Tomorrow’s Transactions—The Transit Reader

Tomorrow’s Transactions
The Transit Reader

A selection of papers, posts and articles from Consult Hyperion about transit payments technology

By David G.W. Birch, Mike Burden, Simon Laker and John Elliott
Edited by Jane Adams
Contents

ABOUT CONSULT HYPERION .......................................................... 4
ABOUT THE CONTRIBUTORS: ....................................................... 6
CHAPTER 1: WHITE PAPER - EMV PAYMENTS IN TRANSPORT ................................................................. 8
CHAPTER 2: SELECTED BLOG POSTS FROM THE TOMORROW’S TRANSACTIONS BLOG ........................................ 19
CHAPTER 3: ARTICLES ABOUT TRANSIT TICKETING .......... 38
About Consult Hyperion

Who are we?
Founded in 1985, Consult Hyperion offers consultants and associates expert in the design and implementation of mobile payments and POS, ticketing products and services, contact and contactless based payment, NFC, identity and Internet. We are supported by Hyperlab - software and design engineers practised in the development and implementation of pilot and commercial grade products and services with expertise in standard programming and software development and management tools as well as technologies including: Microsoft .NET, Windows Phone, Android and iOS development (cross platform development with Xamarin tools), BlackBerry, embedded C, Java, JavaCard, MULTOS, HTML5 and Python, and by an extensive test laboratory used to optimize or certify the operation of these systems.

Why work with Consult Hyperion?
We are independent - we have no off-the-shelf products. Nor do we sell or promote third-party solutions, partner or form strategic relationships with third-party vendors. We are expert, understanding in great detail secure payments, identity management and fixed and mobile communication technology. We have detailed knowledge of the associated technical standards, regulations and business models and how they can be used to secure future revenue streams. We are globally recognised as thought leaders and experts within the areas of mobile, identity, contactless and NFC payment, EMV and ticketing. Our clients consistently praise us for being flexible, responsive, trusted, technical experts and thought leaders.

Our involvement in your project team will ensure that you deliver a marketing leading solution, underpinned by global best practice, readying you for the expected evolution of future technology.

We’d like to thank Eurotransport Magazine for permitting re-use of an article that first appeared in Eurotransport Issue 4 2013 and can be found at www.eurotransportmagazine.com.
More information
For more information about how Consult Hyperion can help your organisation transform its payments capabilities, strategies and operations and make informed and positive business decisions, please contact:

John Elliott
Head of Public Sector
john.elliott@chyp.com

Lanny Byers
Managing Director, CHyp USA
USA
lanny.byers@chyp.com

Mike Burden
Principle Consultant, Transit Practice
UK
mike.burden@chyp.com

CHyp USA Inc.
535 Madison Avenue, 19th Floor,
New York, NY 10022
USA
Tel: (888) 835-6124
Fax: (212) 207-1019

Consult Hyperion
Tweed House
12 The Mount
Guildford
Surrey GU2 4HN
UK
Tel: +44 (0) 1483 301 793
Fax: +44 (0) 1483 561 657
About the contributors:

David G.W. Birch is a Director of Consult Hyperion, the technical consultancy that specialises in electronic transactions. Here he provides specialist consultancy support to clients around the world, including all of the leading payment brands, major telecommunications providers, government bodies and international organisations including the OECD. Before helping to found Consult Hyperion in 1986, he spent several years working as a consultant in Europe, the Far East and North America. He graduated from the University of Southampton with a B.Sc (Hons.) in Physics.

Described at the Oxford Internet Institute as “one of Britain’s most acute observers of the Internet and social networks”, in The Telegraph as “one of the world’s leading experts on digital money”, in The Independent as a "grade-A geek", by the Centre for the Study of Financial Innovation as "one of the most user-friendly of the UK's uber-techie" and in Financial World as "mad", Dave is a member of the editorial board of the E-Finance & Payments Law and Policy, a columnist for SPEED and well-known for his thought leadership blogging and podcasting at Tomorrow’s Transactions.

Dave has been rated by Wired as one of their top 15 sources of business information and by Total Payments as #1 influencer on emerging payments. He has lectured to MBA level on the impact of new information and communications technologies, contributed to publications ranging from the Parliamentary IT Review to Prospect and Financial World. He wrote a Guardian column for many years. He is a media commentator on electronic business issues and has appeared on BBC television and radio, Sky and other channels around the world.

John Elliott is a Managing Consultant and the head of the Public Sector Practice since 2005 and has been with Consult Hyperion since 1998. He is the inventor of Consult Hyperion’s Technology Roadmapping methodology that has been used many times since 2004 for clients ranging from national governments to global payment schemes.

In the field of digital identity, John has advised governments in Europe, the Middle East and the Asia-Pacific region on smart identity cards. He was a key member of the Consult Hyperion team that specified the ground-breaking Hong Kong smart identity card and associated systems. John has led various research reports into state of the art electronic identity for the European Commission.
In the field of transport smart ticketing, John has worked on strategic studies for European governments including cost-benefit analyses for national schemes, design of security architectures and migration plans, and technical specification of extensions to allow the use of Chip and PIN cards and mobile devices for e-ticketing. John has a PhD from the University of Edinburgh and is a Chartered Engineer with over 17 years IT industry experience.

**Mike Burden** has over 20 years experience in transport systems engineering ranging from research into electronic payment systems in transport through to the design of smart card automatic fare collection systems and road user charging schemes. He is a chartered electrical engineer, member of the IET, Institute of Physics and The BCS and is currently responsible for Consult Hyperion’s business development in the public sector, with particular focus on the transport and identity sectors.

During his time at Consult Hyperion he has been responsible for building a range of projects, particularly in transportation with the DfT and TfL and Translink systems in the Netherlands. More recently he has begun to develop a market in the US.

In the identity market he has been responsible for projects with the European Commission and several overseas governments including Ireland, Hong Kong and Saudi Arabia. Mike holds a BEng(Hons) in electrical and electronic engineering, an MSc in optoelectronics and an MBA.

**Simon Laker** is a recognised expert in the design and operation of secure payment services. He has over 10 years experience of designing and implementing EMV enabled solutions, including the authoring of technical specifications and implementation guides for the payment schemes and the certification of third party devices against those specifications. Simon has a working knowledge of the mobile POS market and the technologies that are likely to support this market over the next five years, from projects he has completed for Powa Technologies (mPoS), First Data (NFC & TSM), American Express and Visa International (mobile payments).

He has an in-depth knowledge of the implementation of open payments systems in public transport, using payment cards as a token for travel. He worked with Transport for London and the major payment schemes to define the operational and transaction models to support the use of payment cards in place of transit tickets in the UK. His work has subsequently been adopted and deployed globally by the payment schemes. Simon is currently using his knowledge to help define similar schemes in a number of cities in Europe and the US.
Chapter 1: White Paper - EMV Payments in Transport

Authors: Mike Burden and Simon Laker

Executive summary
Public transport ticketing has come a long way over the last 30 years, moving from paper-based tickets and magnetic stripe to smart cards. However, these are usually proprietary schemes developed by a single supplier, within a closed network, which require considerable capital investment and have substantial operating costs.

As technology has developed in other sectors, most noticeably through mobile communications and the switch to contactless cards in the banking industry, opportunities are opening up for operators to make public transport ticketing more convenient for users and cheaper to run. They also offer new ways of collecting revenue, breaking away from traditional ticketing methods.

The introduction of EMV based card payments in the US will provide a fast, secure and convenient method of payment to regular travellers and tourists alike. There will need to be some technical changes to current PoS devices as well as some changes in liability. However, EMV payment offers several advantages to transit, such as off-line authentication, that can increase throughput, and help transit agencies manage transaction charges.

The paper will address the issues that transport operators need to be aware of when making the move to an open system based on experiences from Transport for London (TfL) including:

- Developing a transaction model
- Designing technology to support the transaction model
- Developing new fare products.

Background
Public transport operators are already appreciating the benefits of smart card ticketing, including faster gate entry or boarding, particularly at peak times. Ticket selling is more cost-effective, with a wider range of sales outlets, including the Internet, whilst the security advantages over magnetic stripe and paper tickets have helped to cut known fraud and highlight other fraud. More information is available about passenger
movements, allowing operators to refine their services and offer loyalty products.

However, customer expectations are changing rapidly. Online retail has changed consumer buying habits and there is an expectation that all transactions can be undertaken in a fast, customer-friendly way. Standing in a queue at a ticket machine does not fit this model. Therefore, leading transit operators such as Metropolitan Transport Authority, New York (MTA), Chicago Transit Authority (CTA) and Transport for London (TfL) are beginning to look at a new generation of ‘open payment’ systems.

**Technology**

Ticketing technology has evolved significantly over the last 100 years as the diagram below shows. This started with cash and moved through paper tickets, to smart tickets on card and mobile phones. There are also examples of identity tokens being used to indicate that the holder is entitled to travel, with payment made after the journey. This trend is starting to reflect what is happening in wider society as payment methods are beginning to change. It is not clear that there will be one” winner” with regards to the technology as some schemes, such as TfL accept multiple technologies and standards (cash, paper, magnetic stripe, proprietary smart card (Oyster), EMV smart card, ITSO smart card) in response to what the travelling public are wanting to use to pay for their journey. This means that systems become more complex in the back office as they need to process some of these transactions in a different way, e.g. proprietary smart card, EMV, ITSO. This means that transit operators, and system vendors, need to specify schemes that will be flexible enough to respond to changing requirements of payments over the coming years, to ensure that the investment is in a scheme that won’t become rapidly outdated.

*Ticketing technology has evolved over the last 100 years*
Open and closed systems

Early smart card schemes, such as Oyster in London and SmarTrip in Washington DC, have been based on “closed-systems” which means that they can only be used in the transport environment to pay for transit. Typically in a closed system the agency issues and manages its own media. These systems have tended to be based on proprietary systems and formats, although in Europe there have been moves to standardize these systems through the activities of Calypso, ITSO & VDV.

There needs to be an infrastructure in place to allow any stored value to be added, either through add-value machines (AVM), third party agents or ticket offices. If ticket products are stored on the cards then these will need to be loaded at the point of purchase using a special POS device.

It is usually the case that all fare calculations happen between the card and reader as the fare tables are stored in every reader and need to be updated whenever changes are made, which is a costly and time consuming exercise.

In a closed system details are stored on the card, usually in terms of ticket products, stored value and audit trails. The back office has limited information about the cardholder or their recent transactions, which makes getting to know customers difficult.

With the banks’ introduction of contactless payment cards there has been a lot of interest from transit authorities in making use of the contactless capabilities of these cards without the cost of having to issue contactless cards themselves. This means that there is no need for expensive infrastructure to reload the cards as the information is held in a central account and not locally on the cards.

These types of schemes are called open-loop, which means that the card can be used outside of the transport environment, particularly in a retail environment.

In this type of scheme the card acts as a token to a centrally held account which calculates all of the fares, after a journey has been made. This makes it much simpler to update fare tables as there is only one location where they are stored. The requirements for validators are also much simpler as the interaction with the card is just to check if the card is valid for payment or not and there are no fare calculations at this level.

