REPLY TO THE CONSULTATION ON THE PSR INTERIM REPORT INTO THE SUPPLY OF CARD ACQUIRING SERVICES

By Neira Jones, CEO Phoenix Edge Ltd

PhoenixEdge

Phoenix Edge Ltd

Registered Address:

33a High Street, Stony Stratford

Milton Keynes, MK11 1AA

Company Registration Number: 6527212

DECEMBER 2020

Table of Contents

INTRODUCTION

About me

I advise organisations of all sizes on payments, fintech, regtech, cybercrime, information security, regulations (e.g. PSD2, GDPR, AML) & digital innovation. With more than 20 years in financial services & technology, I believe in change through innovation & partnerships and always strive to demystify the hype surrounding current issues. I enjoy my work as a strategic board advisor and non-executive director and am also a professional speaker. I also provide coaching and training, payment security expert witness services, and help with M&As cybersecurity due diligence. I like engaging on social media & regularly address global audiences in person or virtually.

I am the 1st member of Advisory Committee for PCI Pal, a global leader in secure payments & chair the Advisory Board for mobile innovator Ensygnia. I am proud to be an Ambassador for the Emerging Payments Association, the National Lead, Payments for the Federation of Small Businesses and a friend of the Global Cyber Alliance.

You'll find me on the Refinitiv list of Top 100 Influencers in Financial Services, the Planet Compliance Top 50 RegTech Influencers, the SC Magazine list of the UK's 50 Most Influential Women in Cyber-Security 2019, the Cybersecurity Ventures Women Know Cyber 2019 (100 Fascinating Women Fighting Cybercrime), the Jax Finance Top 20 Social Influencers in Fintech 2017, the City AM Powerful Women in the City List, the Richtopia Top 100 Most Influential People in Fintech. Tripwire nominated me "Top Influencer in Security To Follow on Twitter" in January 2015, CEOWorld Magazine nominated me Top Chief Security Officer to Follow on Twitter in April 2014, I am the Merchant Payments Ecosystem Acquiring Personality of the Year 2013, the SC Magazine Information Security Person of the Year 2012 and am an InfoSecurity Europe Hall of Fame alumni. I was voted to the Top 10 Most Influential People in Information Security by SC Magazine & ISC2 in 2010 & have served on the PCI SSC Board of Advisors for 4 years. I am a British Computer Society Fellow.

I have previously worked for Barclaycard, Santander, Abbey National, Oracle Corp. and Unisys. My clients span industry sectors, including financial services, fintech, retail, legal, consulting, information security & technology.

What prompted me to reply to this consultation

I was Director of Payment Security & Fraud for a leading acquirer between 2008 and 2015. Since then, I have been continuously involved with the payments and cyber security and fraud prevention industries. During my time at the acquirer, I have witnessed first-hand the various merchant challenges as they conduct their business and accept payments. Since then, those challenges still remain.

EXECUTIVE SUMMARY

I commend the PSR for launching this review, and I have waited in anticipation for the results. This reply was finalised upon reading all related documentation published on the PSR website and drawing from public information sources.

The points summarised below are only some of the reasons that prompted my reply, and I hope this document will be of value for the final PSR report:

- The **merchant services providers** assessed do not seem to be representative of the UK market, and whilst some important players are included, the differences in their operating models make the merchant questionnaire difficult to answer and the replies misleading. With the pandemic driving many small businesses to digital, failure to include a representative sample of merchant services providers will leave out a large proportion of businesses that accept card payments and a large proportion of service providers that offer these services of. The scope of the review should be revisited, if only from a **fairness and competition** angle. (see ADDRESSABLE SPACE section).

- The **specific characteristics of a merchant must be taken into account** when crafting any assessment: what applies to a large retailer will generally not apply to a small ecommerce seller. (See Merchant Services Providers Models section)

- The **merchant questionnaire** seems to take a "one-size-fits-all" approach. The supply of merchant services is complex and depends on a number of factors, such as the size of the merchant. Perhaps due to its complexity, it increasingly lacks transparency. This means that SMEs would find it difficult, if not impossible, to give true answers to some of the survey questions as they have no visibility on the constituents of some elements (See FEES & CHARGES section). This should be examined further from a **transparency** angle.

- The PSR interim report suggests that the benefits of the Interchange Fee Regulation has only been passed on to larger merchants, but not to smaller merchants. This is easily explained as smaller merchants are not offered the transparency on fees that larger merchants benefit from. I suggest further analysis of **all the fees** that apply to the various commercial models, and not just interchange (See FEES & CHARGES section).

- The definition of value-added-services (VAS) is vague and should be considered for further investigation. For instance, PCI fees are charged, but the provision of a PCI portal is not a value-added service as it merely satisfies acquirers' card scheme reporting requirements (See PCI DSS Related Fees section) and merchants have no choice but to pay. The cost to SME merchants runs to tens of millions of pounds per annum.

- Given the current pandemic, the **telephone channel** should be specifically reviewed. In this channel, merchants do not get similar incentives as for other channels (face-to-face or e-commerce), and have to invest in extra fraud prevention capabilities to fulfil their obligations, or face negative financial impact if they don't. Given current trends, **this should be examined from a financial inclusion angle**. If merchants cannot invest in extra fraud prevention capabilities in the telephone channel, this means of interaction will not be made widely available to vulnerable segments. In addition, service providers find it difficult to offer their solutions, which stifles **innovation** in this space. (See Telephone Payments section).

- **Underwriting practices should be examined** from a **competition** and **innovation** angle (see Underwriting section).

Given the PSR's remit around improving **competition**, supporting **innovation** and **promoting end user interests** in payment systems a thorough review of the card market is welcomed. Reenforcing why the supply of card acquiring services is important to the economy and identifying what the industry and regulators need to do to ensure an effective market is key.

The card payments ecosystem is a complex one. In my response, I have taken great care to present an unbiased view of the card acquiring market and all references are from public sources. My aim is to highlight the issues that SMEs face in our constantly evolving and challenging world. It is my belief that the regulators are ideally placed to help them achieve better outcomes, ultimately to the benefits of the end customer. The PSR review is a good start. I also wish to highlight the challenges that other ecosystem players (e.g. PSPs, acquirers, issuers, schemes) are faced with, with the intention to advocate for more transparency in an ecosystem that is so fundamental to the economy.

This document provides a list of clear recommendations (highlighted in grey throughout) after the various problem statements and explanations. I appreciate that, bearing in mind the amount of change that is happening within the industry, any regulatory intervention has to be proportionate and prioritised appropriately. But it also needs to recognise that accelerating societal change is changing the shape of the market currently dominated by cards. With this in mind, the PSR may wish to consider **establishing a working group of experts** to help prioritise and establish a plan of activities to implement findings of the current review and to monitor the need for further action. I would be delighted to help.

I hope you find this report of use, and I remain at your disposal should you have any further queries.

Neira Jones
December 2020
neira.jones@phoenixedge.co.uk

ADDRESSABLE SPACE

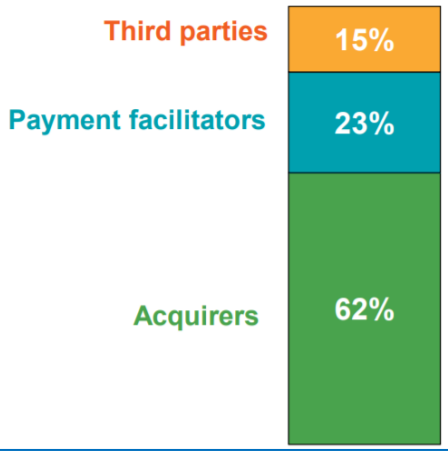
Merchant Services Providers Assessed

The interim report made the following selection as representative of the UK market:

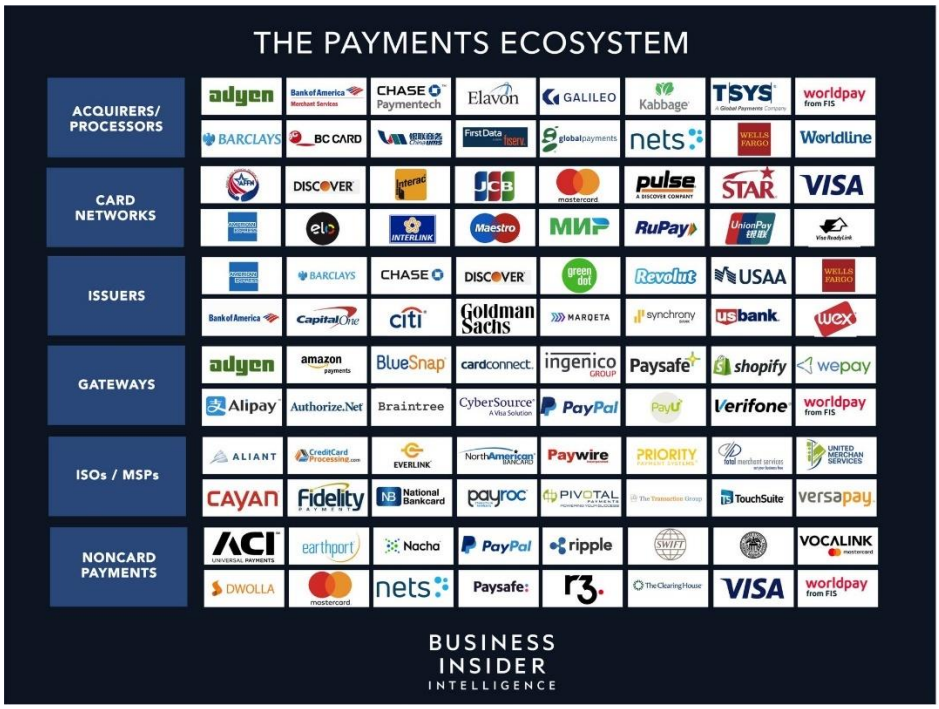
Top 15 main providers identified

Barclaycard
Elavon
First Data
Global Payments
I-Zettle
Lloyds Cardnet
PaymentSense
PayPal
Payzone
Retail Merchant Services
Sage Pay
Square
Stripe
SumUp
Worldpay

Main providers identified by provider type



Merchant services providers can play various roles in the card payments ecosystem. It is dangerous when conducting any assessment of product & services provision (especially when in relation to fees and charges) to treat them equally. For example, the contract types and operational requirements will differ depending on which model is used. In addition, the same players can play various roles in the ecosystem, as illustrated below:



Whilst the Business Intelligence diagram on the previous page shows a majority of global and US players, it illustrates the point. For example, Adyen is both a PSP and an acquirer, so is Worldpay.

The merchant services providers assessed during the study were as follows:

- **Main stream acquirers** (6): Worldpay, Barclaycard, Elavon, Fiserv, Global Payments; Lloyds Cardnet (provided by Fiserv)
- **ISOs** (3): Payzone (now Take Payments), Retail Merchant Services[1], PaymentSense
- **PSPs** (6): Stripe[2], Paypal[3], Sumup, iZettle, SagePay, Square

It is acknowledged that the pandemic has driven payments digitisation much faster than predicted. SMEs have been forced into accepting payments digitally faster than they would have planned. In line with industry statistics, commercial models that facilitate SMEs digital payments adoption have become increasingly popular. These models can be broadly categorised under the banner of "Payments Aggregators". The PSR study included some of these under the generic banner of "PSPs". In addition, some increasingly popular players are not mentioned[4].

