Blog

Privacy in a Cashless Society

12th October 2019

As highlighted in the Access to Cash Panel's final report published in March 2019, consumer concerns over privacy are often cited as a reason that people continue to wish to use cash. In the six months since the report was published, various headlines have highlighted an acceleration in the reduction of free to use ATMs, further bank branch closures and an increase in the number of retailers and public bodies no longer accepting cash as a means of payment; all of which is putting pressure on those who wish to continue to use cash. For those concerned about the privacy of data associated with their transactions, this is a worrying trend.

So, are people right to be concerned over the privacy of their data if they have to switch to using cards or other means of payments? At first sight, it is difficult to argue that the answer is "No". When you walk into a shop and pay by cash, you are leaving no digital footprint behind of your association with the transaction. The retailer's point of sale terminal (and any linked stock control system) will know that a specific item of stock has been sold, but it has no information in terms of the purchaser unless such information is voluntarily provided. The moment a payment is made with a card rather than cash, there is a linkage between the sale of that specific item, the initiation of a payment transaction via the merchant's card acquirer (who would normally supply the point of sale terminal), the handling of the transaction via the card Scheme (e.g. Visa or Mastercard), the transaction authorisation via the card issuer and the subsequent payment from the customer's card issuing bank to the merchant's bank. Data is captured at various points in the transaction cycle and will then be retained (often for years) for regulatory and/or accounting requirements.

At this point, it must be highlighted that no details of the underlying purchases at a store are passed to the acquirers, the card schemes, the card issuers or the banks involved in the transaction. The data remitted will need to adhere to the underpinning ISO 8583 (card) messaging standard. This requires that a variety of data components be captured at the point of sale and passed through for processing (such as the merchant (card acceptor) unique ID, merchant name and location, date and time of the transaction and the total amount). However, a four digit Merchant Category Code is also included in Field 18 of the message which could give insight into the transaction. There are many of these. Some of those used by Mastercard[1] include:

- **5411** Grocery Stores, Supermarkets
- **5813** Bars, Cocktail Lounges, Discotheques, Nightclubs, and Taverns—Drinking Places (Alcoholic Beverages
- **5814** Fast-food restaurants
- **5912** Drugstores and pharmacies
- **5931** Second Hand Stores, Used Merchandise Stores
- **5933** Pawn Shops

[1] Mastercard quick reference booklet – Merchant Edition (Nov 2018) https://www.mastercard.us/content/dam/mccom/en-us/documents/rules/quick-reference-booklet-merchant-edition.pdf

- **5944** Clock, Jewellery, Watch and Silverware Stores
- **7273** Dating services
- **7995** Gambling Transactions
- **9211** Court costs including Alimony and Child Support
- **9222** Fines

In isolation, a transaction provides only limited information. However, over a period of time, the names and business type of the merchants that a consumer uses and the frequency of transactions would likely provide insights into a consumer's lifestyle if this data was to be inappropriately utilised. Concerns on this have been aired in the media from time to time such as the following article from 2011:

https://www.foxbusiness.com/features/mcc-codes-unveil-consumer-shopping-habits

Turning to the retailer (where the underlying details of the transaction is known), things then boil down into two camps; those where the store has an agreement with the customer that their transaction data may be analysed and those that don't. The former is readily highlighted by store loyalty programmes where a customer may receive incentives such as cashback, tailored vouchers or early access to sales or special offers. In exchange, the Terms and Conditions of such loyalty programmes are likely to inform the customer that their data might be analysed for marketing purposes. A hybrid form is also present where the customer may not hold a loyalty account but, at the point of sale, they are asked by the merchant for their zip/postcode and/or address details. This may be explained for an offer to go onto mailing lists or for warranty/guarantee purposes. Again, customer consent permits restricted use of the data at that point.

Any such data held by a company (or others in the payment chain) must be protected in line with local data protection laws. In countries covered by the EU 2018 General Data Protection Regulations, the obligations relating to data controllers, data processors and the associated rights for individuals "to be forgotten" via Subject Erasure Requests extended the earlier data protection obligations that firms had to follow.

However, data breaches can and do occur. In 2013, the US retail firm Target fell victim to Point of Sale malware, which resulted in the theft of data relating to up to 70 million customers. This resulted in Target settling a class action suit from banks and credit unions for $39.4m[2].

Turning back to the core question of whether consumers are right to be concerned over the privacy around non-cash transactions it is easy to see from the examples above how such concerns can arise. For these to be allayed so that these consumers will switch away from cash, more concerted effort and information will likely be needed from retail groups and payment entities as to how consumer data is used, how it is protected, how long it is kept for and the rights of consumers to request that it be deleted.

Phil Kenworthy is a Member of the Access to Cash Panel and Founding Director of the advisory firm Payment Systems Consultancy Ltd

This was first published on the Payment Systems Consultancy website on 11th October 2019

http://paymentsystemsconsultancy.com/payments/privacy-in-a-cashless-society/

[2] Reuters - 3 December 2015 (https://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203)