One interesting new opportunity that open payment schemes present is the potential for using non-payment cards such as ID cards, campus cards or ski passes to identify holders as having the means to travel. A lot of these
options have been implemented in pilots and live implementations in places such as Salt Lake City over the last couple of years.

Several major transit authorities are looking to move from closed schemes to open schemes and are working on the issues that need to be resolved to make this happen in the short term. The diagram below illustrates this.

*There is a trend away from card based schemes towards account based schemes*

**From owners to merchants**

By moving to open payments, operators become ‘merchants’ participating in a bank-led scheme rather than owners of a dedicated ticketing infrastructure. This could reduce costs through the use of off-the-shelf equipment from a range of suppliers, rather than bespoke equipment made to proprietary specifications.

In all the cases discussed so far, with the exception of cash, the means to distribute the travel token has had to be considered as part of the process in deciding the media type used. This broader consideration of issuing tickets, printing or personalizing them with products, and accepting them at the point of entry is far removed from the transit operator’s primary objective of running buses, trains, subways and trams.

Payment cards offer the transit authority the opportunity of relinquishing the distraction of card issuance and focuses its time on running transit systems and accepting cards.
But what is the best way of doing that? In the US, while the contactless magnetic stripe card is ubiquitous, it introduces significant challenges in acceptance for transit merchants where there are tight transaction time constraints, and without the right level of transaction authorization, fraud can be rife.

Introduction of EMV (Europay, MasterCard, Visa) schemes can dramatically change the concept of ticket purchase, offering more sophisticated facilities that take advantage of being able to verify the card’s authenticity at the gate before entry.

Sales and distribution
There is clear evidence of a move away from a station based approach to sales and distribution of fare products to a more personalised approach. This is focused on the Internet and mobile methods of distribution.

Currently it is not unusual to see a long queue of commuters during the early morning rush hour waiting to buy tickets at a ticket machine. Some operators are responding to this problem by developing solutions that allows passengers to purchase their tickets before they get to the station, so reducing queuing times and improving the overall experience. In some cases the tickets have to be collected at a Ticket Vending Machine (TVM) which doesn’t seem to produce any additional benefit as the passenger still needs to wait in line. With the introduction of print at home tickets several
long distance UK rail operators have improved the experience for travellers and made it similar to airlines that have offered the ability to print out boarding cards at home based on barcode technology.

We are now beginning to see a response from transit authorities in allowing passengers to use technology they have with them, rather than issue a card or token to them. This has manifested itself in the form of contactless payment cards in London, mobile phones in Copenhagen and the proposed use of ID cards in Washington. All of these approaches mean that passengers can decide the best way for them to interact with the transit operator and the transit operator can provide the traveller with a convenient means of payment at a low operational cost.

**EMV in transport**

EMV is the technical standard that ensures chip-based payment cards and terminals are compatible around the world. The term refers to Europay, MasterCard and Visa, the three organisations that originally developed the specifications in 1994. The EMV standard is currently managed by EMVCo LLC, which is equally owned by American Express, JCB, MasterCard and Visa. Further information regarding EMVCo and the specifications can be found at [www.emvco.com](http://www.emvco.com).

An EMV payment uses a microprocessor embedded in a plastic card or a mobile device to connect to an EMV POS via a contact or contactless interface. The chip securely stores information about the payments application and performs cryptographic processing. This provides an additional level of card authentication which validates the legitimacy of the payment type being used.

EMV is more than secure retail payments. It opens the door to a range of innovative secure payment and identity solutions across multiple platforms, whilst offering a ubiquitous and low cost infrastructure through which to deliver complementary services.

Any organisation considering deploying an EMV infrastructure today should consider how their products will be used in the PoS, in ATMs, at kiosks, in mobile phones, through set top boxes, at the PC and in the transit environment. With careful design the same products can be used to:

- Remotely identify and authenticate the cardholder, make local or remote payments and deliver loyalty and couponing
- Manage the issuers exposure to fraud by limiting cardholder spend per day, per country or per transaction type (PIN, signature, or contactless) or simply by disabling the application over the air
- Deploy local or closed loop payment services, i.e. services not branded by the international payment schemes.

In the spring of 2011, Visa issued a road map for the U.S. adoption of a smartcard-based payments ecosystem. Since then, the other three major U.S. payments networks have followed suit. These road maps provide milestones for merchants, acquirers, and processors, along with dates on which these milestones are expected to be met. This includes a liability shift for merchants, illustrated below.

<table>
<thead>
<tr>
<th>Year</th>
<th>Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>• October: MasterCard &amp; Visa waive PCI Data security Audit Fee for merchants processing 75% or more POS transactions via EMV</td>
</tr>
</tbody>
</table>
| 2013 | • April: EMV Transactions Must be supported by Acquirers and Sub-Processors  
• April: Maestro shifts counterfeit fraud liability to ATM owner when an EMV enabled card is used outside country of origin, and ATM authenticates via magnetic stripe  
• October: MasterCard only. Merchants processing 75% or more EMV POS transactions receive 50% Account Data Compromise Relief |
| 2015+ | • October: MasterCard Only. Merchants processing 95% or more EMV POS transactions receive 100% Account Data Compromise relief.  
• October: MasterCard & Visa shift fraud liability to least secure entity for all POS transactions except automated fuel dispensers  
• 2016: MasterCard shifts counterfeit fraud liability to ATM owner for all EMV enabled cards used at U.S. ATMs (Credit & Debit)  
• 2017: MasterCard & Visa shift fraud liability to least secure entity for automated fuel dispensers |

Timetable for Liability Shift in the U.S.

Transaction models
Three key areas to consider when designing a new ticketing infrastructure are the scope of the network, interoperability and the likely cost savings. Urban operators have different priorities to their inter-urban or rural counterparts. Speed and self-service are priorities in the urban environment, while inter-urban operators need to offer a greater range of customer focused products and services, perhaps including integrated ticketing with connecting urban or rural services.

‘Pre-issued’ media, such as the bank credit or debit cards, offer the opportunity to develop a ticketing or payment strategy with zero issuance costs, making use of a device that the passenger already carries and is fully interoperable worldwide. But current payment cards are read-only; as a result, transaction data, value top-ups and ticketing products cannot be
stored on the card. Plans are in place to introduce payment cards that can hold transient data, supporting possible future ticketing applications. Meanwhile, the operator can choose to use the card to collect a payment at the ‘point of tap’ or sometime later. In this case, a new ‘middle-office’ infrastructure would collect the taps and charge an ‘end-of-day’ amount.

Mifare media, used in a closed network, can use the card as the primary device and maintain shadow data in the back office. In this case all tickets and value are held on the card and the fare calculation is carried out by the reader at every tap. If payment cards are selected, two basic options are available. In a reader-focused model, a payment transaction is performed and value taken from the card’s offline balance. At the end of the day, the transactions are settled via a merchant acquirer. In a back-office model, the tap would authenticate the card and harvest payment data, but the real transaction would be performed later, after the fare had been calculated.

<table>
<thead>
<tr>
<th>General Contactless Payment rules</th>
<th>Agreed new rules for transport PAYG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price is known before the card is presented</td>
<td>Each tap is £0, then operator back-office calculates price at end of day</td>
</tr>
</tbody>
</table>
| Use of card counters to manage risk & occasionally fall-forward to Chip & PIN | Operator manages risks to provide equivalent protection within the 500ms time limit:  
  • Offline data authentication of card  
  • Deny Lists (DLs) in terminals  
  • Online authorizations from the back-office |
| Terminal field is activated manually by store staff | Terminal field is always active to maximize throughput |

Visa and MasterCard have agreed a transaction model for Europe

Another important consideration is the communications requirements. Can the reader be offline or does it need a direct fast connection to a back-office system? All of the models discussed could operate in either mode, although the primary benefit of the card-based mode is to operate completely offline. The reader and middle-office models can also work offline but they may need occasional network access to pass data, such as hotlists to manage fraud and payment card authorisation requests.
Once EMV technology is available to the transit operators there are a number of models available to meet the fares policy in operation. Simple, fixed fare implementations, on buses for example, could just offline authorize against the balance on the card. Conversely, complex transit agencies such as MTA in New York and Bay Area Rapid Transit (BART) in San Francisco would need to use the authenticated tap as an ID and perform delayed online authorisations and aggregations.

**Operational costs**
The introduction of payment cards can lead to a number of areas of cost reduction. The most significant of these include the reduction of card issuance to zero, the end of dealing with issues raised around the management of a proprietary system and the end of the card and ticket distribution networks.

Based on the information in the chart below TfL considers it realistic to achieve savings of 4% on the current cost of sales, with further savings likely over the medium to long term.

![Split of costs in TfL’s revenue collection system](http://eprint.iacr.org/2008/166)

A recent significant cost to Mifare classic issuers was as a result of the hack on the MIFARE Crypto-1 algorithm that is used to secure the data on the card [http://eprint.iacr.org/2008/166]. This forced expensive migration in some cases to more secure platform utilising publicised cryptographic mechanisms.

The fact is that all of these cost pass to the card issuers and the payment schemes who manage the reader and card specifications. But these are costs they are paying now anyway – so they see benefits too!

However, you get nothing for free in this world. The cost of acceptance is interchange; the charge the schemes make for processing the payment
Tomorrow’s Transactions—The Transit Reader

which is passed to the transit merchant through the acquirer. And there are other costs.

Reader certification is expensive
Reader design is critical to the successful implementation of any project to accept new media. Bad design would increase the cost through unnecessary rounds of re-certification and could affect its vulnerability to security attacks, service denial or data harvesting.

The reader will be required to support numerous applications, so the software for each one – be it card detection, payment card applications such as Visa, MasterCard, American Express, Discover or a proprietary application – should be developed and installed separately, in a way more akin to loading applications onto a mobile phone. Otherwise, changes to one application could result in a need to retest the complete reader. And the high cost of certification will ensure that developers seek to minimise the number of times the reader is submitted, both initially and when changes are made to specifications and code.

Reader design should be optimised for easy and cost effective certification
If the reader is, or might be, handling payments data, the implications of PCI-DSS (Payment Card Industry Data Security Standard) must be considered. Payments data cannot be held or transmitted in a format that would allow it to be intercepted in plain text form. The most secure method for securing compliance would be to encrypt all transactional data at source before it is stored and transmitted.

But, how would operators know that everything will work to specification, and that transactions will not take minutes instead of milliseconds? The
answer is to prototype the system, and test the more complex processing which the reader must undertake. This includes activating the card and selecting the correct application, deny-list processing and other management processes required to meet PCI-DSS. This is the time to make mistakes and fix them.

There are still many challenges to implement readers that are capable of accepting cards from several schemes as contactless EMV is introduced and older technologies are phased out. Some transit operators such as Utah Transit Authority (UTA) have successfully implemented open payments and other operators such as TfL have just implemented them and will start to collect large amounts of data on how the proposition is received by travellers.