However, the payment aggregators come in many forms[5], notably:

- **Payment Facilitators (PayFacs)**: some were included (e.g. Stripe, Shopify)
- **Merchants of record**: none were included (e.g. Uber, Amazon, Paddle)

Many of the smaller SMEs are not able to use payment facilitators or ISOs (for risk & cost reasons), let alone direct acquiring services, and have no other option than to use merchants of record, a trend which can only increase.

In addition, the final study would not be complete if it limited itself to mainstream acquirers, as many smaller entities needing to accept payments, especially during the current economic crisis, would present a risk that mainstream acquirers are not prepared to take. Players such as Credorax, Paysafe, Bambora, checkout.com, Safecharge, trustpayments.com and Acquiring.com should not be ignored (not an exhaustive list), and none were considered in the interim study.

[1] RMS may also have an acquiring license.

[2] Stripe also has an acquiring license.

[3] Paypal now also has an acquiring license.

[4] https://go.forrester.com/blogs/merchant-payment-providers-key-takeaways-from-the-forrester-wave-q3-2020/

[5] See https://www.venable.com/-/media/files/publications/2018/10/identity-crisis-in-payment-aggregator-models/acheatsheetfordistinguishingaggregatormodels.pdf

In addition, the current assessment leaves out card schemes such as American Express and Discover who operate under the three party model. Whilst these card schemes are not dominant players in the UK, they have been left out of the assessment and this might render the final report incomplete, especially as such schemes are actively targeting the UK market. The decision was made not to include these in the final terms of reference but it might be advisable to revisit this.

CONSIDERATION FOR FINAL REPORT:

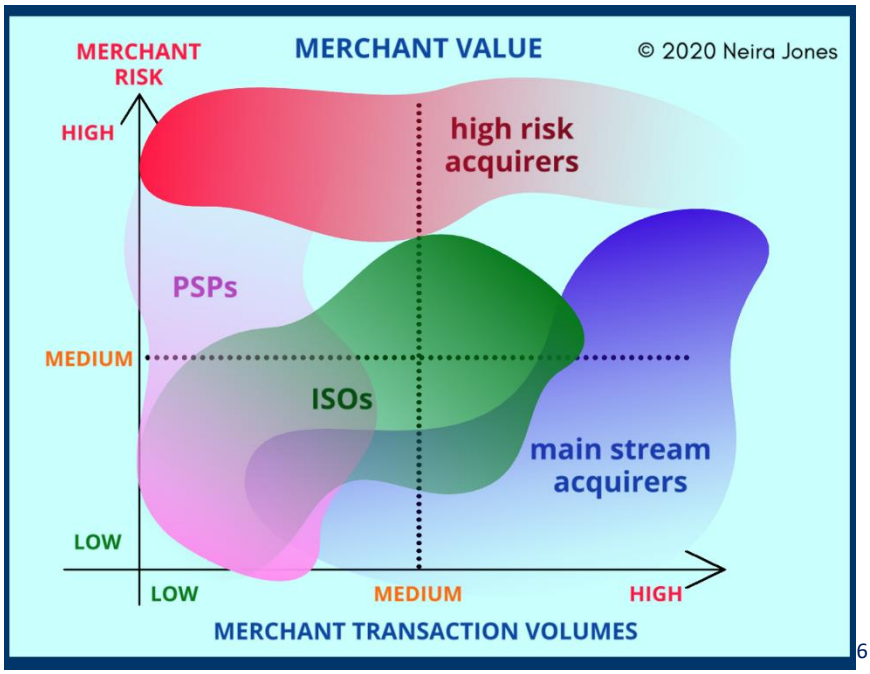
The current sample of service providers is not representative of the addressable market. With the pandemic driving many small businesses to digital, failure to do this will leave out a large proportion of businesses that accept card payments and a large proportion of service providers that offer these services.

In addition, attention should be paid to the fact that a “one-size-fits-all” approach to a merchant questionnaire will not give a true picture of the market. What applies to large merchants rarely applies to smaller ones.

Merchant Services Providers Models

Addressable Market

As explained in the previous pages, the supply of merchant services can be roughly divided as follows:



[6]

It is also worth noting that the "PSPs" category contains a number of different commercial models. Limiting the study to mainstream PSPs (e.g. Stripe) will leave a large part of the small trader population out, especially as these have no negotiating power.

The survey identified only three types of providers: acquirers, payment facilitators and third parties. It is not clear what is meant by "Third Parties" (this term is not defined in the glossary, and the terms of reference specify that these are "providers that do not also supply card-acquiring services", which is confusing) and even what entities are considered "Payment Facilitators".

CONSIDERATION FOR FINAL REPORT:

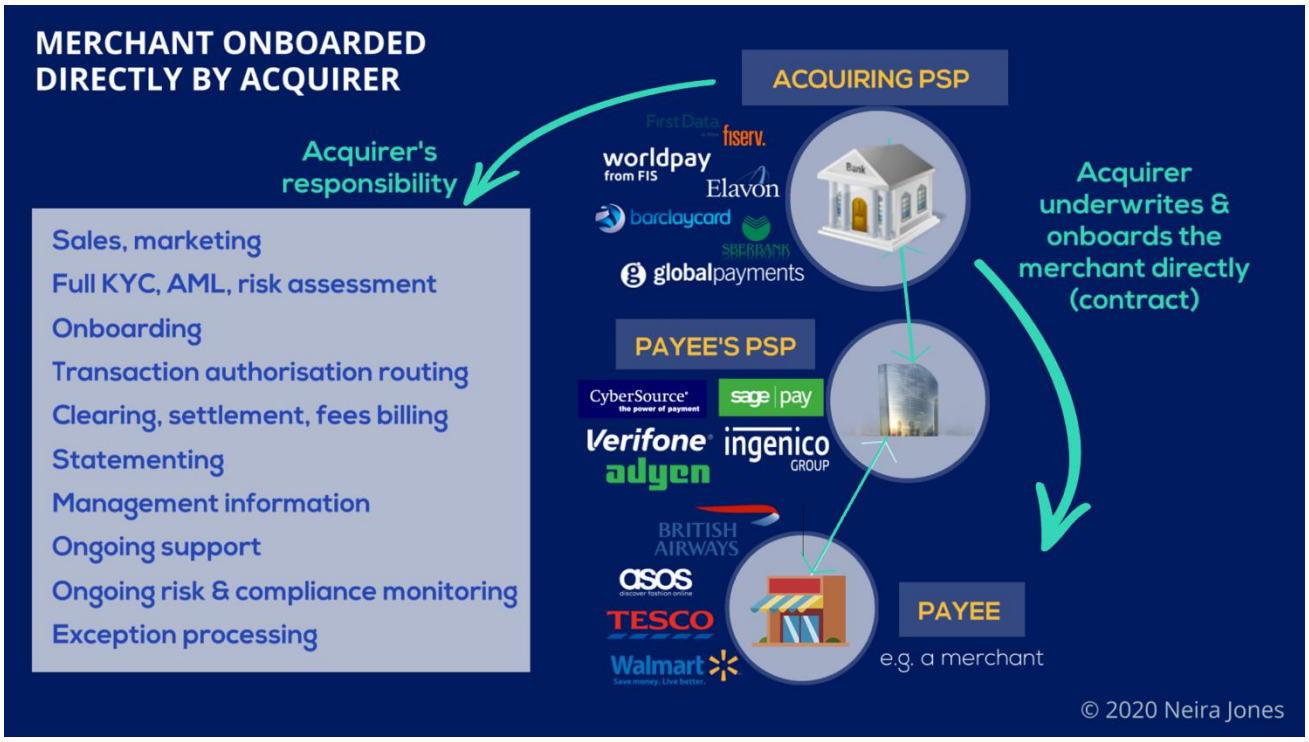
The current sample of merchants (and their service providers) is not representative of the addressable market. With the pandemic driving many small businesses to digital, failure to do this will leave a large proportion of small businesses (those who essentially have little choice or power to negotiate), in the same or a worse position than they are currently.

The following sections will examine the different commercial models.

[6] See Payments 101 – Part 2 – Card Payments Economics https://neirajones.thinkific.com/

Merchants Acquired Directly by Acquirer

In this commercial model, the merchant has a direct contract with the acquirer for the provision of payment facilities. This model is illustrated below:



Understanding merchant needs is key when determining which payment facility is best for them. Determining factors for the fees charged include:

- Transaction volumes
- Merchant type/ industry sector
- Merchant risk profile
- Channels/ payment methods

Underwriting is a crucial stage for the acquirer, and full KYC, AML, and risk assessment will be performed. Some acquirers will specialise in high risk merchants, typically charging higher fees than mainstream acquirers. Acquirers will onboard merchants directly if the merchant value is worth the cost. Too many large volume/ low fee merchants would be detrimental to acquirers, which is generally why they have a cap on the number of large merchants they are prepared to have in their portfolio. Low/medium risk merchants will also bring volumes, but higher risk merchants may not be worth the cost for mainstream acquirers. Acquirers may partner with ISOs or PSPs to bring merchant volumes according to their risk appetite[7].

[7] For example, Take Payments (formerly Payzone) has a partnership with Barclaycard https://www.takepayments.com/

CONSIDERATION FOR FINAL REPORT:

Merchants onboarded directly by an acquirer will know about "card acquiring services" and therefore will be able to answer related questions. However, depending on their size, they may not have visibility of the fee structure (e.g. merchants on blended or tiered models). This means that some merchants, especially SMEs, may not be able to compare like-for-like easily. In addition, it is accepted practice for some providers that merchants might not see the T&Cs until they have signed a contract (or these may be included as a hyperlink in the merchant service agreement, which they generally overlook). **Transparency** is a very real issue.

In addition, the concept of "card acquiring services" is not introduced well in the questionnaire. Question A1 page 2[8] presents a lot of acronyms, even in the explanation. A more helpful question, to capture as much of the market as possible, would have been "Do you accept card payments from your customer? If so, who is responsible for making decisions on how you take these card payments?"

Note: whilst one would be forgiven for thinking that merchants offered a blended model are made aware of the other rates available (interchange + or ++), this is largely not the case. Whilst some of the smaller acquirers would make this reasonably clear, others would at worst not even talk about it, and at best would make some cursory mention of it in their Terms & Conditions (Worldpay, Clause 2.9[9]), whilst still contracting the merchant to a blended rate[10]. In the latter situation, it is understandable why small merchants would not even understand such a clause. It is also understood that some providers provide a link to their Terms & Conditions in the Merchant Service Agreement[11], merchants would actually rarely read these, let alone understand them. This answers the questions as to why merchants can generally not dedicate the time or resources to switch providers, as no information is available to make effective comparisons.

