Small Transactions, Big Losses – The Challenge of Mobile Wallet Re-tokenisation Fraud in Mass Transit.

In this article, Tim Jefferson, Senior Consultant at FirstPartner and Contactless Transit Ticketing specialist, explains the how the passenger convenience and simplicity of mobile phone enabled contactless ticketing has opened a significant and difficult to resolve fraud challenge for transport agencies. This and a range of other fraud issues will be explored in more detail in the Fraud Prevention Roundtable that will be chaired by Tim during the Payments Leader's Summit in London on the 29th-30th April, 2025.

Local train, metro and bus fare ticketing would seem an unlikely target for fraudsters. Average transaction values (ATVs) are low – typically in the range of six to nine pounds (£GBP) per day, and the effort involved in making any significant financial gain is high. Unfortunately, a consequence of the tokenisation and payment authorisation method adopted to make transaction processing as efficient as possible for transit operators offers fraudsters a simple to exploit loophole with a ticket to unlimited free rides.

So, how does it work? Contactless ticketing payments made with a mobile wallet such as Apple Pay or Google Pay typically use tokenisation and a “deferred authorisation” model. This allows offline ticket issuance and instant access at ticket gates without the delays associated with online authorisation. Under this model, the contactless taps made by a passenger over the course of a day are identified by the tokenised virtual card credential generated by the mobile wallet (known as the Device Primary Account Number or DPAN), and are collated and then authorised by the passenger’s card issuer at the end of the day. Compromised cards and DPANs that fail authorisation are put on the transit agencies “deny” list that prevents them being used for subsequent journeys.

Unfortunately, this process opens two loopholes for a fraudster to exploit. Firstly, the deferred authorisation enables a fraudster using compromised card details to travel for up to twenty-four hours before an authorisation is attempted. Then, at the end of the day, they are able to extend their access by re-tokenisation or “card tumbling”. This involves simply deleting the compromised card from the mobile wallet and reloading the same details (referred to as the Funding Primary Account Number, or FPAN) the following day. This generates a new tokenised DPAN which is different from the DPAN on the operator’s deny list and so is not stopped the next time the wallet is used for travel.

This type of fraud is a typical in that fraudsters are attacking vulnerabilities in the processes and procedures that bank credential issuers, mobile wallet providers and card payment schemes use to provide a seamless onboarding solution for adding new payment card credentials to mobile wallets. The lack of friction in the virtualisation of the FPAN into a mobile wallet with a DPAN, was key to driving the uptake of cEMV on mobiles but is open to simple exploitation.

This type of fraud has been around for some years but increasingly transit agencies such as Transport for London (TfL) and the MTA in New York have been saying that it now represents an increasing percentage of the total fraud/fare evasion for ticketing. But we need have a real perspective on this messaging, as total fare evasion (all types of not paying a fare) on TfL, is 3.9% of total revenue, which equates to over £130m ($US173M) in unpaid journeys. This is much lower than the MTA, which has an evasion rate of some 13%, which is a calculated at a staggering $US700M (£530M GBP) per year in lost revenue. But re-tokenisation fraud is a very small fraction of these totals, as cEMV is roughly 60/70% of total ticket sales and mobile (tokenised transactions) is about 70% of those (in London). So, again compared to eComm the actual fraud figures are really quite low. Transit agencies do not publish statistics of actual re-tokenisation fraud for obvious reasons, but from Freedom of Information (FOI) requests figures of around 0.015% of the total value of card payments, is the approximate figure for TfL.

While the vulnerability is well understood, it is not easy to mitigate. One of the key challenges is the complexity of the ecosystem that enables contactless mobile payments to be collected as the graphic below from TfL demonstrates:

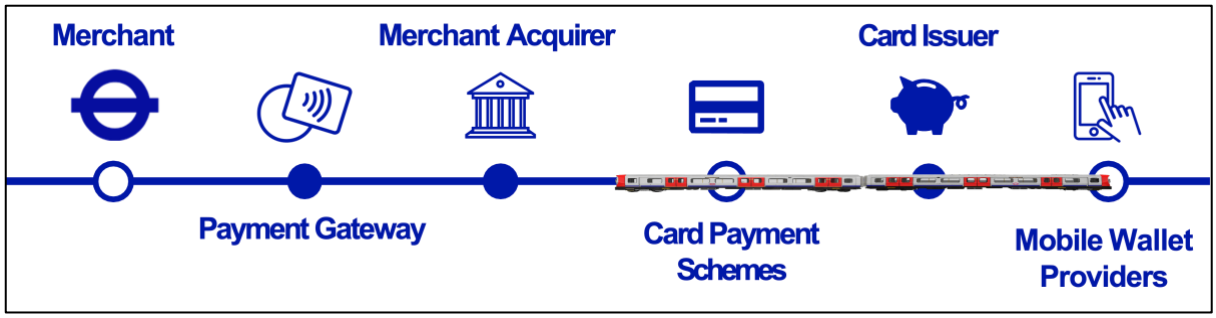

Fig 1. TfLs view of the complex transit ecosystem for cEMV acceptance - March 2025 (source TfL)

As can be seen, TfL as the merchant is reliant on coordination between at least five other ecosystem players to tackle this type of fraud.

Card Payment Schemes have tried to help by introducing a "re-provisioning block", where DPAN's, which are created when the end user loads a virtual card onto their digital wallets, cannot be re-enabled for the same FPAN for a defined number of days. This is helpful in theory, but fraudsters are innovative and some just use different card credentials on different days.

Some Card Payment Schemes have used velocity checks, for example counting the number of times a card is provisioned, the user spend or the volume of transactions to highlight suspicious behaviour. This is a standard fraud detection technique, but it has not fully addressed the issue.

Transit agencies, such as TfL or the MTA, have said openly that it is not just down to the Card Payment Schemes, but also the card issuing bank or e-money licence holder, to ensure they monitor and manage their card holders effectively. Unfortunately, there is a continuing dependence on legacy systems and processes that don't always track or manage repeated re-tokenisation attempts. Card issuers also, rely on the OEM wallet providers, such as Apple and Google Pay for most of the effort, in creating DPANs and delivering the essential seamless user experience.

For card schemes setting the rules and card issuers delivering payment products to their customers there is a fine balance between product innovation and risk. Card schemes are keen to not be overly prescriptive in the enforcement of scheme rules, for fear of stifling product innovation.

FirstPartner has experienced the impacts of the need to strike this balance between risk and innovation, including around this re-tokenisation issue, the move from 6 to 8-digit issuer BIN ranges and specific EMVCo non-compliant transit acceptance devices, where scheme rule "waivers" are commonplace.

Transit agencies can do some things themselves. An example would be adopting the newer 8-digit issuer BIN ranges, so that suspect BINs can be identified and blocked. The 8-digit BINs provide more granular information about the issuing bank (than the previous 6-digit version), making it easier to identify and track transactions related to a specific card issuer. However, this can be difficult and costly. TfL, for example, would have to change all their cEMV acceptance readers, their payment gateway and acquirer systems would need to be updated to accommodate the acceptance, identification and management of 8-digit issuer BIN numbers.

Another thing that agencies and their technology vendors can make more use of, with the card issuers and payment schemes is the Payment Account Reference (PAR), which was introduced EMVCo in 2016, but only recently hit near 100% penetration in the UK. PAR is a 29-character alphanumeric string which links the card’s PAN with the one or more tokenised virtual cards created from it. This is really useful at identify cards and providing the merchants with real customer data, but many transit agencies cannot make use of it, as their acceptance terminals and/or their technology vendors are yet to support PAR. This will be addressed in the next technology refreshes, but it is taking a long time.

As with many things in payments, this simple to commit cEMV transit ticketing fraud can be complex, costly and time consuming to manage effectively. With such a complex payment authorisation and processing ecosystem, all the players have to be synchronised in their understanding of each others' issues and work together to find suitable solutions. Collaboration - with sharing information and best practices is the way forward and transit agencies are pushing hard at present to get even more collaboration with the wider payments eco-system to drive this effective collaboration.

Tim Jefferson - Senior Consultant - FirstPartner - tjefferson@firstpartner.net - + 44 (0) 7836 660 419