As the convergence of payment methods begins, bringing together payment card schemes and transport operators, there are many institutional issues that need to be addressed. But in the long term, convergence will produce benefits for all stakeholders and passengers.

**Conclusions**

Multiple technologies exist that can be used in automatic fare collection systems, ranging from paper tickets through, smart cards, mobile phones and identity cards. Operators are looking to maximize revenues and generate increases in ridership; by making payment simple and convenient for passengers, that is one less barrier that needs to be overcome.

A challenge that equipment vendors and scheme operators will face is to make the multiple technologies work together while being aware of new payment methods and which of these the travelling public will wish to use to pay for their travel.

When a new technology is implemented it should be put in place to support the fare policy. With new technologies it is possible to develop a new range of fare products from those currently available to transit schemes. With this in mind it is important that as part of any new scheme there is a thorough review of the fare policy and the new possibilities are identified and understood.

Developments in mobile provide a wide range of benefits to all parties. Much discussion has been ongoing around NFC in transit, but there are many other opportunities to use mobile devices as portable TVMs, which when combined with their GPS capabilities and ability to send and receive data provide the potential for many new and varied services.
Chapter 2: Selected blog posts from the Tomorrow’s Transactions blog

For the average person in most of the world, transport vies with retail as the place where they most frequently spend their money, not on the web or in the cloud, and these are the points-of-sale where innovation needs traction. This chapter gathers selected blog posts from the past few years by Dave Birch about transactions technology and innovation as it applies to transit. We have included some more general posts where they appear relevant. Many of the posts refer to Transport for London systems – TfL is a longstanding customer of Consult Hyperion and we have been closely involved with their payments systems development.

Mobile Payments will be huge, whatever the public say - 16/02/2011

Last year, I read a Deutsche Bank Research note about mobile payments that was given to me in a meeting with one of our clients (E-Banking Snapshot 34, August 2010). It highlighted a Forrester Research finding that 74% of European consumers and 64% of US consumers are not interested in purchasing goods or services via their mobile phones and said that this means there are substantial barriers to adoption of mobile payments. Well, there are certainly substantial barriers to the adoption of mobile payments, but in my experiences consumers are not one of them. Quite the reverse: in every project that I have been involved in, consumers have loved buying things using their mobile phones. The discrepancy comes, I think, because when you ask consumers about something new in a field they don’t care about (let’s face it, consumers don’t really spend that much time thinking about payments) they will react conservatively. Say to the average British consumer “would you like to use your mobile phone to pay for cups of coffee” and they can’t envisage what you are talking about, especially if they don’t live in London and use Oyster all the time or use 2D barcodes for travel tickets or whatever.

In a survey of 2,500 members of Springboard UK, the market research experts, on behalf of Vision Critical, half of respondents (51%) reported being fairly or very uncomfortable at the prospect of mobile payments.

[From British ‘uncomfortable’ about making mobile payments - Marketing news - Marketing magazine]

When consumers are given a mobile payment system that works and is convenient, adoption is rapid. Incidentally, in that survey only a fifth of
consumers said they were interested in a prepaid wallet. I’ve heard this over and over again: one of the arguments against substituting cash (which most consumers don’t see as a pre-paid product) with some form of ‘purse’ product is that people don’t want to pay up front for good or services that they might use in the future. Fair point. Oh, wait…

Starbucks Corp. customers loaded a record $700 million on to the Seattle coffee chain’s prepaid card accounts during its most recent quarter, up 39% from a year earlier

[From Starbucks Prepaid Loads Jump 39% - American Banker Article]

Turns out that if you know stuff about marketing, consumer behaviour, distribution, management, convenience, payment choices, advertising, incentives and, above all, retailing then customers are only too happy to go with mobile prepaid. That’s how come Starbucks went from a mobile payments experiment…

The ultimate goal of the program is to get customers to trade in their physical Starbucks Cards for the digital variety — it’s a time saving exchange for the customer and a cost saving exchange for the company. Already, one in five of all in-store transactions are paid for via Starbucks Card (mobile or physical), and more than $1 billion will have been loaded on to cards by year’s end.

[From Starbucks in New York Now Accepting Mobile]

...to a national roll-out in a quarter. Our good friend Brett King gave the Starbuck’s national mobile payment scheme a try and said that

...this is far superior to a current interaction using cash or a card for a number of reasons. This gives us a glimpse of what the cashless society will be like; it isn’t risky, it isn’t subject to fraud or theft, it is safe, secure and fast.

[From Brett King: Starbucks Mobile]

We all know that mobile will be the focus for the evolution of retail payments, and I think the message is getting out. Eric Schmidt’s talk at Barcelona— saying that NFC will be profitable—attracted a great deal of attention, mainly from people who didn’t listen to what he said when still CEO of Google.

Google wants the next generation of Android phones to replace credit cards, Eric E. Schmidt, Google’s chief executive, said
Tomorrow’s Transactions—The Transit Reader

Monday at the Web 2.0 Summit in San Francisco. The newest version of Android, Google’s mobile phone operating system, code-named Gingerbread, will come out in a few weeks, he said. It will include NFC...

[From Schmidt: Android]

There’s still a long way to go in the mass market though, and it’s fair enough to comment on it. Consumers, journalists, commentators don’t yet understand how this new infrastructure is going to work.

But I think that’s about to change. Britain’s biggest retailer is Tesco, so they are a benchmark for the acceptance of new technology, and they are going to go contactless this year.

Tony Saunders is the director of marketing for VeriFone in Europe, the Middle East and Africa... Saunders told us that within six months, Tesco will be rolling out near-field communications capabilities to its 35 - 38,000 checkouts across Britain.

[From The future of the high street: near-field communication (Wired UK)]

This might be connected with a story that I touched on before in another context, illustrating the point about the ability of retailers to exploit the new contactless technologies in interesting ways.

Tesco will relaunch its Clubcard scheme as an online rewards programme as it gears up to reach customers in the digital age. Developing a ‘secure, multichannel’ smart card, the UK retailer will move the scheme to digital channels in an effort to simplify its rewards programme and cut down on direct-mail costs.

[From Tesco will relaunch Clubcard scheme in 2011 : WCJB]

Incidentally, I didn’t quite understand the rest of the Wired story, so I dropped an e-mail full of NFC articles to the reporter who had said that:

The only obstacle could be similar, but proprietary, technologies set up by banks—which are known as “contactless” payment options. Barclays’ contactless cards are a good example, as are Visa’s PayWave cards, which are being trialled in Europe using an iPhone dongle.

[From The future of the high street: near-field communication (Wired UK)]
I shouldn’t make fun. The technology might be old to us, but it’s new to the mass market. And I should not that it isn’t just UK journalists who get a bit confused.

For example, special payment stickers are available already that allow merchants to NFC-enable their point of sale terminals by simply affixing a sticker to the terminal, Litan said. Such stickers go for as little as $18

[From Analysts: Apple]

Wait, what? I think the journalist got the wrong end of the stick on this one! Let’s be clear. The contactless payment schemes are NFC and the cards, phones, stickers, watches, hat, badges or anything else will all work with the NFC POS terminals. The key point here is that the retailers are rolling out NFC at POS not just because they want to accept NFC contactless cards, which many of them don’t really care about, but because of NFC contactless phones, which promise an entirely new mobile shopping experience. The retailers want mobile wallets as soon as they are practical, because the value-adding opportunities around coupons, loyalty, location-based marketing and all sorts of other things besides payments are so great.

You’ve got to pick a pocket or two, boys - 21/09/2011

I don't understand why the London Assembly Transport Committee were questioning Forum friend Will Judge from Transport for London (TfL) about the security of contactless payment cards, since the security of those cards is the concern of the banks that issue them, not the merchants who use them, whether Tesco or TfL. But whatever.

Giving evidence to the London assembly transport committee about TfL's plans to introduce contactless payment to London's transport network, he answered yes when asked by a member of the committee whether the system was "100% safe" against "invisible pick pocketing".

[From Transport for London says new contactless]

Will is, naturally, correct. If I am able to sneak a bogus reader onto the Underground and surreptitiously hold it against people's pockets to read the card data inside, it's not much of a crime. I have to put the reader up against your wallet. If I want to read your card from the other side of the carriage, I need an antenna the size of a wagon wheel pumping out so much power that the coins in commuters’ pockets would be sparking.
Tomorrow’s Transactions—The Transit Reader

But even if I can access the card in your pocket, I can't use the data to make counterfeit cards and I can only put spurious transactions through to a merchant account at a bank: I can't "pickpocket" anything, in the sense that I can steal anything of any value. But it seems to me that electronic pickpocketing meme is unstoppable.

An ongoing effort by credit card companies to issue 1 billion radio frequency identification chip-enabled contactless cards by 2016 will dramatically increase the public's susceptibility to identity and financial theft from electronic pickpocketing, Identity Stronghold announced today.

[From ‘Electronic Pickpocketing’ Threat Worsened by Credit Card Industry Plan to Issue 1 Billion Contactless Payment Cards, According to Identity Stronghold - pymnts.com]

Now, I have to say, in all honesty, that I know of no report from a reputable source of any incident of electronic pickpocketing ever having taken place anywhere in the world. Not one. I have never seen an unauthorised charge on any of my contactless cards and if I did see one I would simply call my issuer and have it wiped.

The real question, of course, is security: If a special little reader can take and use your credit card data from your phone, how is Google going to ensure this only happens when you want it to happen?

[From ComputerWorld]

This is a misunderstanding of the difference between stripe cards and chip card (whether contactless or otherwise). We wrote an Android app to use a Square to read the magnetic stripe data from a credit card, decode it and then send it on. But the problem here is not Square or Android or Twitter but the magnetic stripe. If you read a magnetic stripe, you have all the data you need to make a magnetic stripe transaction. But if you read a contactless card, you do not have all the information you need to make a contactless card transaction.

Contactless card and phones, the ones with NFC interfaces like the Google phone referred to above, don't send the data necessary to construct a bogus magnetic stripe and you can't use the data that they do send to make a bogus NFC application because the secret keys that you need to create the secure messages are never transmitted - they stay inside the secure element (SE), just as they stay inside the chip on a chip and PIN card. So the strength of the electronic pickpocketing meme does not come from the technology, nor can it come from experience.
As I've said before about contactless, there must be something about contactless, about wireless interaction, that causes irrational concerns.

*Among those that are not yet ready to use contactless, security appear to be the dominant consideration. Which means, of course, that whatever we might think about actual security situation we must get better at communicating it.*

*[From Digital Money: Contactless update]*

I'm at a loss what to do though. If I were the UK banks, I might try to persuade the BBC to get a contactless card story into Eastenders, as that seems to be the standard public education channel these days. Otherwise the stories will just keep coming.