[8] https://www.psr.org.uk/sites/default/files/media/PDF/MR181.5_Consultation_on_our_merchant_survey_questionnaire.pdf

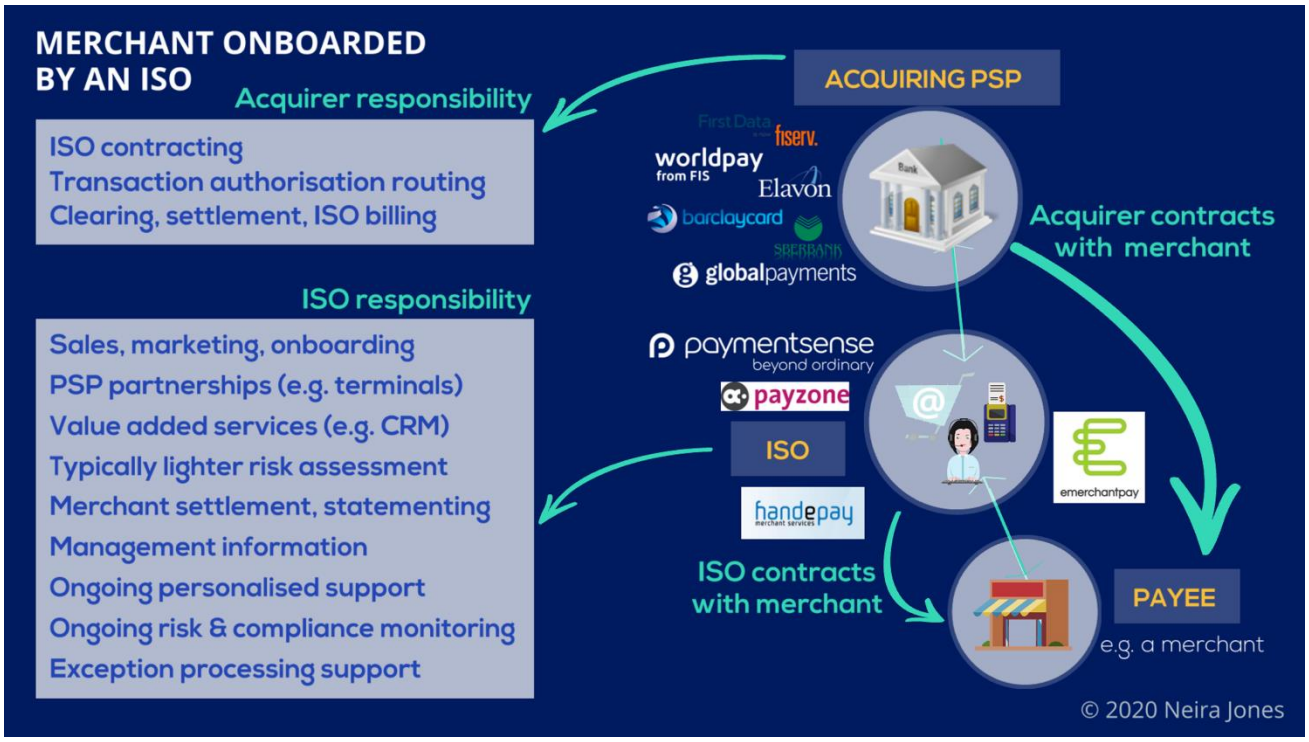
[9] Worldpay T&Cs https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/general/merchant-services-agreement-standard-tscs.pdf?la=en-gb

[10] See Article 9 Interchange Fee Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0751

[11] https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/general/merchant-services-agreement-standard-tscs.pdf?la=en-gb

Merchants Acquired by an ISO

In this commercial model, the merchant has a direct contract with the ISO, and also with the acquirer for the provision of payment facilities. This model is illustrated below:



Merchants onboarded by an ISO will generally pay lower fees than if they are directly onboarded by an acquirer. This is because acquirers will give ISOs wholesale rates so they can pass on savings to merchants. In this case the merchant will have a contract with both the ISO and the acquirer. ISOs can also partner with other providers (e.g. terminal providers or ecommerce payment gateways) and can be considered as a one-stop-shop for payment services for their market segments and generally offer a more personalised service.

ISOs add an extra layer between the merchant and the acquirer, as they take on additional risk. They will charge merchants for that additional risk, but this is compensated by their partner acquirers wholesale rates. This is why, generally, newly established merchants with little or no credit history are unlikely to interest ISOs. For these merchants, a "PSP" may be more suitable.

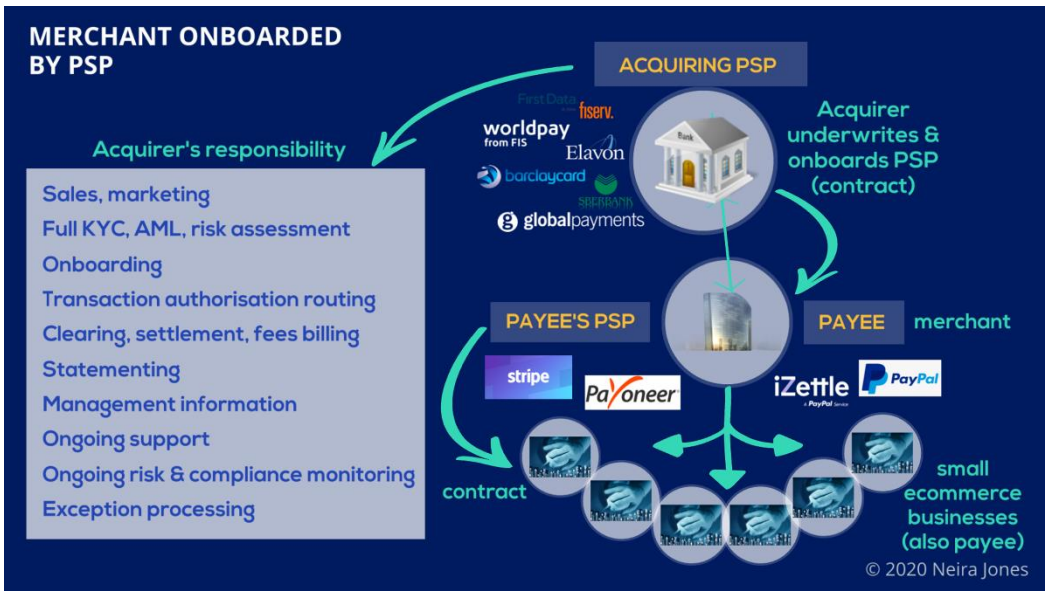
CONSIDERATION FOR FINAL REPORT:

Merchants onboarded by an ISO may know about "card acquiring services" and therefore might be able to answer related questions since they have a contract with the acquirer as well as the ISO. But as explained on the previous page, the fee structure will be different and they may not be aware of its detailed constituents.

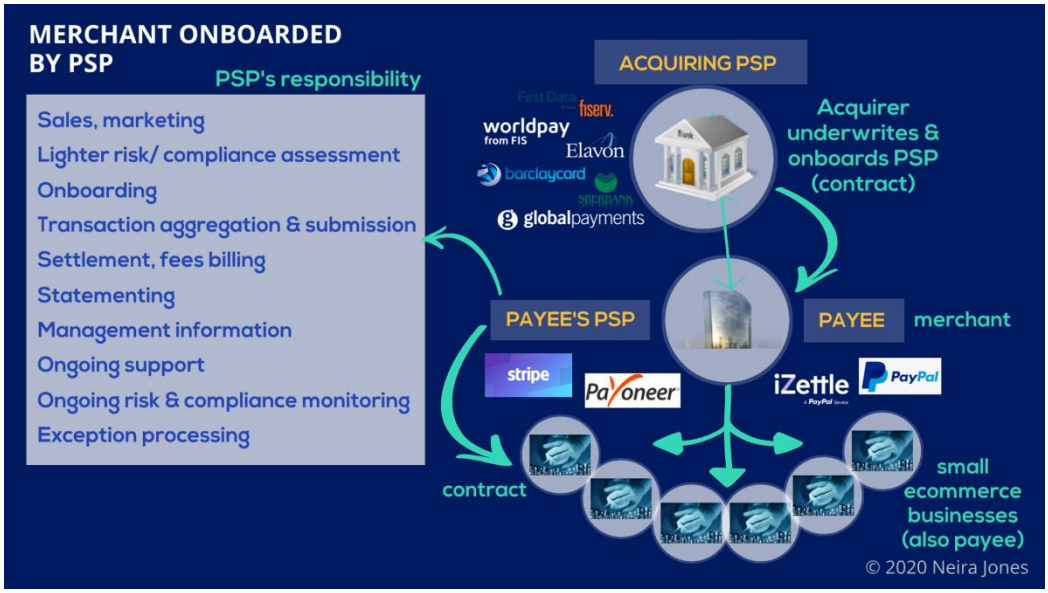
Merchants Acquired by a PSP

In this commercial model, the merchant has a contract with the PSP only. Here, the term "PSP" is used in its loosest sense, as there are many commercial permutations depending on the type of merchant.

In addition, the acquirer will have a contract with the "PSP", as illustrated below:



As the merchant only has a contract with the PSP, the latter will have a number of responsibilities, as illustrated below:



Acquirers will contract with PSPs to bring internet volumes. The PSP isolates the acquirer from underlying merchant risk as they can aggregate a multitude of smaller entities.

PSPs generally have more flexible, light-weight systems optimised for dealing with large numbers of small merchants. To keep costs down, they must also deploy significant automation, and merchant self-provisioning.

CONSIDERATION FOR FINAL REPORT:

Merchants onboarded by a PSP may not understand the term "card acquiring services" and therefore might not be able to answer related questions since they only have a contract with the PSP (e.g. Stripe). They will only see one rate for the payment facility. For those merchants that have deliberately chosen this type of PSP (e.g. Stripe), they are generally more able to switch providers (depending on contract terms) as there are many reputable ones on the market (e.g. Braintree, Shopify, etc.).

Some of the "sub-merchants" acquired by PSPs can themselves be merchant aggregators for yet smaller entities (who would not otherwise be able to afford payment facilities because of their very low volumes).

CONSIDERATION FOR FINAL REPORT:

This type of situation happens at the lower end of the market, especially for very small merchants selling digital goods. In such instances, the provider of the payment facility will be a sub-merchant of a PSP themselves. This model is sometimes referred to as Merchant of Record (e.g. Paddle, Thinkific). As the pandemic is driving even more small businesses towards digital, ignoring this segment of the market is not advised. This type of model provides a low cost option for small merchants. Again, merchants in this situation are isolated from the basic card acquiring fee structure which the PSR interim report concentrates on.

Furthermore, the merchants using these types of services would have their primary interaction with the Merchant of Record, and whilst they may see an option to set-up the payment method (say, using Stripe or Paypal) which is done when the relationship is set up, they would not necessarily know, or even remember that they have done this.

PSPs provide one-size-fits-all pricing, and fees are generally higher than other options, which make them unappealing to larger merchants (who would choose to engage with an acquirer, either directly, or through an ISO). They are however very attractive to smaller merchants as they are relatively hassle free.

Telephone Payments

The current pandemic has driven increased digitisation. In the UK, a market already heavily digitised, the trend has been no less exacerbated by the crisis. The increase in contactless limits has driven increased use of cards in the face-to-face channel, and we are all familiar by the controversy around ATM closures, especially affecting rural areas and vulnerable segments of the population.

Whilst telephone payments do not traditionally represent a very large proportion of the overall payments landscape compared to other channels, current trends and statistics should not be ignored[12][13][14].

This drives me to point out that vulnerable segments that have traditionally relied exclusively on cash (either by preference or necessity), only have one other avenue familiar to them, and that is the telephone. Some organisations have recognised this, such as Morrison's, who made the telephone channel only available to vulnerable self-isolating segments via their Doorstep Delivery[15] service.

