerprinting and biometrics.

"Behaviour analysis is one of the most discussed of the new technologies available to combat fraud," says Dr Akif Khan, director for products and services at CyberSource. "Fraudsters will often take a very direct and identifiable route to the checkout, in a manner that can be patterned and recognised. By examining the 'clickstream', e-tailers can identify patterns that look like fraud."

Device fingerprinting – which validates the authenticity and geographical locations of the computer being used to make a purchase is also becoming more significant – although it can be the cause of false negatives with an increasingly mobile customer base likely to be shopping legitimately from a locations which does not match their payment card or delivery details.

"Longer term, biometrics are the most likely next development, potentially linked to mobile devices," says Justin Fraser, at Secure Trading. "There are already voice-based solutions in the market place, but they are hampered by the lack of take-up from consumers. Whatever the next step is it has to be convenient to the consumer to dissuade basket abandonment."

Looking ahead Fraser may be right. According to futurologist Dr Peter Cochrane, contactless technology will be mainstream by 2015 but by 2020 something mobile will be taking over: "Personal technologies are going to become something that you wear, then a jewellery or a badge. Instead of holding up your phone to the counter, you'll be holding up a bracelet on your wrist."

By 2025 Dr Cochrane believes that such items will be replaced or augmented with biometrics such as fingerprint or retinal scan. Such technologies have, of course, been available for years and retail point of sale systems using fingerprint ID go back to the 1990s. Adding a reader to ever PC or mobile, and registering every fingerprint in a central system for international authentication would be rather more complicated. ∎

A MATTER OF BALANCE

RETAILERS NEED TO MEET SHOPPERS' EXPECTATIONS TO INSPIRE TRUST IN THE PAYMENT PROCESS – AND RECOGNISE THAT THOSE EXPECTATIONS VARY IN DIFFERENT PARTS OF THE WORLD. CHLOE RIGBY REPORTS

Buying online is an act of faith for shopper and retailer alike. If a transaction is to succeed, the shopper must believe that the retailer will give them goods in exchange for their money, and that a refund will be forthcoming if they don't ultimately warm to the as-yet-unseen items. For the other side, the retailer must believe that the deal is a good one, backed up by real money from a real customer. If both parties do not believe in the purchase, then either the customer may decide not to part with their card details or the retailer's fraud screening will rule out the customer's business.

The onus is firmly on the merchant to mitigate that risk for both parties – and to communicate this clearly. By doing so, the retailer will inspire trust in the customer. And by having reliable fraud-screening processes, the retailer will know when it's safe to accept the customer's payment. Nowhere is that trust more critical than at the point of payment, says Jean Marc Noel of the trustmark scheme Trusted Shops. "Without trust there is no trade so it's utterly important for an online seller to inspire trust in the buyer," he says. "The payment is eventually the result of the trust in the transaction."

COMMUNICATING TRUSTWORTHINESS
Inspiring trust is easier said than done. For while consumers do want reassurance that their payment details will be safe with a merchant, at the same time they don't want to be held up through

cumbersome verification processes that give the merchant piece of mind.

Balancing those two requirements starts well before the point of payment – with first impressions. For those with well-known brand names, those impressions start before the customer arrives at the shop, when it's important that a website confirms previous expectations. For all retailers, strong, relevant images and branding, good navigation and a well-functioning search engine are all part of creating the all-important early impact. "The brain computes within 100 milliseconds your first impression and you decide whether something you're looking at is trustworthy or not," says Noel. "So the first thing is to have the proper appearance and be trustworthy at first sight."

Just as a travel retailer will reassure through the presence of an Atol or an Abta logo, trustmarks may also help to reassure. Noel says that behind its Trusted Shops logo lies the organisation's guarantee to customers of problem-free shopping when they buy from an accredited store. "If you ordered and the goods don't come, or if you send the goods back and don't get the money in 30 days, we will reimburse the online buyer and take care of all the discussions with the shop," he says.

This type of reassuring message can also be communicated on the site, leading up to and throughout the payment process. Trusted Shops' own studies found that there's a higher rate of cart abandonment for carts containing higher-value goods. Focusing reassurance on higher-value transactions can therefore have an impact on checkouts. This is a good time to remind customers of promises, whether that's a money-back guarantee or the pledge of free and easy returns. For more on this, see our merchandising feature (page xx).