*At least once a year, the contactless payments industry, indeed all of us, has to put up with someone spreading fear about contactless cards and the ability of someone to scan the card of a passerby with a portable contactless reader. Yes, it's true. It can be done. But who cares? The risk is beyond minuscule.*

*[From PaymentsJournal - Non-Existent Monsters in Your Wallet]*

If the London Assembly were being really forward looking, they would have asked Will what terrific new services TfL will be able to deliver once customers begin using the coming generation of NFC phones instead of contactless cards. This is only just around the corner now.

"*Until we see implementations of NFC that allows us to get repeatable transaction times within 500 milliseconds, this is going to be a concern for us,"* Will Judge, Transport for London head of future ticketing, told NFC Times.

*[From Transport for London Calls for Faster NFC SIMs | NFC Times – Near Field Communication and all contactless]*

He also said, at the Transport Card Forum in London in December, that some "very clever people down in Guildford" are going to make this happen. Modesty forbids me from providing a link to these transaction heroes; suffice to say that I fully expect the targets for TfL's Future Ticketing Project (FTP) to be met.

**Slick transit - 25/10/2011**

Today is a rather special anniversary. A hundred years ago today, the London General Omnibus Company (LGOC, a precursor of London
Tomorrow’s Transactions—The Transit Reader

Transport) took the last horse-drawn bus out of service in London. The motor had won.

The last LGOC horse-drawn bus ran on 25 October 1911.

[From Buses in London - Wikipedia, the free encyclopedia]

When engines were first introduced, there was an explosion of variety. Steam, electric, hybrid (yes, one of the first motorised London buses used a generator to power an electric motor - I'm told this was to avoid using gears, which the drivers didn't understand having come straight from horses) and petrol. The first buses merely replaced the horses with an engine, but they didn't redesign the rest of the bus.

It takes a while for a new technology that improves on one part of a system to embed in a redesigned system. It's a well-known phenomenon that the first electric motors were used to replace steam engines, and it took a while for factories to be redesigned so that there were lots of motors where they were needed rather than a big motor in the middle transmitting power via belts and drives. When the modern ‘one man’ buses were first introduced, there was a similar dynamic. The buses were fitted with turnstiles and machines that you had to drop money into in order to get a paper ticket, just as you would have done with the human conductor.

Things stayed this way -- handing over cash to get a paper ticket -- until the contactless smart card came along (although magnetic stripe tickets were introduced on the tube starting in 1964). When the first smart cards with contactless interfaces arrived in London, the Oyster cards, they were used to simulate the complex cardboard tickets: weekly and monthly tickets, annual season tickets, staff passes, children and old person’s concessions and so on. The real revolution arrived a little later, when they began the capping system so that you could ride around on your pay-as-you-go (PAYG) Oyster card but your charges would be capped at the cost of a one-day travel card. Now, to all intents and purposes, everyone in London has an Oyster card.

TfL spent a lot of money developing the Oyster scheme because one thing hadn't changed from the days of the horse-drawn LCOG buses to today: the banks didn't provide a payment mechanism that was quick enough and convenient enough for public transport, so the public transport operators had to sort things out from themselves. Well, now they do. Since the banks decided to roll out contactless payments, TfL have decided to institute a major programme to accept these bank products for travel in London. Starting next year with the buses, TfL are rolling out new readers so that customers will be able to use their bank cards to travel. No need to buy an Oyster card any more.
Contactless credit and debit card payment will be rolled out across the London transport network by the end of 2012, making the capital the first in the world to embrace the system so comprehensively.

[From TfL]

At Consult Hyperion's recent workshop on Open Payments in Transport, Matthew Hudson from TfL explained to the delegates why TfL is moving to accept these ‘open’ (i.e. Visa, MasterCard and Amex) contactless payment cards on the buses and tube starting next year. Given the thousands of acceptance points, millions of users and zillions of transactions this will involve, it's quite a big deal in our neck of the secure electronic transactions woods. Nick Deere from Consult Hyperion explained how the system will work and the complexity of the reader development.

The Tri-Reader® 3 supports multiple card schemes – for example, with Oyster in the UK, ITSO and contactless EMV cards can now be read concurrently on the same contactless reader. The Tri-Reader 3 was developed by Cubic on behalf of Transport for London and the company has a worldwide licence for its use for open payments.

[From Cubic receives contactless]

Oyster is a fantastic product and has been a huge success. But Oyster costs money to run and TfL is under significant pressure to reduce costs. As Forum friend Shashi Verma (TfL's Director, Customer Experience), has frequently observed about this before, they see they their job as running a transit system, not a ticketing system. TfL reckon that their overall ticketing system costs them about 14p per £1 collected in fares. Some of this is ripe for reinvention. Product sales alone account for almost a third of costs, and this could easily be halved: monthly and yearly season tickets won't go away for a long time, and since they are efficient products to sell, there's no reason to stop them, but most of the ad hoc non-commuter trips could be shifted to open products. According to a leaked document quoted in last night's Evening Standard.

The move would mean mass ticket office closures and the loss of more than 1,500 jobs. The Operational Strategy Discussion Paper says £2 billion could be saved by 2018.

[From Driverless trains on the Tube by 2021 | News]

That's serious money and an obvious driver for change in the ticketing system. There's another issue as well. While Oyster is a great customer
experience that is much appreciated in London, it's not a perfect customer experience. Just to give one example: because the data is stored on the card, it's difficult to give consumers a good customer experience online. With the shift toward multi-channel sales and servicing underway, this is now important.

As I'm sure many of you know, Consult Hyperion has been advising TfL on this project for some time so we share their excitement about it going live in the not-too-distant future. The experience that we have gained in the prototyping, design and certification of card and phone EMV products in a demanding transit environment is literally unique, so we are hardly impartial observers. But I'm sure you'll agree that TfL's decision to set a high bar in terms of functionality and performance has paid off for them and for the industry as a whole.

While I appreciate the history of transport in London, I'm looking toward the future. Another change that will come with open payments is the arrival of mobile payments and ticketing. Since the gates will accept bank contactless card they will also accept Visa, MasterCard and Amex payments via mobile phone and that opens up the potential for value-adding services on the mobile that are simply not possible using cards.

*Transport for London (TfL) has stated it will support NFC payments on mobile phones in 2012.*

*[From Transport for London to accept NFC payments from 2012 • NFC World]*

It's a big deal. It's not been possible to experiment with Oyster in mobile phones because the chipsets used for NFC do not (yet) support the more secure Oyster cards and the software emulations are too slow for practical use. By going down this route, TfL can avoid this problem completely and start to explore the next smart ticketing revolution, which will be integration of ticketing and mobiles.

**Back to transit - 11/01/2012**

When I went to get on the SF Muni the last time I was in San Francisco, I realised that my Clipper card had only a few dollars left, so I decided to top it up. I went to the BART top-up machine. It said that it accepted debit cards only, so being half-asleep (it was very early in the morning) I put my Barclays debit card in the slot. Transaction declined. Then I realised that they meant ‘debit’ in the American sense of non-Visa/MC scheme debit that has a PIN. I didn't have any cash, so I gave up. But as I was walking to the Muni gate I saw another Muni machine that clearly said credit or debit top up. So I tapped my Clipper, selected the $20 top-up, and inserted
my Barclays debit card again, this time selecting ‘credit’ as the payment option. It worked. But then I realised that I hadn't got a $20 top-up, but 10 $2 Muni rides, no good for my ride on Caltrain later. If anyone asks you why we want to use the mobile phone to replace cards when the current system works fine, tell them they're full of it.

What I should be able to do in a civilised society is to not have to care about any of this stuff. I should be able to get off the plane at SFO and walk on to BART by just tapping my phone. There are two ways to do this: load the transit applications into the phone, or get the transit system to accept ‘open’ payment cards (the London solution). I have got a Samsung NFC phone, but sadly there's no way to load a Clipper card into it, because Clipper uses DESFire and the phone NFC chipset doesn't support this in hardware. At some point, I suppose, Clipper will have to upgrade to DESFire EV1 (not implemented in phone chipset either) because DESFire is compromised, but I don't think that will be any time soon. Why will they have to upgrade? It's because of security: you can clone certain kinds of MiFare cards because they rely on a proprietary security algorithm that was broken some time ago.

_The case came to light when a counter worker at an unnamed railway station reported selling 100 cards to the same person, Nos says. Further investigation showed the cards were being manipulated so that they appear to have been uploaded with €150 in cash. The cards are then sold on to third parties via Internet sites such as Marktplaats._

[From DutchNews.nl - Public transport smart card fraud]

Oops. Oh well, this doesn't mean you have to panic, abandon the current system and buy a new one immediately. It's about risk management.

_BART says there aren't enough Clipper smart-card transit cheats to warrant card changes. The San Francisco Chronicle says there's been a surge in the number of riders misusing Clipper cards, but officials decided Thursday that the number of cheaters hasn't risen to a level that makes changes to the card necessary. Up to 200 commuters may be cheating the system each day._

[From BART says not enough smart-card cheats for fix]

Transit is actually a very interesting to study when trying to understand the implications of the new network technologies on various stakeholders. For one thing, people in many cities never leave home without a transit card, so it's an obvious focus for those trying to introduce new payment technologies.
Tomorrow’s Transactions—The Transit Reader

Take the specific example of the ‘hacking’ of transit cards. It's not worth spending very large amounts of money on security for transit cards that have to cost very little in order to pay for transit fares that are even less. But if someone else has put a high-security system in place, then you might as well use it for transit: then the payment/ticketing security burden is at least shared and in some cases eradicated. Does transit then define the path for mobile contactless because it provides a clear win-win? Yes and no.

My prediction? ISIS and MNO initiatives will be successful in Transit. Retailers will migrate to a new commerce network that steers clear of Visa and MA.

[From NFC – Announcements Galore ! « FinVentures]

This is a very interesting prediction. In the short term, transit is central to many markets but, as I wrote recently, there is every reason to imagine that the retailers, rather than MNOs or transit operators, will shape the longer-term evolution in the space, but we'll return to that another time.

Beyond the leather - 07/03/2012

A typically excellent piece by Karen Webster over at pymnts.com surveys the mobile wallet landscape. She concludes by suggesting that consolidation is inevitable.

But I am going to lay down a wager that consumers will have only a handful of icons on their phones that connect to a single-tender type (payment app) or a wallet (multi tender types) and that merchants accept payment with mobile only for a few of these icons.

[From Commentary - Karen Webster Sizes Up the Rapidly Changing World of Mobile Payments | PYMNTS.com]

I'm sure she's right. I might be tempted to further and say that they will only have one mobile wallet. Personally, I can't wait. The idea of taking all of your payment cards, loyalty cards, money, ID documents and such like and chucking them all into some sort of mobile wallet in your handy device-formerly-known-as-the-mobile-phone is most appealing. Indeed, as Karen notes, mobile wallets are all the rage at the moment. Visa has one called ‘V.Me’. Google has one. The US telcos have got together with some of the card issuers there to make ‘Isis’. Square has its ‘CardCase’. And there's an elephant in the room yet to declare...
Since 2010, Apple has filed a series of so-called "iWallet" patents that deal with mobile device payments including NFC systems that are linked to credit and debit accounts.