If we agree with the premise that payments over the telephone are set to increase, then we should consider some of the well known issues traditionally associated with the supply of card acquiring services in that channel.

For the purpose of this section, I will limit the analysis to the telephone channel (because of volume trends), but all my observations equally apply to mail order (so that the MOTO – Mail Order/ Telephone Order - channel is covered).

The Orphan Channel

Telephone payments, from a risk and liability angle, have never been treated in the same way as face-to-face and e-commerce payments.

The 2nd Payment Services Directive (PSD2) and subsequent European Banking Authority responses do not resolve this matter, leaving interested parties having to resort to direct specific questions through the EBA Single Rule Book, or best effort interpretation. This area is still confusing[16]. In any instance, and outside of PSD2, current card acquiring practices for this channel should be understood.

---

[12] https://thefintechtimes.com/six-ways-to-cope-with-the-huge-spike-in-customer-call-volume/

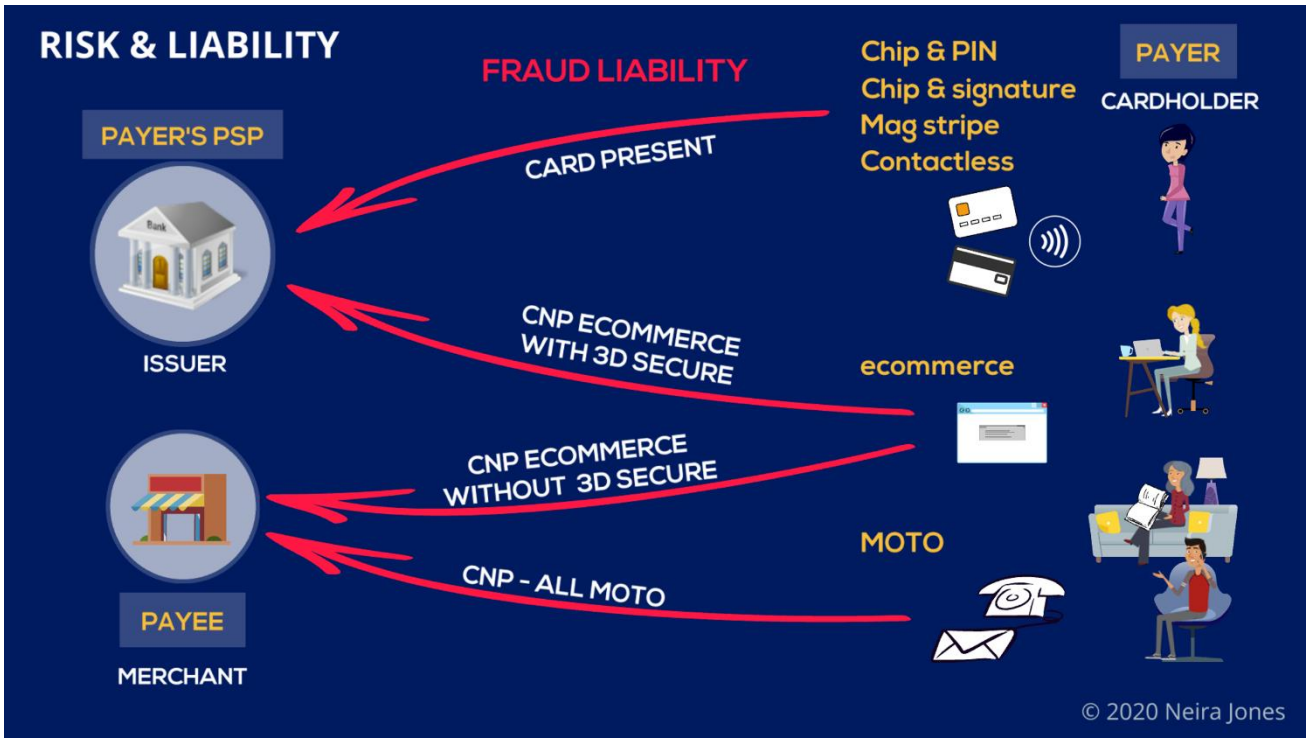
[13] https://www.iovation.com/blog/how-covid-19-is-causing-a-fraud-pandemic-in-call-centers

[14] https://www.clevelandfed.org/en/newsroom-and-events/speeches/sp-20200923-payments-and-the-pandemic.aspx

[15] https://my.morrisons.com/doorstep-deliveries/

[16] https://www.visa.co.uk/dam/VCOM/regional/ve/unitedkingdom/PDF/visa-preparing-for-psd2-sca-publication-version-1-1-05-12-18-002-final.pdf

The concept of liability is well understood in the card acquiring space. From a merchant's point of view, the concept of **liability shift** is an important one. This is described below:



17

As described above, if fraud happens in the face-to-face channel (e.g. cloned card), the issuer bears the liability. This means that the merchant still gets paid, and the cardholder doesn't lose any money.

If fraud happens in the e-commerce channel, and the transaction has been authenticated with 3D Secure, the issuer bears the liability. This means that the merchant still gets paid, and the cardholder doesn't lose any money.

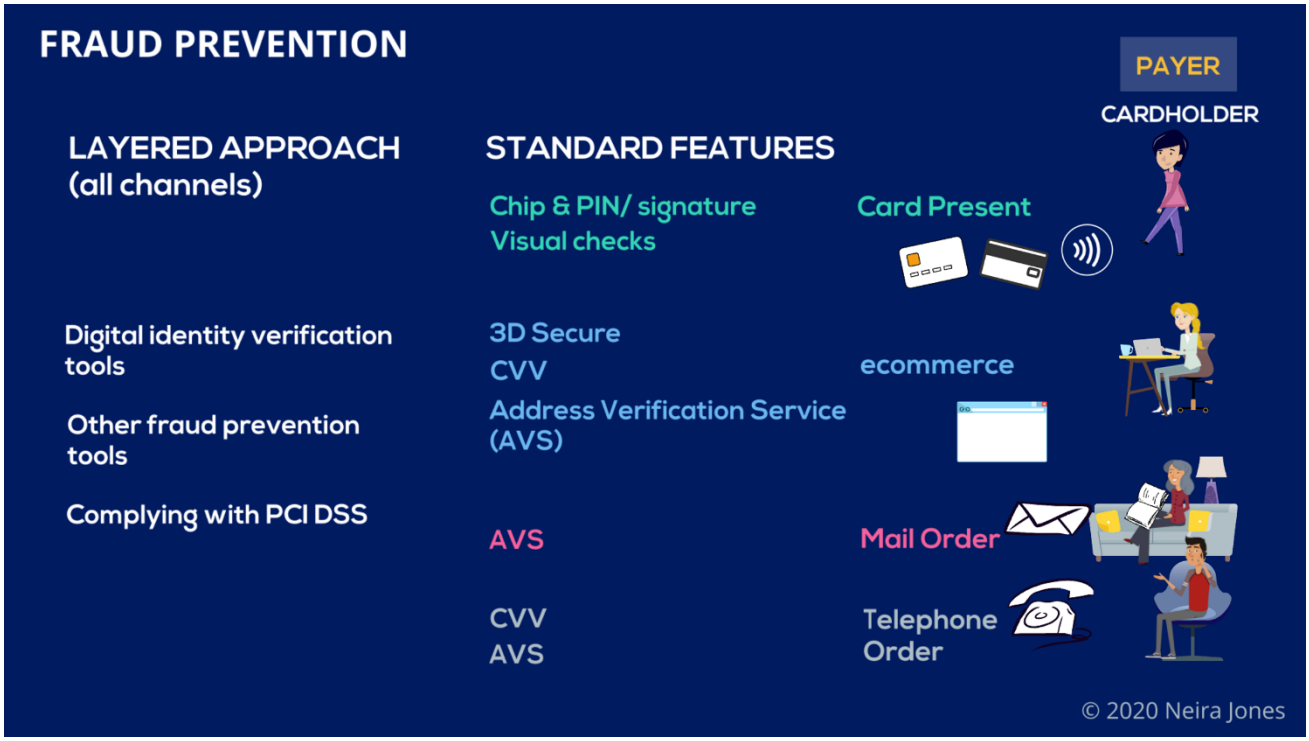
If fraud happens in the ecommerce channel, and the merchant hasn't deployed 3D Secure, the merchant bears the fraud risk. Simply put, depending on fraud levels and risk appetite, it is generally in the interest of ecommerce merchants to deploy 3D Secure, as they get a liability shift. This is an important fraud prevention incentive.

Merchants have no such choice or incentive in the telephone channel, as, regardless of extra fraud prevention measures deployed, they bear the fraud risk on any transaction through the MOTO channel. Merchants will probably not be aware of this risk and acquirers are unlikely to alert them. Especially for SMEs unaware of fraud or security risks, keeping

[17] See https://neirajones.thinkific.com/

written or recorded media that may include full PAN, CVV, address etc. could be a breach of PCI DSS requirements, which again might generate more fees.

To further the explanation, below are the tools available to merchants to prevent fraud in any channel:



The standard features in the face-to-face channel are well known and self-explanatory.

3D Secure and the use of the Card Verification Value (CVV) in the ecommerce channel are also well understood.

The Address Verification Service (AVS) is a service provided by major card schemes to enable merchants to authenticate ownership of a credit or debit card used by a customer in the card-not-present channel (AVS can also be used in the face-to-face channel, although this is not common/necessary in EMV Zone 1 & 2 countries). This will be included as part of **card scheme fees**, and depending on what contract a merchant has (see Merchant Services Providers Models section), merchants may not even be aware of this.

The main point to remember is that card scheme approved standard features are available that would give merchants the incentive of a liability shift in the ecommerce (3D Secure) and face-to-face (Chip, PIN, signature, visual checks) channels. No such incentives are available for the telephone channel.

For the telephone channel, equivalent protection for authentication and fraud prevention is an expense that needs to be considered carefully, as merchants can't justify this on the

basis of any liability shift. PSD2 doesn't even help with this as requirements for Strong Customer Authentication for the telephone channel still remain vague.

CONSIDERATION FOR FINAL REPORT:

For e-commerce and face-to-face merchants, card scheme approved methods (e.g. 3D Secure) are available to give them the incentive of a liability shift. For provider of 3D Secure solutions, accreditation processes are available. But merchants are not free to select any equivalent (or potentially better) authentication measures, and authentication solutions providers wanting to offer solutions in that space must work to the 3D Secure specification. **This should be examined further from a competition angle**.

For the telephone channel, merchants will not get any liability shift and are confined to use standard features (e.g. CVV, AVS), and invest in extra fraud prevention capabilities. Given current trends, **this should be examined from a financial inclusion angle**. If merchants cannot invest in extra fraud prevention capabilities in the telephone channel, this option will not be made widely available to vulnerable segments. In addition, service providers find it difficult to offer their solutions, which stifles **innovation** in this space.