Trustworthiness is also about meeting expectations. Consumer expectations formed through advertising, PR and

> **The onus is firmly on the merchant to mitigate the risk of fraud – and to communicate this clearly to customers**

word-of-mouth recommendation, both on and off social media networks, can be powerful. But to be effective, those expectations must be confirmed. That happens for customers through their judgement of the website itself, as well as on-site ratings and recommendations. "Ensuring good service is fundamental to gaining those recommendations in the first place," says Noel. "It's a really important thing if you can provide genuine customer reviews that show others have had a good experience, or if they had a bad experience online sellers can tell how they solved the issue: that's how you create trust."

MEETING EXPECTATIONS IN DIFFERENT MARKETS

But in the payments process itself, delivering on expectations is also about offering the payment types that consumers expect – and that varies from market to market.

While consumers in the UK expect to pay through credit or debit cards or alternative payment methods such as PayPal, shoppers in other markets have different expectations. Featuring the iDeal bank-to-bank transfer system is a given for those hoping to sell in Holland – something that Marks & Spencer recognised when it recently launched a dedicated website for the Netherlands. Similarly, German consumers, who are less likely to have credit cards, expect a cash-on-delivery option. Researching local markets, both by analysing local websites and the dedicated websites of those UK retailers who do well in that market, will clarify what local expectations are.

But just as different payment types will meet different expectations of paying in other markets, there are also varying expectations of the verification processes that sites will take their customers through.

Close to home, there's a growing perception that security systems such as 3-D Secure, which interrupt the payment flow and rely on customers

MOBILE FUN: ENGAGING CUSTOMERS THROUGH INTERNATIONAL PAYMENTS

In recent years, mobile accessories retailer Mobile Fun has expanded fast in international markets. The company, founded in 2000, now sells in more than 30 countries around the world, having launched in 20 new markets in the last financial year alone. Managing director Mohammed Hussain says payments have been key to this rapid overseas expansion.

"Customers want to pay using methods that they are familiar with," he says. "If we didn't offer iDeal in The Netherlands or COD (cash on delivery) in Germany, we would lose customers. "It is extremely important to get payments right for all countries. We have invested time and effort in understanding and localising payment options for each country we operate in."

To do that, Mobile Fun's dedicated country managers work with local payment providers to set up payment methods locally. "Although we are aware that there are global payment providers who offer local payment methods internationally, for a premium," says Hussain, "we have so far not chosen to use them as we have developed an in-house capability to integrate directly with local payment providers in other countries. Our local office managers have found that offering local payment options is more popular with customers."

Engaging with customers throughout the payments process is part of the expansion strategy. Each Mobile Fun website is designed to enable customers to flag up any problem areas quickly, though features such as customer feedback points. "Local accreditation from third-party reputation management sites also serves to reassure customers," says Hussain.

Hussain advises companies moving into new markets not to underestimate the importance of localisation – and that includes using the local payment provider. "Don't assume that your UK credit card provider can take payments in other countries, even when they claim it is possible, as payment failure rates can be very high in countries where the UK provider is used. A local provider is usually the better option so, in countries where local payment types are prevalent, take the time to consider all of the options and then decide which is best, from an effort versus reward basis."

When it comes to deterring fraud however, the company has found that following UK best practice guidelines works well. It sets strict rules for assessing transactions, and finds that the rules that work in the UK also function well overseas. "We can conduct security checks on orders at our local offices," says Hussain, "but our advice is to follow UK best practice as we have found that it works when dealing with international payments too."

remembering yet another password, can deter them from buying (see the logistics feature on page xx for more). Over-zealous fraud screening systems may also run the risk of turning away too many customers. Overseas, there may be lower tolerance of the interruptions that fraud screening can present. Don Bush, VP marketing at

> **" Taking conversations around payment and fraud beyond the website can be effective in driving sales "**

Kount, suggests that Americans, for example, may be less patient of third-party screening processes that take customers off the site. "I know in certain countries in Europe this is much more acceptable in the marketplace, but once you step outside Europe, go to the US, Canada, Australia, if they're truly an international company, going through third-party offsite processes is a conversion killer," he says. That's a thought worth considering, given a recent Barclays study that found retailers believe the United States is the most difficult market to break into.

Also important is to consider the implications of different fraud processes for consumers and retailers. For example, there's no limit to the length of time that consumers in Germany have to chargeback an unsatisfactory online purchase.