[From Apple nabs parental controls patent for 'iWallet' transactions]

Now we read that, dissatisfied by the choices available to them from payment companies, technology companies and software companies, the major US retailers, Wal-Mart and Target included, are going to band together and make their own mobile wallet.

At a strategic level, this is about more than sticking more coupons in a wallet to provide some value-added services around payment instruments. To the retailers, the payments themselves are a problem. When you hear people in the payments industry asking questions like "why bother with [insert new technology/product/service here] because cards work and everyone's happy?" you know they haven't looked at the big picture. Not everyone is content with the status quo.

Right now, Google’s Wallet, ISIS and Visa’s V.me are all about taking existing plastic cards and using virtual versions of them, but this must surely be only a stepping stone to new retail payment instruments.

[From Ordinary people]

While it's a digression here, I have written before (more than once) that much of the analysis that we have done in this space, going back some years, has flagged the development of new retailer-centric instruments as a more-likely-than-not development, an opinion that has been reinforced by the successes of, and lessons learned from, the Starbucks mobile solution.

I’ve suggested that a plausible, logical step for retailers will be to abandon the antiquated infrastructure of payment cards—issuing and acceptance, interchange and rules—for new, retail-centric payment mechanisms.

[From Retail and the long game]

Meanwhile, in the UK, Visa Europe has invested in the Monitise/Carphone Warehouse joint venture to bring the SimplyTap service to the high street, hoping to provide a wallet service that is attractive to retailers here. Not wallet wars, exactly, but as I wrote before, certainly skirmishes. I have to say that my personal, early experiences with the rudimentary UK mobile wallet in my Orange phone (which has a prepaid Barclaycard MasterCard and a contactless interface) have been positive: it's fun being able buy a coffee by tapping my phone instead of getting a card out and I have already (on more than one occasion) lived the dream of the marketing
people by leaving home without my wallet but with my phone. I've found that the use of the prepaid card works very well in this context. Prepaid cards might be a bit of a pain, but prepaid cards in a mobile wallet are not: you can see what your balance is and top it up while walking down the street.

Fun and mildly convenient... probably not enough to set the world on fire. Karen says that she doesn't know who will win the wallet wars and I don't either, but I think I do have some clues as to the winning proposition. The winning mobile wallet won't be an electronic emulation of a mundane wallet. The mobile wallet won't be a virtual reality version of a leather wallet. It will be a hyper-reality version of a wallet: not an electronic version of a wallet as it is, but an electronic realisation of what a wallet should be. At the Mobile World Congress in Barcelona, Alberto Jiménez from Citi called this "going beyond the leather", which I thought was a terrific description. But what does he mean? How will the wallet in your mobile phone differ from the wallet in your pocket? There are probably three main differences.

First of all, if you lose your mobile wallet, it doesn’t matter in the same way that losing a real wallet does. If you lose that, it’s gone. But if you lose your mobile wallet, then it can be tracked, traced, monitored and turned off. You can go and get another phone and in a few minutes have your wallet restored, automagically via the airwaves. And your phone can be locked, with a PIN today but with your fingerprint or voice in the future. So the m-wallet is more secure than the wallet.

Secondly, your mobile wallet understands context. It knows where you are and what you are doing. If you open your mobile wallet in Tesco, it won’t bother showing you your Waitrose loyalty card. If you’re in W.H. Smith and you have W.H. Smith coupon in your wallet, it will apply it automatically for you at point of sale. Your mobile wallet might contain thousands of loyalty cards, store cards, coupons, targeted offers, digital receipts, alerts and so on, unimaginable with the bulging leather version jammed into my back pocket. So the m-wallet is smarter than the wallet.

Finally, your mobile wallet is connected. This is where I expect to see the unexpected consequences of innovation! I’ve no idea what will happen when my wallet becomes connected to Facebook, Twitter and Foursquare -- although some of Amex's recent announcements provide some interesting pointers -- but I can imagine life getting very interesting! I'll post some more about the ‘social wallet’ in the future. So the m-wallet has more friends than the wallet.

All of these things together are why I feel that the mobile wallet mania is not only justified but may be a rare case of under-hyping! The history of mobile to date is one of explosive growth, rapid adoption and sweeping
change. The secure, smart, connected mobile wallet will bring genuinely new functionality and business models that are very different from the business models around payment cards today.

London buses show us the way – 7/10/2012

The Mayor of London, Boris Johnson, has been talking about the next major revolution to come in London transit ticketing.

Public transport travellers will be able to swipe credit or debit cards in the same way as Oyster cards by 2012, Boris Johnson revealed. The Mayor said the phased scheme will start on buses in the run-up to the Olympics and then move on to the Tube. Prices will be the same as with Oyster. Mr Johnson has also pledged that a "next generation" Oyster card will be released by 2014.

[From Commuters will soon be able to use credit cards like Oyster by 2012 | News]

What this all means is that visitors to London -- and, indeed, Londoners -- will no longer need to get prepaid Oyster cards. They will be able to use their bank cards (such as, for example, the one of the ten million cards that Barclays has already issued with contactless interfaces) to tap-and-go their way around town.

Another option might be to use Oyster cards in shops. It does seem odd to me that when I'm on an Underground platform and dying of thirst, the Coke machine doesn't take the one currency that every single person on the platform actually has: Oyster. In other regions, this is seen as being a natural development of widespread mass transit contactless systems. Taiwan is following Hong Kong and Singapore in allowing the transit e-purse to be extended out into retail.

The EasyCard, a contactless smartcard system for use on the Taipei MRT system, will soon become an electronic purse that can be used to purchase small-value items... The new payment system, which will allow up to NT$10,000 (US$312.50) to be stored in the card, will be put in place a year after the Legislative Yuan passed an amendment to the Act Governing the Issuance of Electronic Stored Value Cards that paved the way for the new payment vehicle.

[From Electronic purse expected to become operational in March - Taiwan News Online]

It's clear that, as we all know, transit is the vanguard for electronic money and therefore it provides a unique opportunity to drive cashlessness. But that doesn't necessarily mean that transport operators should get in to retail payments: the alternative path is to let retail payments systems operate in
transport. This is the path that London has chosen, as noted above, and is true in many cities around the world. Transit operators see ticketing as not part of their core business, which is running public transport. If other people can provide the ticketing solution, then fine.

*Toronto transit officials are not the only ones keen to get out of the business of collecting fares and phase out closed payment schemes. Their counterparts in London, New York, Chicago and some other cities are moving at varying speeds toward open-loop payment.*

[From Canadian Transit Card Operator: Not So Fast to Open-Loop Payment | NFC Times – Near Field Communication and all contactless technology.]

There's another reason, though, why I think that this trend is gathering momentum. It costs money to stay in the security arms race: the ticketing systems (especially as they move into the world of mobile phones) need to be sure that the activities of fraudsters do not impact revenue. When the transport operator has to spend money on continually upgrading and enhancing systems for revenue protection purposes, that's money that could be better spent. It's not always about counterfeiters and criminals, by the way, sometimes it's just people gaming the system.

*Determined token hoarders will have to buy their tokens one by one, at token vending machines, and that's not the only step the Toronto transit bosses are taking to fight stockpiling. The Toronto Transit Commission (TTC) has now introduced adult paper tickets with an expiry date on them. “The TTC won this,” said Angela Leung, an Ontario College of Art and Design student who amassed over 100 tokens during the 2007 fare increase and had the same game plan for the new year.*

[From Excalibur Web edition - Extinct bus tickets temporarily reappear to combat token hoarders]

If payment systems spend the money to develop fast, secure new payment mechanisms (using contactless cards, phones, stickers and who knows what else) then the transit operator doesn't have to.

**You wait ages for a contactless terminal then 8,500 turn up at once - 13/12/2012**

An e-letter arrives from forum friend Shashi Verma, Director of Customer Experience at Transport for London (TfL) and an all-round jolly nice chap. He says...
I am writing to let you know that we are introducing contactless payment tomorrow (i.e. today, Ed.); this will initially be available on any of London’s 8,500 buses.

[From TFL - Service Changes]

Hurrah! This has been long awaited by many in the contactless community, because the relationship between wallet or phone or card and mass transit is well-understood to be central to nudging consumer behaviour. There are a great many people (millions) in London who have a contactless bank card but have no idea what it is or how to use it. Hopefully, they will see other people using bank cards on yellow buttons on public transport and be encouraged to try it for themselves.

Yes, the buses have been fitted with the new ‘open loop’ payment terminals. This means that customers will no longer have to buy an Oyster card for travel but can simply use their shiny new contactless bank cards. When I was chatting to someone about this yesterday, their first question was "why bother - Oyster works fine" and indeed it does, but...

TfL reckon that their overall ticketing system costs them about 14p per £1 collected in fares. Some of this is ripe for reinvention. Product sales alone account for almost a third of costs, and this could easily be halved: monthly and yearly season tickets won't go away for a long time, and since they are efficient products to sell, there's no reason to stop them, but most of the ad hoc non-commuter trips could be shifted to open products.

[From Slick transit]

It cost a lot of money to upgrade TfL’s infrastructure and all of the readers at something like 20,000+ gates, but it will save them money in the long term. And what's more, foreign visitors with contactless bank cards will be able to jump straight on a bus without having to get into gigantic queues at Paddington or Victoria to buy and load Oyster cards. And never ones to take corporate PR as a substitute for reality, on your behalf we ventured into the freezing London morning to check it out.

We're very excited about this because it is a project that Consult Hyperion has been involved in from the very beginning, when we were selected by TfL as their consultants for this project. As well as helping with the analysis and specification of the new system, Consult Hyperion also developed the prototype contactless terminal for TfL to experiment with (we're a little different from other consultancies because we have a full-time, in-house development team that builds prototypes and proofs-of-concept for clients.
Tomorrow’s Transactions—The Transit Reader

In addition to upgrading thousands of readers around the system, TfL have developed a sophisticated back-office system to manage the mixture of closed-loop and open-loop payments and are now offering that system to other transport operators in the UK. This means that in time, ticketing may earn some money for TfL as well as reducing its costs.

The second question I was asked, and I won't shy away from it here, was "great, I'll be able to use my phone to jump on the bus". Unfortunately, for reasons that are too technical (and too boring) to go into here, the only NFC/card handset combo on sale in the UK today, the Orange Galaxy S3 QuickTap, doesn't work with the TfL bus readers. So if you want to amaze your friends (or are too lazy to get out a wallet) and jump on a double-decker using a flick of your smartphone, you’re better off getting yourself a Barclaycard PayTag and sticking it on the back.

To make the simple tap-and-go work for millions of consumers taking millions of bus rides, reliably and securely, is very complicated. To hide all of the complexity from consumers and make the tap work in a few hundred milliseconds was a tall order. But they've done it, so well done TfL.

Real data on contactless EMV in transit - 30/01/2013

At the excellent, and well-attended, Transport Ticketing 2013 event in London I saw a terrific presentation from John Hill of CUBIC reporting some early data from Transport for London (TfL's) migration to open-loop payments. In the first instance, as you will recall, TfL began to accept contactless EMV cards on the buses and later this year they will begin to accept contactless EMV cards on the underground as well.