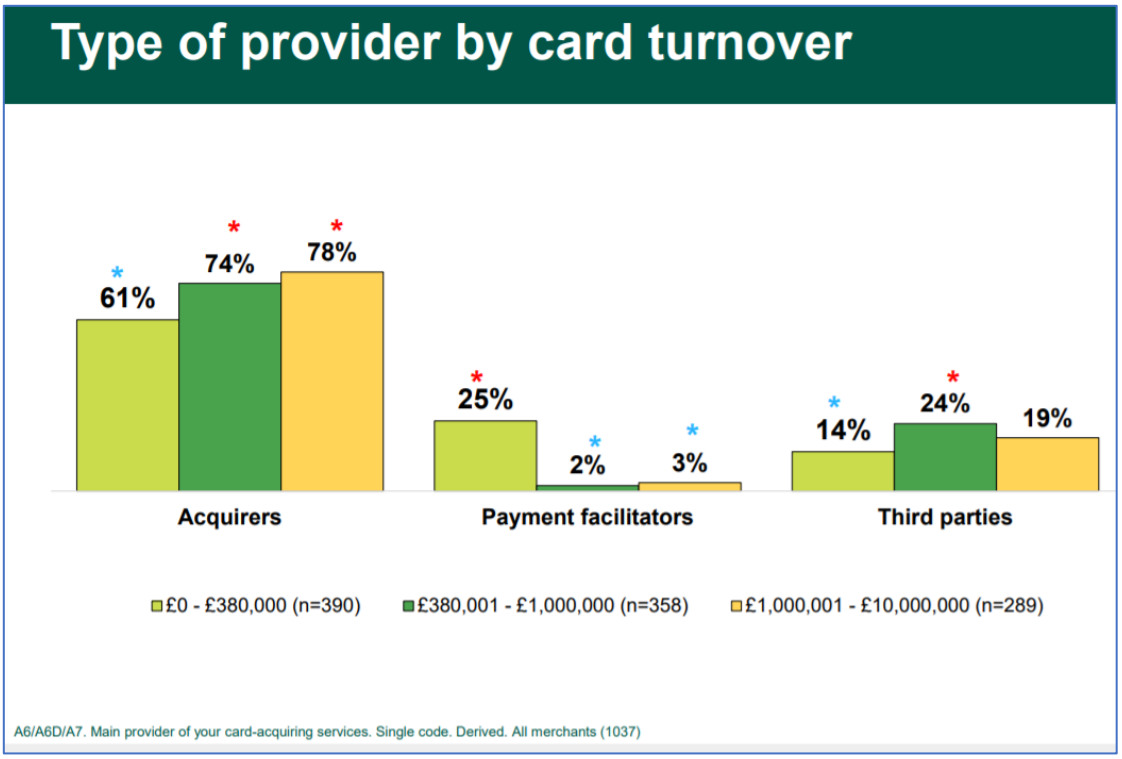
FEES & CHARGES

Understanding Fees & Charges

Understanding merchant service provider models is key to understand fees and charges levied on the various types of merchants.

The following sections will explain how fees and charges are calculated and how they apply to the various merchant models.

In the meantime, it becomes clear as to why the following diagram does not reflect a true picture of the UK market:



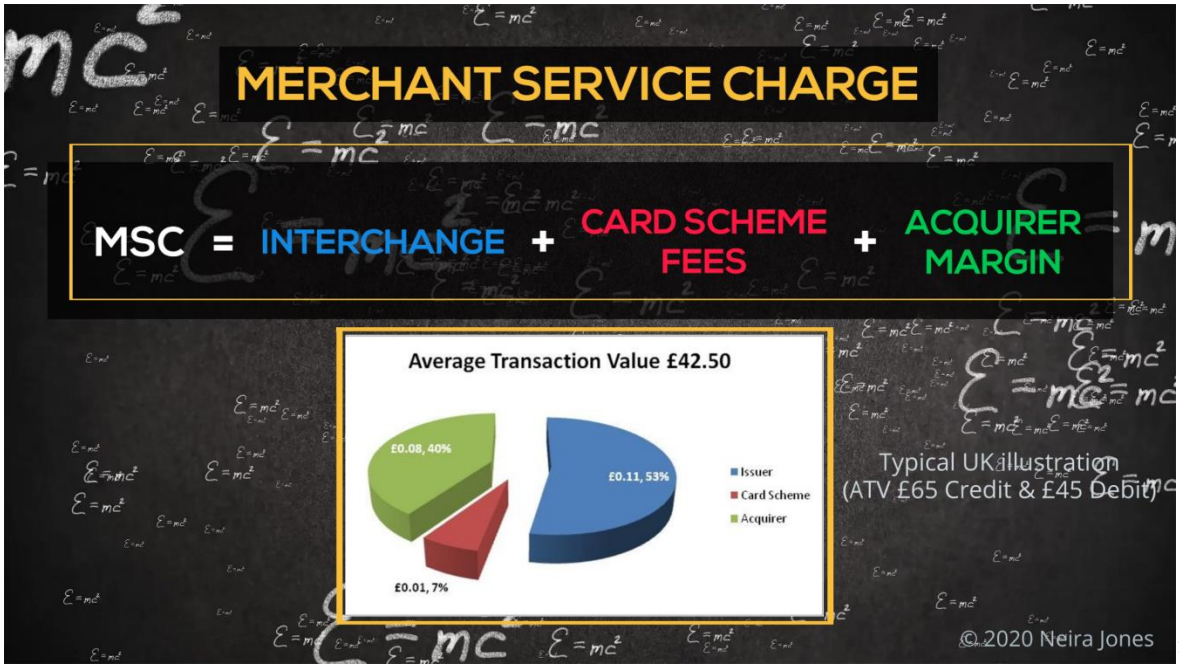
As previously mentioned, a number of factors will affect fees and charges:

- Merchant model, risk and size (transaction volume and value)
- Channel (Card Present, Card-Not-Present)
- Value-added-services (VAS) and other services
- Compliance related charges
- etc.

Typically, a merchant directly acquired by an acquirer will be charged the Merchant Service Charge (MSC) monthly for the provision of a payment facility or facilities. The merchant will also pay for other elements which will also be described in this section.

The Merchant Service Charge (MSC)

The MSC is calculated as follows:



[18]

Interchange

Interchange is a percentage of the transaction value. In the four party model, this amount flows from the acquirer to the issuer. It is the single largest cost to the acquirer. Depending on the card programme and product type, it may be the largest single income line item for issuers. Interchange rates vary depending on card type (e.g. debit, credit, consumer, commercial, etc.), channel and other factors.

Under the EU Interchange Fee Regulation (IFR), interchange is capped at 0.3% for consumer credit transactions and 0.2% for consumer debit transactions (higher rates apply for non-consumer cards).

Card Scheme Fees

These are not publicly disclosed, and they are unregulated. These can be rather obscure, and even acquirers don't completely understand the details and will generally only concentrate on items that stand out. The PSR makes some acknowledgement that these fees have gone up and it is generally accepted that they represent on average 0.03% of the transaction value, irrespective of card type.

[18] See Payments 101 – Part 2 – Card Payments Economics e-learning https://neirajones.thinkific.com/

CONSIDERATION FOR FINAL REPORT:

I recommend that the card scheme fee manuals be reviewed and understood so the final report takes into account the details and implication of these fees and see if there could be any way of simplifying them so they could be better understood by all affected parties.*

As an example, the switch to make all contactless transactions have an online authorisation introduced an additional card scheme fee. With Covid 19 and the lift in contactless limits, the card schemes will experience a massive increase in revenues from this source and merchants have no choice but to pay.

As these fees generally get passed through to merchants, this has been a major contributing factor as to why merchants saw little benefit since the Interchange Fee Regulation came into play. The interim report seems to suggests that benefits have been passed on to merchants, but at the very same time, several trade associations complained very publicly[19].

*Note 1: as an example, one type of card scheme fee is the ATM locator fee charged by MasterCard, and all acquirers have to pay it. An intriguing factor is that this fee will be charged even if an acquirer only processes ecommerce transactions as it is applied by BIN.
Note 2: Barclaycard publicly lists some of the scheme fees applied on transactions[20].

Acquirer Margin

Of course, the acquirer margin will depend on a number of factors, including the merchant's ability to negotiate. This will be explained in the next sections.

[19] https://www.bbc.co.uk/news/business-54606252

[20] https://www.barclaycard.co.uk/content/dam/barclaycard/documents/business/help-and-support/Interchange-Rates-and-Scheme-Fee-Guide.pdf

Payment Acceptance Merchant Rates

MSC = Interchange + Card Scheme Fees + Acquirer Margin

Interchange+

The merchant will see the interchange amount, and a fixed percentage will be added.

Interchange++

The merchant will see the interchange amount, the card scheme fees, and a fixed percentage will be added.

Blended or tiered

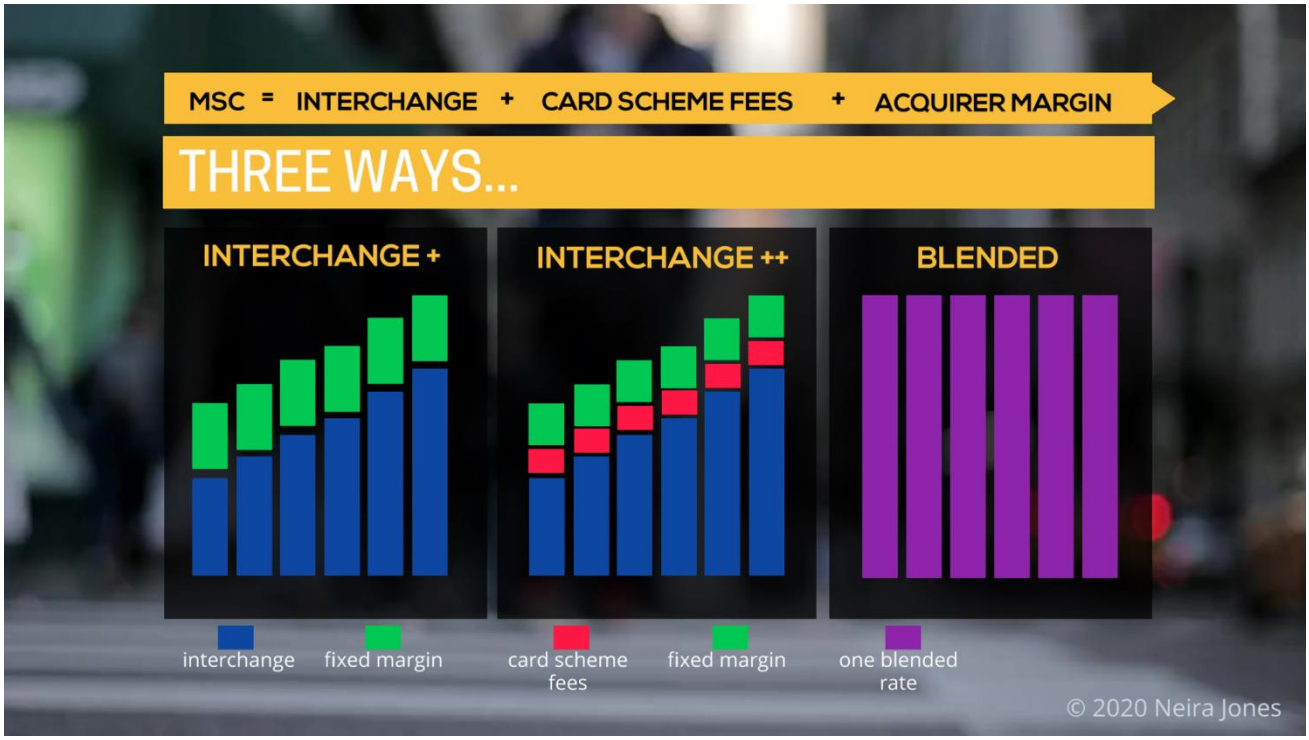
The merchant only sees one rate, with no contractual tie to interchange. This rate is generally the rate offered to SMEs, and also typically the structure used by PSPs.