COMMUNICATING THROUGH THE PAYMENTS AND FRAUD PROCESS

It's difficult to overstate the important of communicating with shoppers throughout the payment process. We've already looked at how retailers can use reassuring messages close to purchase to overcome shoppers' doubts about purchase. Keeping that communication open throughout the payments process remains important, especially when paying takes the customer into verification processes that ultimately exist for the retailer's protection. If payment will take the shopper to a third-party website for verification, a clear explanation of that fact, emphasising the security benefits to the consumer, will promote both understanding and acceptance. Similarly compliance with the PCI Data Security Standard should also be explained, and in layman's terms.

Taking the conversation beyond the website can also be effective. Ellen Valentine, product evangelist in the marketing department at email marketing services provider Silverpop, points to ways of communicating payment options to both potential and existing customers through automated email campaigns.

As well as reminding customers of payment options and membership trust-based organisations in initial welcome emails, Valentine says email can also be relevant for communications around the payment process. "Since one of the reasons someone may have abandoned their cart or basket is price or other payment considerations, in the remarketing emails retailers can again remind customers of the different payment options and link to a page on the site with more details," she says. Emails sent to confirm purchases can also usefully remind customers of safe payment processes and the retailer's ability to store credit card details for the future.

But whether communications take place on or off the website, it's imperative that retailers continue to engage and talk to their customers throughout the payment process. ■

WHAT'S NEW

International markets have become a key focus for retailers looking to boost growth rates over recent months. Getting payments and fraud right is a prerequisite for engaging with potential customers likely to be new to the brand. Think local and research new markets to find out what payment methods will be most successful.

A midst all the froth and fuss surrounding the move to cross-channel retail, it's sometimes easy to overlook the fact that a merchant's digital presence ultimately needs to be judged on whether it's effective. The most stylish websites and interfaces don't do their job if customers won't part with money after visiting. All the talk in the world about grand strategies, moving into new markets and the rise of new devices as sales channels can't hide this fact.

So are retailers acknowledging this truth? On the balance of what we've found researching this latest *Internet Retailing* supplement, we'd offer a guarded yes to this question. Perhaps in part because economic conditions continue to be so difficult that commentators now routinely talk about a new normal of low growth and even stagnation, retailers are having to look hard at the bottom line. This has meant a new focus on the whole area of payment and fraud.

There's also a new sophistication around the fraud part of this equation. As we discovered researching the logistics feature, companies are no longer prepared to run the risk of turning away valid customers for the sake of avoiding a few bad transactions. Instead, there's a pragmatic recognition that merchants need to accept a certain level of loss in order to drive sales. Make a website too difficult to use and it really shouldn't come as any surprise that customers won't use it.

In addition, forward-looking retailers are fully aware of changes just over the horizon. The world of e-wallets, mobile payments and near-field communication may be in its infancy but larger companies especially are already preparing for this new reality.

Furthermore, as retailers begin to expand overseas, many have gained experience of the problems around the different payment options that are expected in different territories. Granted, companies may be understandably nervous of, for example, the Chinese liking for cash-on-delivery shipments where customers pay the postman for goods, but they're still acutely aware that there's an opportunity in this vast new market.

Against that, payments and fraud still remain an unglamorous afterthought for too many within the ecommerce sphere. This attitude needs to change. As we discovered when talking to usability experts for the interface and design feature, fine-tuning the layout of checkout pages can add significantly to sales. This may not be as sexy as organising a marketing campaign, but it may ultimately yield more returns for the company.

Finally, while news of the decline in PC usage is clearly recognised within the industry, there's arguably not enough recognition of what this means. Where once ecommerce professionals could assume they were going to push customers down a sales funnel, and that the customer would have easy access to a keyboard to type in personal details and credit card numbers, that's no longer the case. While the cardinal rule that the checkout process needs to be as quick and easy as possible remains, retailers need to recognise that this may involve designing a slick checkout process that's optimised for a tablet. Quite what best practice here will look like, we're not yet sure but retailers still need to be thinking ahead to this day.

This supplement is the latest in *Internet Retailing's* ongoing series. Each explores questions facing e-retailers today through six key aspects: interface and design, merchandising, cross-channel experience, logistics, strategy and customer engagement. We welcome your input and suggestions for future themes at editor@internetretailing.net.

Chloe Rigby and Jonathan Wright
chloe@internetretailing.net
jonathan@internetretailing.net