John was kind enough to share the detailed transaction timing data that we (i.e., Consult Hyperion) had previously seen as part of our work on the Future Ticketing Project (FTP) but were not able to share before it was made public. I've included John's slide below with the kind permission of TfL. What this data shows is that the mean transaction time for bus taps is around 530ms. Of this 530ms, around 100ms goes on the terminal polling to determine which Oyster, ITSO (the UK's national standard for contactless ticketing) and open-loop (EMV) products are on the customer's card, so when you take this into account with some other overheads, it looks as if the overwhelming majority of contactless EMV transactions are taking 400ms. This is slower than Oyster (which takes about 350ms) but not a big deal. As John mentioned in his presentation, we are working with CUBIC and TfL to find ways to reduce the transaction times further so that 100ms polling is in our sights right now. Anyway, here is the key slide:
In addition to the 545ms mode peak, John's figures clearly showed much smaller peaks at 420ms and 490ms as well as a long tail out over 900ms! This is clear evidence that different card families and form factors (i.e. dual-interface vs. tags) take different times to process the transactions and that the fastest cards (at around 420ms) are twice as fast as the slowest cards. This is an unexpectedly wide variation. John politely resisted my calls from the floor for him to name and shame (!), but it boils down to this down: the fastest EMV cards are executing the transactions faster than the new Oyster card, but the majority of EMV cards are slower.

Another early learning from the TfL migration was put forward by Nick Mackie from Visa Europe in the panel (on open-loop migration in Europe) that I chaired at the event. As Nick pointed out, there's been a problem with 'collisions'. What this means is that customers who are used to waving a wallet or a purse or a pocket that has an Oyster card in it, they are now waving a wallet or a purse or a pocket that has both an Oyster and one of more contactless EMV cards in it. When the terminals see multiple cards, they (as currently configured) do nothing. There are currently far too many collisions being reported, so there's a customer education issue here. Retailers (including transit operators) have to explain to people that if they present multiple valid cards, then nothing will happen (yet another reason for moving to mobile, where Nick pointed out that Barclaycard have "hundreds of thousands" of PayTag stickers out there and customers like them).

And here's some more hard data from the event that might be useful: there are currently 9,000 open-loop transactions per day on the bus. This is a tiny fraction of the 6.3m transactions per day, but it is growing at 2% per
 Tomorrow’s Transactions—The Transit Reader

annum. People seem to like it (a friend visiting from Scotland e-mailed me last weekend to say how great it was to be able just use her Barclays debit card while visiting instead of buying an Oyster card). It's a good start.

Why does all this matter? Well, it's because the transit experience, in many markets, is disproportionately important to the contactless trajectory. I'm might only use my contactless card twice per day on the bus, but because I use it on the bus it becomes the card in my back pocket and I might then use it to buy coffee and lunch with contactless as well.

In any case, transit is one of the rare use cases where NFC payments add some real value to the user experience simply because it is more convenient to tap your phone as you rush through the rail gate or board the city bus rather than fumbling to find a contactless bank card or transit smart card.

[From NFC - Yes, NFC, That Speeding Train is Headed Your Way | PYMNTS.com]

Incidentally, while much of the talk yesterday was about the shift to open-loop in transit, that's not the only model. There is indeed a completely opposite roadmap, whereby the contactless cards used for transit have such high penetration and are so well-established that it makes sense to use them instead of bank cards. Look at the Asia-Pacific region. Taiwan is following Hong Kong and Singapore in allowing the transit e-purse to be extended out into retail.

The EasyCard, a contactless smartcard system for use on the Taipei MRT system, will soon become an electronic purse that can be used to purchase small-value items... The new payment system, which will allow up to NT$10,000 (US$312.50) to be stored in the card, will be put in place a year after the Legislative Yuan passed an amendment to the Act Governing the Issuance of Electronic Stored Value Cards that paved the way for the new payment vehicle.

[From Electronic purse expected to become operational in March - Taiwan News Online]

It's clear that, as we all know, transit is mass market, technically challenging, high profile, important and demanding. It's at the intersection of NFC, mobile, payments and (soon) big data. I love it.
Chapter 3: Articles about transit ticketing

A step forward?

[March 2012] Public transport ticketing needs to take a step forward, not back, says John Elliott, Head of Public Sector Practice at Consult Hyperion

Earlier this month, the Transport Secretary, the Rt. Hon Justine Greening MP, expressed her view that the Government and the rail industry can – and must – do more for passengers and for taxpayers. Her goal for this sector, outlined in a paper entitled ‘Reforming our Railways: Putting the Customer First’, goes on to state her commitment to building on recent efficiency gains in order to improve the performance of the industry, as well as the passenger experience.

As part of this vision, the Government has announced plans to expand existing “smart ticketing” schemes like London’s Oyster card by rolling out smartcards across both England and Wales, and across different operators.

Although this may sound like progress, this may actually be a step backwards for both operators and passengers. London’s Oyster scheme has undoubtedly been a success, but a great deal of technical and commercial progress has been made in the development of payment systems since 2003.

Standards for electronic payment/ticketing schemes currently fall into two categories: either proprietary or open. Proprietary products such as Oyster were specifically developed for the transport environment, offering fast throughput and an all-in-one media to meet the needs of multi-modal operators. These standards can be specific and tailored, as they do not have to conform to any interoperability requirements.

By comparison, open standards such as ITSO and EMV (Europay, Mastercard, Visa) are designed for national or global acceptance. Each is primarily designed for a target environment – ITSO for transport and EMV for payments – but both could be used to cross the boundary. As such, open payment systems offer the prospect of using contactless bank cards and new media for transport ticketing in place of dedicated smart cards like Oyster.

This widespread acceptance of contactless debit and credit cards for travel in the UK would help to reduce the production and distribution costs connected with traditional paper-based and smart card ticketing channels.
Unlike proprietary systems, these open standards offer operators benefits that include greater interoperability, low issuance and improved security. In addition, this type of open payment model could reduce costs through the use of off-the-shelf equipment from a range of suppliers, rather than bespoke equipment made to proprietary specifications.

The opportunity to use contactless debit and credit cards in this way will also offer much greater convenience for passengers, since they’ll be able to use a card that they already have, instead of having to carry and top-up an Oyster card, and will not need to take any action before they travel. As such, visitors arriving in the UK with their contactless bank card would no longer need to queue up to buy an Oyster card or top-up their Oyster card in order to use public transport.

The major payment schemes are already working on producing a dedicated data area on bank cards that will allow operators to record tap data which could be used for other payment models and revenue inspection, so all of these benefits of a smart card system can be retained, including the significant operational, cost-saving and security benefits associated with reduced cash-handling costs.

However, the major shift is away from smart-card based systems (ITSO, Oyster) designed in the 1990s to modern account-based systems (held in the back office) which use ‘smart tokens’ to identify which account to use to pay. In the future we could see any smart token being used to authenticate (payment card, Oyster card, ITSO card).

In the not too distant future, NFC mobile phones will also be used to pay for travel or store transport tickets in a similar way, using the same contactless technology as Oyster, but as part of an open, rather than proprietary, system. This is just shifting the smart token inside the mobile phone and taking advantage of its Internet access to provide other channels for purchases and account top-ups. Near Field Communications (NFC) is a short-range, high frequency wireless communication technology that enables the exchange of data between devices that are close to each other.

We predict that more NFC-enabled smartphones will be being issued than non NFC-enabled devices by 2013. The ultimate “tipping point” for mobile contactless transactions is expected to be around 2015, however, as this is the date by which the combination of NFC-enabled smartphones, contactless and mobile POS and “mobile wallet” applications will drive the rapid growth in the number of mobile contactless transactions.

Technological developments like these will continue to drive progress in this area, providing much greater flexibility as well as broader social inclusion, thanks to the strategic collaboration between some of the
world's leading mobile technology developers, smart card manufacturers, service providers, and standards bodies. As such, by pursuing open – rather than closed – payment systems to achieve these goals, it will be possible to make public transport more convenient for passengers, and also less costly for operators.

A Touchy Subject

[June 2012] There are increasingly frequent claims that contactless smart payment cards are insecure because they can be read while in your wallet or pocket. Can this really be true? And if so, is this threat really any greater to consumers than what already exists? **John Elliott** investigates.

One of the most exciting new developments in payment technology has come in the form of “contactless” payments, the name given to payment card transactions that require no physical connection between the customer’s credit card and the merchant’s sales terminal. Instead, customers simply tap their card against a contactless card reader to make a purchase. Today, rather than only being used to buy fast food and transport ticketing, these cards are now also starting to be accepted in book shops and stationers. Latest figures from UK Cards indicate that, in the UK, there are currently more than 20 million contactless credit or debit cards issued and 80 thousand readers where they can be used at merchants.

HSBC has been the latest bank to announce that it will start replacing customer debit cards with contactless cards¹. But, interestingly, they are allowing customers to opt out if they would rather not have the new contactless technology in their wallets. Of course, we can only speculate whether this decision has been taken because stories continue to circulate about these cards being unsafe - and HSBC wants to afford its customers peace of mind. But, what’s more likely is that it’s simply due to the fact that the contactless ecosystem is still in its infancy, so many HSBC customers might not benefit from having these cards in their wallets just yet, so the Bank is choosing to give its customers more choice. However, this investigation is not looking at the merits of contactless payments versus cash payments, or contactless versus Chip & PIN. The aim of this paper is to take a detailed look at the technology itself, and to establish whether the threat of ‘Snooping’/‘Sniffing’ (where it’s claimed certain card details can be read ‘over the air’ by fraudsters), is a major concern for consumers and to see what the risks are, if it’s true.

¹ [http://www.guardian.co.uk/money/2012/may/09/hsbc-joins-contactless-payments-movement](http://www.guardian.co.uk/money/2012/may/09/hsbc-joins-contactless-payments-movement)
A new industry created from fear
Ever since the banks and the financial services industry started rolling out contactless payment cards, and merchants adopted contactless payment terminals, a new security industry has grown warning us of the threat of having your card data read. In fact, you’ve probably seen the articles or YouTube videos that claim that your new contactless payment card details can be read by an attacker while your card is in your pocket, perhaps closely followed by a sales pitch for some sort of foil sleeve which can prevent your card from being read\(^2\). So as part of this investigation I thought it would be interesting to see exactly what information can be read from these cards, what kinds of fraud an attacker might conduct with it, and how these risks of contactless data loss compares with if your card were stolen or cloned.

Attacker home-made terminal can read some data from your payment card in your pocket

What can be read?

When a card conducts a transaction with a card reader, the reader is the master and the card is the slave. So, to some extent, the card will do what it is told, and this involves giving up some information about the card. The necessary specifications are easily obtained and the kit is cheap, so it is not hard to make your own contactless payment card reader to obtain the free-read data from all contactless cards to which you can get close enough (less than 10 cm is what the standard says, but attackers can increase the power of their reader and extend the range)\(^3\). The table below shows the information that can be read from the contactless chip, and compares it with related information that can also be read by visual inspection from the face of the card i.e. if you lost your card or it was stolen and used for fraud.