The difference between rates

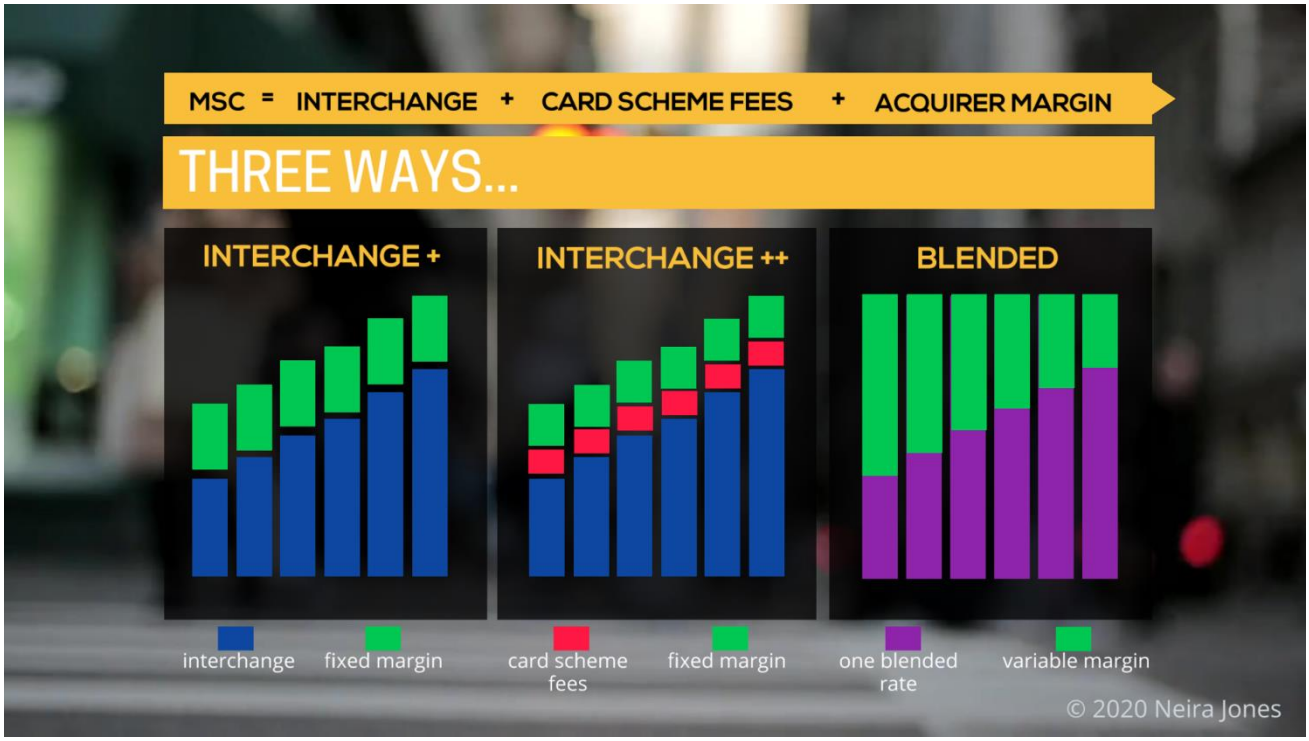
It is clear that Interchange+ and Interchange++ offer more fee transparency for merchants. These rates are reserved for the largest of merchants, who have the power to negotiate, because they bring volumes (or when they are available, it is generally not obvious for merchants to find them). These rates are generally not offered by default to SMEs, who will mostly be on a blended or tiered model (or if they are, merchants may not understand what this means to them, seemingly in direct contravention of Article 9 of the IFR[21]).

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0751

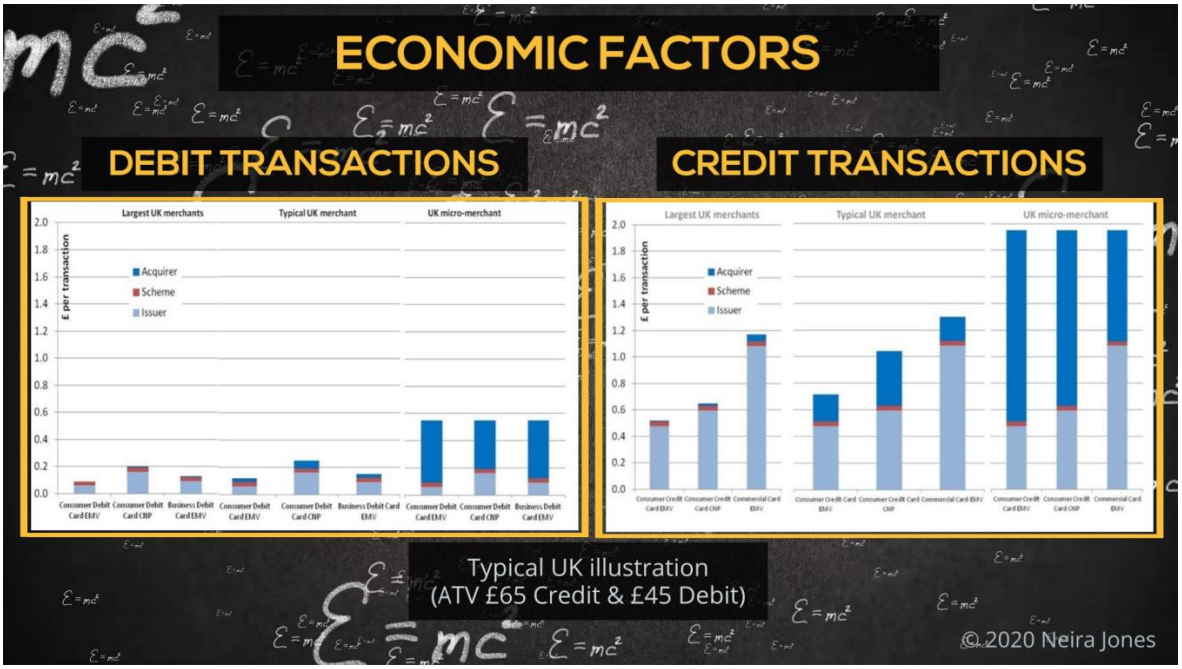
This is illustrated below:



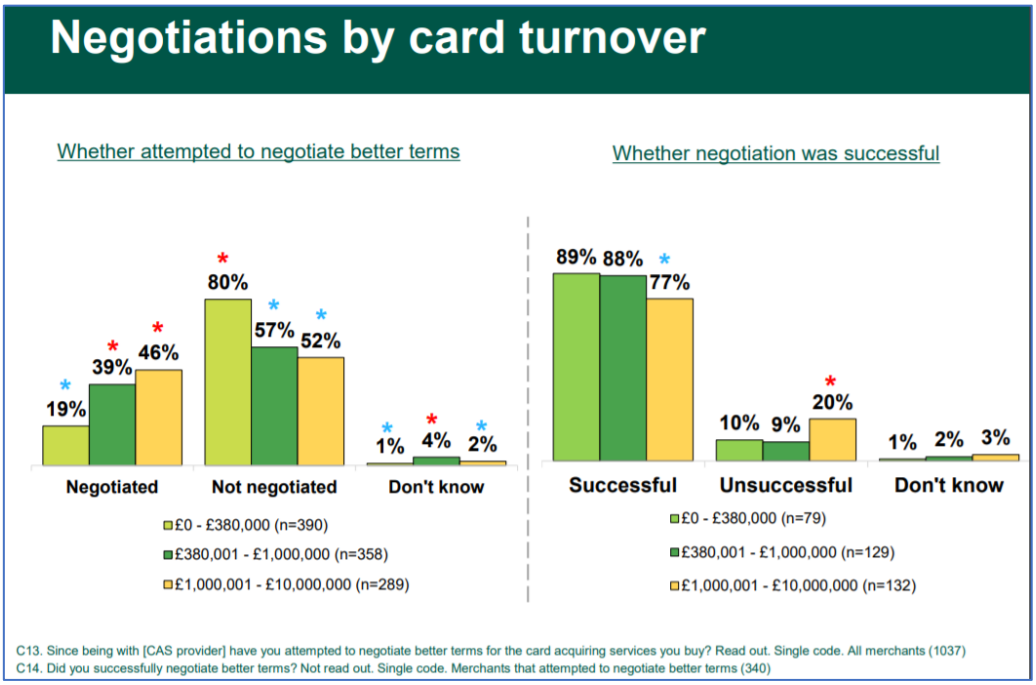
In addition, whilst for larger merchants (Interchange+ and ++), the acquirer will apply a fixed margin, for smaller merchant, because of the above model, the margin will typically be variable, as illustrated below:



This is further illustrated below, showing the different card transactions:



It is clear that when seeking merchant feedback on fees and charges, the questions must take into account the size of merchant and the commercial model used. For example, a merchant on a blended/tiered rate (who has no transparency as to margin applied) should not be asked the same questions in relation to MSC as a merchant on interchange++ (who has complete transparency and negotiating power). Consequently, the following diagram will be misinterpreted if the relevant factors are not taken into account:



In relation to the diagrams presented on the previous page, a diagram showing whether merchants' ability to negotiate depending on the type of provider would have been more helpful, but this wasn't provided in the study.

CONSIDERATION FOR FINAL REPORT:

A **merchant's ability to negotiate or switch is dependent on the commercial model used**, and therefore what type of provider has the main relationship for payment facilities. Questions related to commercial terms should not be the same for all payment facility providers as the terms can be vastly different.

In addition, taking a one-size-fits all approach will introduce **bias** in favour of larger merchants, leaving the SME segment no better than they were before.

Since this consideration was part of the Final Terms of Reference for this market review (section 3.5), it should be assessed accordingly.

Other Merchant Charges

The purpose of this section is not to present an exhaustive list of additional charges, but only the most notable ones.

Minimum Monthly Processing Fee

Typically, this is a fee that merchants will incur if they do not process a minimum level of transactions in a given month. This is a fee generally levied on small merchants by acquirers and some ISOs[22]. This fee is never levied on large merchants, for obvious reasons. (Also known as Minimum Monthly Service Charge [MMSC]).

CONSIDERATION FOR FINAL REPORT:

Monthly minimum processing fees are generally always declared, and therefore merchants entering in the commercial agreements that include it will generally do so in full knowledge.

Early Termination Fee

As the name suggests, smaller merchants may be locked into lengthy contracts because the early termination fee and notice period can be prohibitive (this wouldn't be an issue for larger merchants). This also further reduces any ability (if they have any in the first place) to negotiate.

CONSIDERATION FOR FINAL REPORT:

Early termination fees are generally always declared, but, whilst a merchant could technically terminate an acquirer agreement after 12-18 months, they might be locked in with their provider (e.g. ISO) if they have a 3-5 year terminal rental deal. This is a major source of complaints on TrustPilot[23]. I acknowledge that some remedies are suggested in the PSR Interim Review.

Set-up Fees

Set up fees, arrangement fees or joining fees are often charged for businesses that are new to cards. Years ago, these fees used to be charged as a matter of course and were typically £100 - £200. Smart business owners will negotiate them down, but others will just pay it. Some PSPs or ISOs may still have this practice. In addition, when the merchant is deemed high risk, the fees can go up a lot higher. In some instances, these fees could be refunded when the provider cannot place the business.

[22] See https://www.cardswitcher.co.uk/cheapest-merchant-services-for-small-businesses/

[23] See https://uk.trustpilot.com/review/worldpay.com?page=4&stars=1

Operational Fees

Here, the term “operational fees” is used as a catch all category reflecting that these are fees that are charged during the normal course of business. Therefore, a merchant may consider these as “operational” as they might not understand that the various fees are different in nature (e.g. a service, or a card scheme fee). They include terminal rental, payment gateway provision, chargeback fees, authorisation fees, any fees resulting from the merchant breaching any card scheme monitoring programme (e.g. excessive chargebacks, fraud to sales ratio, etc.). These fees are generally applied across the board by acquirers, regardless of merchant size.

CONSIDERATION FOR FINAL REPORT:

These types of fees are generally explained in the merchants’ Terms and Conditions. However, they may be described in very generic terms, and merchants may not realise that they could incur some of these when they sign a contract. More **transparency** and plain English should be recommended. I acknowledge that some remedies are suggested in the PSR Interim Review.

Value-Added-Services Fees

These are fees levied on merchants for the provision of VAS to enhance their payment acceptance environment (this is up-sell for an acquirer), such as mobile top-up, loyalty, dynamic currency conversion, factoring, etc.

CONSIDERATION FOR FINAL REPORT:

Merchants should be aware of these fees, as they are essentially paying for a service/product that they need or want as part of their business operations. These are generally clearly explained.

However, the provision of PCI DSS reporting portals to merchants is sometimes described as a VAS, but does not represent a value-added-service and the use of this term for that facility is misleading. (See PCI DSS FEES section).

Assessments (aka “fines”)

There are many assessments that can be levied on merchants. Technically speaking, under EU law, the term “fine” has a specific meaning and its usage could lead to regulatory issues, but for this report, we will call them “fines” as the implications for merchants are the same. These “fines” relate to any breach of card scheme operating regulations, and these terms are always included in the merchants’ terms and conditions for those that have a contract with an acquirer. For example, a merchant may suffer a payment security data breach (this is called a “data compromise”), in which case they could be liable for the following costs:

- Engagement with a forensic investigator and remediation costs
- Fines levied by the card scheme(s) on the acquirer
- Card fraud losses as claimed by the issuers affected.

CONSIDERATION FOR FINAL REPORT:

Acquirer’s discretion governs whether fines/ losses are passed on to the affected merchant (this is not something the card schemes get involved in). This generally means that those merchants that have less negotiating power (SMEs) are generally more penalised, which becomes a fairness issue.

PCI DSS Related Fees

These are fees that started appearing in the card acquiring market around 2009-2010. The state of payment security was such that the card schemes were putting increasing pressure on acquirers to drive PCI DSS compliance in their merchant portfolios. This included fines from the card schemes levied on acquirers for not meeting portfolio PCI DSS compliance thresholds. The PCI DSS related fees are complex, which is why they require a section in their own right (See PCI DSS FEES section).

CONSIDERATION FOR FINAL REPORT:

Please note that PCI DSS related fees should not be considered as a “value-added-services”. They are now essentially imposed on SMEs (these do not apply to large merchants), and should at least be investigated for transparency, purpose and fairness. Please see next section for details. In addition, PCI DSS fees are specifically included in the Final Terms of Reference of this market review, section 3.3[24], but no mention of them is made in the interim report.

[24] https://www.psr.org.uk/sites/default/files/media/PDF/PSR_MR18_1.2_card_acquiring_market_review_Final_terms_of_reference_January_2019_0.pdf

PCI DSS FEES

Introduction & History

The PCI DSS standard

The Payment Card Industry Data Security Standards has been around since 2004 to prevent card payment fraud. It is an excellent data security standard and applies to all entities that would process, store or transmit cardholder information, either electronically or manually. With the worldwide increase in digital payments, this standard was welcome (and still is). It is now a mature standard and has evolved drastically, in line with ever evolving cyber threats. We are now on version 3.2.1.

Card Schemes Operating Regulations

Compliance with the PCI DSS is clearly set out as a requirement in the card scheme operating regulations for card scheme members. This essentially means that a breach of PCI DSS requirements, as set out by the scheme via mandates (e.g. member letters), will attract an assessment fee (i.e. fine) from the card scheme on the member (e.g. an acquirer). What happens to that fine once it has been levied on a member (e.g. an acquirer) is entirely at the member's discretion.

In the early days (i.e. 2006 to 2015), the card scheme focus was on PCI DSS compliance given that PCI DSS industry compliance levels were low and fraud and data breach levels were high. As a result, the card schemes, given their role of preserving the integrity of the ecosystem, specified acquirer portfolio compliance thresholds, and deadlines by which to meet these thresholds. Failure from acquirers to meet those thresholds would attract fines.

The challenge for acquirers was to be able to manage the compliance status of their portfolios and to be able to report on that status to the card schemes. Reporting was usually done on a quarterly basis, and reporting spreadsheets were defined by the card schemes for that purpose.

Another challenge was to determine how to manage, and potentially re-distribute, the levied non-compliance fines to the merchant portfolio.

At that time however, it was clear that the justification for any re-distribution of non-compliance fines to the merchant portfolio (or part thereof) was on the basis of non-compliance fines that were levied on the acquirer by the card scheme.

Merchant Levels

An acquirer's merchant portfolio is categorised by "Merchant Levels". These are based on transaction volumes, not value. These are broadly defined below:

- Level 1: the largest merchants (more than 6 million transactions per year per scheme)
- Level 2: large merchants (between 1 and 6 million transactions per year per scheme)
- Level 3: large-medium ecommerce merchants (20,000 to 1 million)
- Level 4: small merchants (less than 20,000 ecommerce and up to 1 million transactions for all other merchants)

The compliance requirements by merchant levels are explained in Appendix 1: Merchant Validation Requirements.

The Acquirer Response

In order to fulfil the **compliance reporting requirement** imposed by the card schemes, and to avoid fines, acquirers needed to implement processes and systems. Smaller acquirers would manage this (if at all) through spreadsheets. Larger acquirers, with many thousands of merchants, deployed "PCI DSS Compliance Portals" as provided by suppliers such as Security Metrics, Trustwave, Sysnet, etc.

These industry compliance portals were specifically targeted at Level 4 merchants (i.e. SMEs) and essentially replicate the paper Self-Assessment Questionnaire (SAQ) in a digital form, as well as offering vulnerability scans for e-commerce merchants (where required).

Please take some time to look at https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-B.pdf for the simplest of these SAQs (SAQ B), which typically applies to small face-to-face merchants. It is apparent, when reading this SAQ, why small merchants would find it difficult to complete, whether on paper or digitally. The intention was that the PCI DSS compliance portals would enable acquirers to present a reflection of the compliance status of their merchant portfolio.

The way that acquirers managed the compliance of larger merchants (Levels 1, 2 and 3) varied across the board, generally either through spreadsheets or end-user technologies such as MS SharePoint.

Merchant Terms & Conditions

In order to cater for the usage of these portals, specific PCI DSS compliance clauses were introduced into merchants' Terms & Conditions.

Why and How the Fees were Introduced

Between 2006 and 2010, as PCI DSS compliance figures stagnated and fraud levels were high, most acquirers decided to introduce “Non-Compliance Fees”, ramped up communications with merchants (via call centres and other means), to encourage them to become compliant and avoid the fees (and supposedly decrease the risk in their portfolio).

CONSIDERATION FOR FINAL REPORT:

PCI DSS became a major source of complaints for all acquirers, and was monitored at the highest level. These complaints ranged from not knowing who the call came from (when contacted directly by the compliance portal provider as part of the chasing activity), to not getting any help as to how to complete the SAQs, and of course complaining about the non-compliance fees, which they couldn’t avoid since they were included in their terms and conditions. This resulted with merchants at best ticking boxes just to make it go away (thus defeating the original objective of getting a handle on compliance), and at worst not doing anything and seeing the fees pile up.

It has been long acknowledged in the industry that PCI DSS non-compliance fees have not achieved the objective they were supposed to fulfil.

The following report from Sysnet's 2nd Annual Acquirer PCI Sentiment Survey[25] says it all:

Key Findings

Similar to last year, the majority of respondents agree that small merchants are not effectively engaging with PCI programs: many respondents believe that this is a result of a lack of knowledge of how to engage, a lack of understanding as to why they should engage, not knowing they need to engage and also a lack of time to do so. The stand out findings from this year's survey are as follows;

70%+

Acquirers expectations regarding the compliance rate for their small and medium-sized merchant is rising. This year 93% of respondents indicated 70%+ to be an acceptable rate of compliance compared to 84% in last year's survey.

93%

of respondents are uncomfortable with their current compliance rate and would like it to be higher.

89%

of respondents agree that merchants struggle to understand which security tools they need to ensure their business and customer information is protected.

86%

of respondents agree that PCI non-compliance fees should not be charged for any longer than 24 months. 11% of those feel it is never appropriate to charge non-compliance fees, down on last years' 21%. Just 14% indicated that it is acceptable to charge non-compliance fees indefinitely, down from last year's 21%.

59%

of respondents consider adding merchants to a managed compliance service to be the most viable alternative to charging non-compliance fees. Other options include threat of termination (19%), and withholding funds (16%).