\(^3\) The ISO/IEC 14443 Proximity Card standard is used, the same as that used for many contactless transit cards.
<table>
<thead>
<tr>
<th>Data/information available on a bank card</th>
<th>Card face data (visually available)</th>
<th>Chip data available over the contactless interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Account Number (PAN).</strong> The long number across the middle of the card which identifies the issuing bank and the account which will be used to ultimately pay.</td>
<td>PAN</td>
<td>PAN</td>
</tr>
<tr>
<td><strong>The name of the cardholder</strong></td>
<td>Cardholder Name</td>
<td>Some early contactless cards do allow it to be read, but increasingly this is not the case.</td>
</tr>
<tr>
<td><strong>Expiry Date:</strong> The date after which the card is no longer valid.</td>
<td>Expiry date</td>
<td>Expiry date</td>
</tr>
<tr>
<td><strong>Security Code:</strong> A code which is not allowed to be stored by merchant systems but is used for ‘card not present’ (CNP) payment authorisation. Knowing this code is supposed to indicate that you are in possession of the card, rather than just having a copy of the card details from merchant records.</td>
<td>Security Code (going by various names such as CVV2 (Visa), CVC2 (MasterCard), 4BDC (Amex))</td>
<td>The security code printed on the card and used for card not present transactions is <strong>not</strong> available over the contactless interface.</td>
</tr>
</tbody>
</table>

Let’s look at each data element in turn:

**Cardholder Name**
The UK Cards Association recommends that cardholder name is not provided via the contactless interface. So, it should not be possible to be sniffed by our attacker with his homemade reader. Recently, it has been shown that some contactless payment cards in the field do allow the
Future Transactions—The Transit Reader

cardholder name to be read⁴. This will probably be prevented in the next generation of these cards, and other current cards already do not allow the cardholder name to be read. However, your name is written on the face of your card and so might be observed by someone each time you take out your card to use it, so can easily be obtained whether you’re paying via contactless, Chip & Pin or using the magstripe.

PAN
In contrast, the PAN can be read covertly from any contactless payment card while the card is in your pocket. The PAN is the long number, again also found on the card face and it is comprised of several components including numbers identifying your issuing bank, the bank product, your account within the bank and a check digit at the end so that a computer can tell if the PAN has been entered incorrectly when used online.

Expiry Date
The expiry date can be read, and is the same as the one printed on the face of the card.

Security Code
Finally, the security code printed on the cardface cannot be read over the contactless interface by an attacker. Associated with a payment card are several security codes, which are all different from each other. The idea is that they help show that the card is actually present at the time of a transaction:

- There is one printed on the card (usually on the back), sometimes called CVV2. This is the one that you should be asked for (last 3 digits) when you make a payment on the Internet or over the phone.
- There is one in the card magnetic stripe, sometimes called CVV. This is read when your card is swiped in a magnetic card reader and cannot be read from any other source. The idea here is to prevent a fraudster from making a magnetic stripe card clone of your card if they only collect your other card details from, say, an Internet merchant.
- There is one on the chip that is used on the contactless interface, sometimes called iCVV. If a fraudster reads your iCVV, they do not have your CVV2 or your CVV and so do not have enough information to successfully clone your chip data into a magnetic stripe card, or make an Internet or telephone payment, provided that the merchant follows the payment scheme rules and asks for the CVV2 when all purchases are made. More on this below.

⁴ http://www.theregister.co.uk/2012/03/29/visa_cards/
According to payment scheme rules, the merchant is not allowed to store any of these security codes with your other card details. If they break this rule, the payment schemes would investigate and could result in heavy fines and loss of the ability to accept payment cards.

So, how scary is that?
Well, the short answer is, that’s not very scary at all, for the cardholders, and the threat is much greater should you physically lose your card and a fraudster uses it, than if information was obtained over the contactless interface. But, let’s now look at a few frauds discussed in the press recently that attackers might want to try, and see whether they can do it with the data sniffed from your contactless payment card as easily as they can with physically having all your card data.

Privacy and identity threats
There are some people who don’t like their name being available from their payment cards in the same way that I don’t like my name and address being available from my UK Driving Licence. It can be argued that there is no need at all for cardholder name to be available from the face of the card. There might be a bright future where anonymity is preserved, but right now this is the way it is – as soon as you use your card (Chip & Pin or contactless), that information can be viewed by anyone who wants to look, cashier or fraudster. So, if you don’t want anyone to be able to read your name or your card number, then you should not use payment cards at all. Every time you do a Chip & PIN transaction, these are captured by the merchant. However, for contactless transactions, cardholder name is not used, so it could be argued that things are moving in the right direction with the introduction of this technology in helping to preserve identity.

Cloning your contactless payment card
This is perhaps the hardest attack to carry out because the attacker would need to know how to program a contactless chip (which is no mean feat) and would also need more data than he has obtained from reading your card. When the reader does a transaction with your card, the card chip is required to perform cryptographic operations that prove it has secret cryptographic keys that are only known to the card-issuing bank. For each transaction, the cryptographic calculation required by the terminal changes, based on transaction details, so it has to be calculated each and every time and cannot simply be stored in advance by an attacker.

Therefore, cloning your contactless card using only the details the attacker has sniffed from your contactless card is not possible. These are the same reasons that Chip & PIN cards cannot be cloned. The chip provides an extra level of difficulty for attackers.
Making a counterfeit magnetic stripe card with your details

Magnetic stripe cards use older technology that preceded chip payment cards like Chip & PIN and the new contactless payment cards. However, modern payment cards still have the magnetic stripe so that the cards can be used around the globe at merchants where chip card terminals don’t yet exist (e.g. much of the US). It is also there as a fall-back in case a chip-card terminal fails, so the card is swiped and your signature is provided as authentication.

If you have someone’s payment card, it is trivial to copy the magnetic stripe details and write them to another magnetic stripe card of your own before giving it back. This was a very common fraud before chip cards, known as skimming. However, the information needed to correctly populate a magnetic stripe requires more data than the attacker has managed to read from the contactless payment card in your pocket. In particular, the Security Code required to make the magnetic stripe data (CVV) is not readable. The iCVV held inside the chip card is different from the security code printed on the card face (CVV2) and different again from the one held in the physical magnetic stripe details (CVV).

Therefore, making a magnetic stripe card using only the details the attacker has sniffed from your contactless card is possible, but the details would be wrong and should be detected when you go to use it. I say should, because merchant terminals that accept magnetic stripe cards should go online to allow the card-issuing bank to verify that all the details are correct. This process should spot the missing cardholder name and also the wrong security code and the payment transaction should be declined. If the attacker is lucky enough to find a payment terminal that accepts magnetic stripe cards without going online to check, then they could conduct a fraudulent transaction. However, in this case, it is the merchant or their acquiring bank who would be liable, as they had not followed payment scheme rules/guidelines and checked the transaction details online. And you, the consumer who had some of your contactless card details sniffed, would not be liable for a penny.

Online payment card transactions are sent from merchants to acquirers to check details with the card-issuing bank

---

Making a fraudulent payment with your card details

The final attempted fraud we will look at is the attacker using your sniffed card details for a ‘card not present’ (CNP) transaction, say, to purchase something on the Internet or over the phone. The schemes say that in order for a merchant to accept a CNP transaction without being liable for fraud, they must collect all of the following:

- Cardholder name
- Billing address
- PAN
- Expiry date
- Printed security code (CVV2)

Once again, as outlined in the earlier table, our attacker only has two of these by sniffing your contactless payment card. The idea is to require so much information that an attacker would not bother to find it all out. In order to make a fraudulent transaction using only your contactless card information, he would need to find a merchant that is prepared to accept only PAN and Expiry date and these are increasingly hard to find. However, as Channel 4 News recently reported, some merchants as big as Amazon are accepting purchases without requiring the full details that the payment schemes dictate. We tested this and it was indeed true. It is not clear how long this has been going on and how long it will be allowed to continue. However, again because payment scheme rules/guidelines have not strictly been followed, this makes the merchant (Amazon) liable for any fraudulent cards that they accept. However, the success of Amazon would indicate that this can be a risk worth taking. It should be remembered that in the case of Internet purchases, the attacker has to supply an address at which they wish to receive the goods, so this adds an extra level of security checks.

Our verdict: are we safe from sniffing?

So, the question remains: how much do contactless cardholders really need to worry about ‘sniffing’ or ‘snooping’? According to the payment scheme rules, cardholders are protected against both of these threats – provided that they do not break the rules (such as revealing their PIN). After all, debit and credit card transactions of all types come with their own risks, just as walking down the street with a wallet full of cash can open you up to a risk of being mugged.

However, all the examples of successful fraud outlined in this investigation are where a bank or a merchant has not fully implemented the security protocols set out and supported by the payment schemes. In

---

these cases, the banks or merchants are taking the risk and are liable for any fraudulent payments, not the cardholder.

But the good news doesn’t end there. Security concerns aside, contactless cards have been designed to speed up payment processes and ultimately make queuing for things much more efficient. As with any new payment technology, much like when cards were introduced, you’re being offered more convenience, but perhaps slightly more risks, but this technology is still safer than carrying cash.

So the general rule of thumb with contactless cards, and with a ‘normal’ card for that matter, is to keep your card safe and close by and don’t reveal your PIN to anyone. However, if you still have concerns about what can be read from your contactless payment card in your pocket (i.e. your card number and name), then I suggest that you simply wrap it in a piece of kitchen foil, since that alone will prevent any reader from reading it unless the foil is removed. That should give you total peace of mind – as well as a much better alternative to the card shields vendors who will no doubt continue to fuel the misconception that contactless cards are not safe.

Acknowledgments

The author wishes to express his sincere thanks to his colleagues at Consult Hyperion for supplying and checking the facts in this article. In particular:

- Richard Allen
- Dave Petch
- Andrew Whitcombe
- Dave Birch
- Simon Laker

Contactless bank cards pass two million milestone on Transport for London buses

Eurotransport talks to Shashi Verma, Director of Customer Experience at Transport for London, for an update on how the first phase of the network’s contactless bank card roll-out has gone so far on London’s 8,500 buses. The interview was created in association with Consult Hyperion and first appeared in Eurotransport Issue 4 2013 and can be found at www.eurotransportmagazine.com.

Q. When we last spoke about the project it was some time before the bus launch. Can you remind us why Transport for London (TfL) is adopting contactless payment cards?
A. Of course. The opportunity to use contactless payment cards (CPCs) will offer much greater convenience for our customers since they’ll be able to use a contactless debit/credit card that they already have, instead of needing to get and keep an Oyster card topped up. It’s part of our ongoing focus to improve customers’ experience of travelling in the capital.

Paying for transport should be as easy as buying a sandwich. Enabling customers to use their contactless payment card on the buses and from early next year on London Underground, DLR, London Overground and trams, removes the inconvenience of needing to top up an Oyster card or dig around for cash before making a journey. Plus, it also makes London's public transport far more accessible for visitors, as anyone with a CPC will be able to enter the transport network as soon as they arrive simply by ‘touching in’ with their payment card. In addition, visitors will also have confidence that they are getting the best value possible, as opposed to having to understand complicated local fare structures.

Q. The benefits for passengers are clear, but surely there are benefits for TfL as well?

A. Indeed. For a start, the ability to accept contactless payments will reduce commissions and processing costs for TfL. In addition, we will not need to issue as many Oyster cards, which are expensive and we’ve seen them be discarded by visitors after only a few days’ use, so there will be much less environmental waste.

We are leading the world globally with the widespread acceptance of CPCs. Not only that, but TfL has become one the world’s largest single ‘merchants’, (as transport operators are known in the payments world), by accepting CPCs. By this I mean that now when passengers touch their cards on a reader they are making a transaction in much the same way as they do in the retail environment. Although it’s been a lot of hard work to get to this stage for us and our partners, it’s been well worth it and we’re very proud of this achievement.

Q. Yes, it has been six-months now since TfL launched contactless payment card (CPC) acceptance on London buses, Why on the bus network first?

A. We rolled it out on buses first as these journeys on the network are charged at a flat fare which allows the ‘retail model’ to be used (the cost is known in advance of the journey and £1.40 is charged to your card), so only a simple back office is required. So although still very difficult, it is easier than the model required for zoned transport (i.e. rail) where the fares vary. For these the cost is not known until the journey is complete.
Therefore, all the card ‘taps’ are collected in the back office, where the fare for a journey is calculated. Then at the end of the day the total amount charged for all journeys taken in the day is calculated and this authorisation for this payment is requested, so a much more complex process.

CPCs on buses is extremely simple in concept: a fixed flat fare – equivalent to the cheaper Oyster fare - is charged to the bank account associated with the CPC.

The idea for bus customers was that we want to provide an alternative payment mechanism for those who usually pay the higher cash fare (up to 85,000 per day) or casual users of buses. We are not trying to displace Oyster cards which are still the best option for many of our customers. CPC transactions are currently running at about 0.5% of the trips made by adult fare paying Oyster card users on buses.

Q. How has it gone so far? We’ve seen reports that you’ve reached well over the 2 million contactless cards transaction mark now?

A. Yes, It has been quite exceptional, and we’re very pleased with the uptake.

Before the launch, we forecasted that there would be 90,000 CPC payments on buses per week by the end of 2013. In reality there are already 130,000 per week and this is not yet showing signs of reaching a plateau. To put this in context, this is approximately half the number of CPC transactions that are currently being taken by M&S, the retailer currently taking the most CPC transactions in the UK.

We’ve now seen over 2.5 million contactless transactions across the bus network, and the figures show that more and more passengers are choosing to pay for their journeys with their contactless card. More than 10,000 cards are used each weekday of which about 1,000 are new to the system. We will see this continue to increase as more cards are issued by the banks and they become more widespread.

We’ve seen weekly transaction rates continue to grow across all the bus routes with particular popularity on the central London bus routes. The number of people using their contactless payment card has continued to rise each week. From 2,061 people making 2,586 journeys paid for on their contactless payment card on the first day in December we are now seeing up to 23,000 journeys each week day.
Q. It's clear the technology is working as it should do and people like using their contactless cards on the buses. Can you explain the work involved to date?

A. The technology has bedded in just as it should have and we’ve had no problems. The buses are using 3G mobile communications to send 6.3 million transactions (both Oyster and contactless) over-the-air to the back office each day. But, as you’d imagine...equipping 8,500 buses with the new readers capable of reading Oyster and CPCs was a major project in itself.

We are now embarking on the controlled rollout of the reader software that will add the CPC functionality to the current Oyster functionality at Tube, London Overground, DLR and tram stations.

Q. I also remember that you were concerned with overcoming the much slower transaction speeds for CPCs compared with Oyster – how successful have you been on that front?

A. Yes, that has been a really tough challenge as contactless debit/credit cards currently take around half a second, which is a little longer than Oyster cards take to transact, largely because of the added security features. The speed that CPCs can transact with a reader is important for the transport environment as we want to maintain fast boarding and therefore journey times for our bus customers and the speed at which customers pass through gates at stations.

We’ve continued to work closely on this next phase with an independent consultancy called Consult Hyperion that specialises in this kind of technology, as well as with some of the major chip manufacturers to test and measure this impact on the buses. Our research showed that transactions speeds need to be below 550ms or else they will have a tangible impact on bus dwell times.

With our partners we’ve managed to ensure that CPCs could be read within the threshold but the actual time taken depends on the technology the issuing bank uses. To date, of all the cards seen on the buses across the network, the average mode read time has been 540 ms - just within the threshold that we required - but inevitably, the time to read CPCs will decrease significantly further as the technologies improve.

Q. But surely, as with any major tech rollout, there are always ‘teething problems’ as consumers get used to it as we’ve seen recently with reports from retailers where people claim they’ve inadvertently paid via contactless?
A. Overall, the feedback from our customers has been very positive. Our call centre has been receiving a very low level of queries, around one per day, relating to the use of CPCs on the buses. We are seeing that there are some contactless payment cardholders who are not aware they even have a CPC in their wallet and what we need to do is educate them about how to store and use the card.

The single biggest customer issue has arisen when both an Oyster card and a CPC have been presented to the card reader in the same wallet. If the reader detects both cards, it will reject both and not charge any card. However, if the wallet or purse contains a number of cards and other items, it is possible that the reader will detect one card without seeing the other (for example, if they are on opposite sides). This can result in the customer’s CPC being charged when, for example, they have already bought a season ticket. If this has occurred we have given the customer a full refund. No instances have occurred where both an Oyster card and a CPC have been charged for the same trip and our advice to customers is to keep their card (Oyster or CPC) separate when presenting it to the card reader.

Q. So, more education for consumers might help, and how about the much hyped and heralded NFC enabled phones, could they be a viable prospect soon?

A. Yes, as we get closer to the expansion of CPCs to the rail network we will be carrying out a comprehensive education campaign, working with the card schemes and issuers.

With regards to NFC enabled phones, we’ve naturally had one eye looking even further into the future and have again worked with Consult Hyperion and a small number of mobile payment platforms to test CPCs hosted on NFC enabled phones on the network.

Unfortunately, as things stand at the moment, these are all much slower than CPCs and currently are not fast enough to be acceptable on TfL buses if large numbers of passengers were using them. Fortunately, there are no contactless debit or credit card products widely available on NFC in the UK at present, so we’re some way from this being an issue, and again we expect these times to improve as the technologies improve.

Q. So now by accepting contactless cards, TfL is essentially a merchant, and a very significant one at that. In terms of meeting security and compliance standards, how hard has that been?

A. The PCI Data Security Standard (PCI DSS) is required for anyone who accepts credit cards, and in terms of sheer numbers of CPCs across the
network, TfL has become a very significant merchant. So, it has been paramount to stay close to the payment schemes and achieve PCI DSS compliance. This has proved challenging because PCI DSS was not designed for the world of contactless payments, let alone the world of transport payments where there are typically no PIN entry devices. PCI documentation and requirements do not currently provide for smart card readers without PIN pads, so there was further groundbreaking to be done.

Working with our QSA (NCC) it took 18 months to achieve PCI DSS compliance, which is granted, ultimately by the payment schemes themselves (Visa, MasterCard and American Express). Another key part to this was achieving merchant acquirer and scheme acceptance of the overall system security. Again, it helped working closely with our partner Consult Hyperion, who wrote some of the detailed reader security requirements for protecting the PAN.

Owing to the leading edge nature of this project, much was learned on all sides which TfL and all the partners can carry forward with us.

Q. Technology aside, how is the new payment model shaping up and what are the next steps?

A. The ‘flat fares’ model used on buses works really well as the new 3G connection links each bus to TfL’s Central Office so that transaction information can be periodically uploaded (rather than having to wait until the end of the day, as was previously the case). This has allowed early deployment without significant Central Office development.

Now that we’re working on extending the acceptance of CPCs to the Tube, London Overground, DLR and trams, a new ‘transit payment model’ will be introduced, making it possible to charge according to distance travelled, rather than the flat fare of the current bus-only implementation. Again, working with Consult Hyperion and the payment schemes (Visa, MasterCard and American Express) we’ve been able to design a completely new transit payment model which will not only allow zoned fares, but also daily and weekly capping to be applied.

In turn, the payment schemes have now adopted this transit payment scheme into their rules and requirements so that it can be adopted. In the UK, this is facilitated by the UKCA, so we’re hopeful this will not be too far away.

Q. That is a real milestone, so what are the next phases of the project?

A. Yes, it’s been a great achievement to get the new payment model working well in the trials, and we’re working to an early 2014 date, where
Tomorrow’s Transactions—The Transit Reader

customers will be able to use contactless payment cards on the rest of the TfL network. Customers will be also be able to set up online accounts to check their journey history, and what fares they have paid, whilst still continuing to be safeguarded by the same EMV security technology underpinning Chip and PIN transactions, that the card issuers and schemes have developed.

From a TfL and business point of view, we are in a unique position to be able to offer the back office technology that we have built in house and the commercial leverage we have with the card payments industry to other transport operators outside of London to implement on their networks.

Q. Yes, I’ve seen at some of the industry conferences where TfL has presented about the contactless migration work that there has been interest from transit operators both within the UK and abroad?

A. Yes, as what we’ve been doing is groundbreaking, we have tried to share what we’ve learned along the way as much as we can and help others who perhaps are having similar problems to what we came up against and ultimately overcame. One of the main attractive features is that the banks issue the CPCs, so the transport operator does not need to, and they are already proven to be internationally interoperable. If the card does not work, the cardholder should contact their bank, not the transport operator.

The missing part of the jigsaw for the transport operators new to CPCs is the ‘back office’ which accepts the CPC ‘tap’ transactions merchants collect, calculates the equivalent fare (including any capping) and settles with the acquiring bank. In the payments world, this role is known as the transaction processor, and large merchants, such as supermarkets, typically use processors, rather than deal directly with acquiring banks themselves. This role of ‘processor’ has not been done before in the transport environment, so TfL is in a strong position to offer its back office transaction processing and settlement service to other operators who do not wish to spend several years developing their own.

Q. That’s an interesting model, so plenty of potential for TfL to generate additional revenues by offering other operators a back office processing facility?

A. Yes, these are all areas we are looking at with our partners.

There is still plenty of hard work ahead of course with the future phases of CPCs on our network, but there are some really interesting times ahead as we continue with our longer-term objectives, laid down when we embarked on this project several years ago. For example, we hope to start
working with system integrators to support their solutions to operators throughout Europe, and of course CPCs provide a platform for wider, global interoperability capabilities too. So, the work we’ve started here in London will hopefully pave the way for a joined up and much more efficient and cost effective way to operate global transport network.