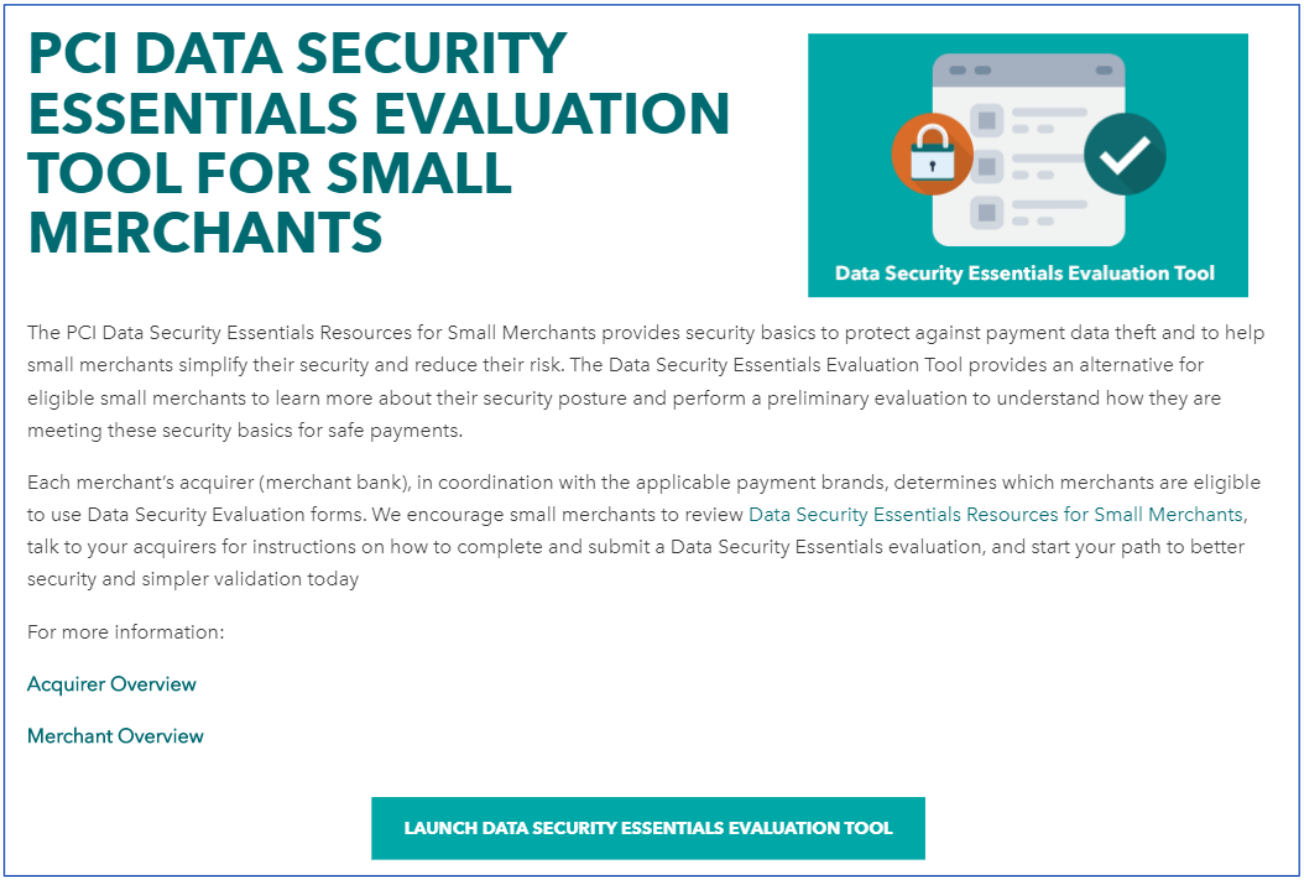
72%

of respondents agree that PCI non-compliance fee revenue is an income the industry needs to wean itself off, this is up 20% on last year's survey findings.

[25] https://sysnetgs.com/blocks/2nd-annual-acquirer-pci-sentiment-survey-home-banner-block/2nd-annual-acquirer-pci-sentiment-survey-ebook-image/

As compliance figures were still stagnating, the PCI Security Standards Council (PCI SSC, the industry body responsible for the development of the standard) and the card schemes decided to try a different approach. The fundamental principal of the approaches was to try and **get a handle on the risks posed by merchants by the way they deploy their payments infrastructure**. Notable initiatives include:

- In August 2018, the PCI SSC launched the **PCI Data Security Essentials Evaluation Tool for Small Merchants**[26], simplifying PCI DSS self-assessment by providing an easy to use visual tool, with plain English explanations and clearly highlighted risk factors.



To date, no acquirer, to my knowledge, has communicated to their Level 4 (SME) merchants regarding the availability of this simplified tool and the merchants eligibility to use it. If these initiatives were implemented, PCI fees should largely fall by default.

- In October 2018, **Mastercard** launched their **PCI DSS Validation Exemption Program for Eligible Merchants Using Secure Technologies**[27]. Similarly, to my knowledge, no acquirer has communicated with merchants in respect to this tool.

[26] https://www.pcisecuritystandards.org/pci_security/small_merchant_tool_resources

[27] https://globalrisk.mastercard.com/wp-content/uploads/2018/10/PCI-Validation-Exemption-Program.pdf

In addition, in 2015, the **card schemes revisited their approach and decided to focus on portfolio risk rather than non-compliance**. Notable facts include:

- **Non-compliance portfolio fines removed** by card schemes on acquirers (effective 31st October 2015)
- **Quarterly reporting reduced and new targets set**. For acquirers not meeting thresholds, card scheme would require a remediation plan, and would potentially conduct an audit on the acquirer.
- **Data breach fine structure revisited** according to the knowledge the acquirer has on the merchant and their compliance status at the time of the breach (e.g. penalty reductions of between 25% and 100% in favour of acquirers will be applied based on self-notification of a breach and the PCI DSS compliance of the merchant). The intention here was to let acquirers manage the risk in their portfolio in a more flexible way, and this was welcomed by the industry.

CONSIDERATION FOR FINAL REPORT:

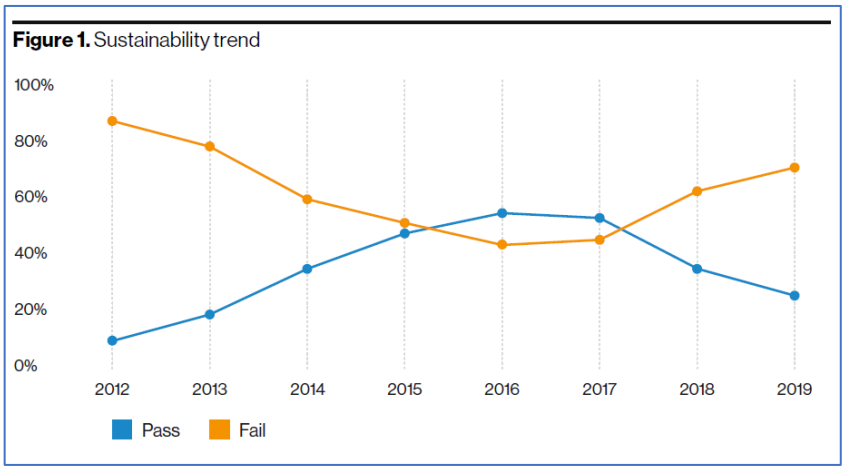
The original reason for levying non-compliance fines on small merchants (passing on PCI DSS card scheme portfolio non-compliance fines) **no longer exists**. Therefore, the purpose of these fees should be examined carefully. There are many ways merchants are charged for the risks they may bring to the ecosystem (see Merchant Services Providers Models and FEES & CHARGES), and remediation mechanisms are well understood. For cyber-risk (essentially payment security risk), fees should only be charged if it can be demonstrated that the risks are understood and that merchants can actually remediate them.

Some acquirers may argue that they deliver a service to their merchants for providing them with a portal to attest to their compliance. **The provision of a portal to attest to compliance is not a "service"**, it is solely for the benefit of the acquirer to fulfil their card scheme reporting obligations. Some acquirers, realising this, created enhanced offerings including further security products to help their Level 4 merchants towards compliance. The low take-up of these services suggests that merchants, as expected, do not understand these products.

Some acquirers deployed premium security products for SMEs (e.g. managed security services), to be used if they failed to meet certain compliance threshold. **Enrolment of merchants on these products should be investigated to determine whether they have given their consent to their purchase and are indeed able to use them**.

Alternative and easier methods for PCI DSS compliance validation have been available for a few years. The reasons why these methods have never been offered to merchants by acquirers should also be investigated.

Furthermore, the recent **Verizon 2020 Payment Security Report** highlights the following PCI DSS compliance trend:



This represents a systemic failure in PCI DSS compliance management, and clearly highlights that PCI DSS fines are not working.

These fees represent a **substantial amount of revenue for acquirers which can run into tens of millions of pounds per annum.**

The compliance (or non-compliance) trends above suggest that this revenue can only increase. Perversely, from a commercial point of view, **it is in the interest of acquirers who charge fees that their merchants remain non-compliant**. This however doesn't mean that 100% of non-compliant merchants present a risk to the ecosystem.

Further considerations:

- There is no evidence that PCI DSS fees (other than those related to data breaches) are ever levied on large merchants (Levels 1 and 2).
- Some acquirers also include Level 3 merchants in their compliance programmes.
- In some instances, **the total of PCI DSS related fees can amount to a higher amount than that paid for the card acquiring services themselves.**

CONSIDERATION FOR FINAL REPORT:

The FCA stated their objective[28] to "ensure fair treatment for consumers and small firms - making sure that firms give strong and clear support to customers, recognising challenges that everyone is facing".

In relation to PCI DSS related fees, **transparency and fairness should be investigated** thoroughly, as merchants of different sizes are treated differently. This could also be in breach of related regulations[29].

[28] https://www.fca.org.uk/news/press-releases/fca-sets-out-priorities-2020-21

[29] https://www.fca.org.uk/firms/fair-treatment-customers

Types of Fees

Since card schemes removed portfolio non-compliance fines, some acquirers started renaming the non-compliance fees as "admin/programme fees" or similar. It is however fair to say that there will be broadly speaking three types of fees: those related to non-compliance, those related to usage of the portal, and those related to security products.

Some examples are given below:

Acquirer	Public Information	Comments
Barclaycard	https://www.barclaycard.co.uk/business/help-and-support/accepting-payments/security-help/pci-dss/pci-dss-faqs https://www.barclaycard.co.uk/business/help-and-support/accepting-payments/security-help/pci-dss/becoming-compliant	It is known that programme fees are £4.80pcm (or £15 for the premium portal), non-compliance fee £25pcm, all per merchant ID. The fees for vulnerability scans are not listed.
WorldPay	(it is difficult to find these fees listed online with only the lowest fees published on the website, making it difficult for merchants to compare) website: https://www.fisglobal.com/en-gb/merchant-solutions-worldpay/products/safer-payments	It is known that programme fees are £5pcm (or £12 for the premium portal), non-compliance fee £15pcm, all per merchant ID. Vulnerability scans are £35pcm where applicable.
Global Payments	(it is difficult to find these fees listed online with only the lowest fees published on the website, making it difficult for merchants to compare) website: https://cdn-gx.dataweavers.io/-/media/global-payments/uk-new-images/globalfortress/global_fortress_sales_sheet.pdf (only the £3.50 fee is mentioned) Old reprice letter (minimum fee is now £75 instead of £50) https://www.globalpaymentsinc.com/-/media/global-payments/files/uk-migration/resource-center-uk/card-processing/globalpayments_know_the_risks.pdf?la=en-gb	Minimum £75pcm irrespective of turnover and 15p/transaction if 500+ transactions pcm), all charged per MID. The fees for vulnerability scans are not listed. Please note that Global Payments typically charge 5 times as much as the two biggest acquirers, whereas portfolio risk is broadly the same.

Acquirer	Public Information	Comments
Fiserv	Merchant agreement: https://www.firstdata.com/downloads/pdf/en_gb/First_Data_Merchant_Conditions.pdf website (no mention of fees): https://www.firstdata.com/en_gb/products/small-business/all-solutions/pci-dss-compliance.html	Non-compliance fee £35pcm, per merchant ID. Other fees are not listed.
Lloyds Cardnet	website: https://www.lloydsbankcardnet.com/Content/pdf/pci-dss-update.pdf	Programme fees are £5.50pcm (or £15 for the premium portal), non-compliance fee £20pcm, all per merchant ID. The fees for vulnerability scans are not listed.
Elavon	website (no fees are mentioned): https://www.elavon.co.uk/solutions/security-and-pci-compliance/security.html Statement explainer (only best case presented): https://www.elavon.co.uk/content/dam/elavon/en-gb/documents/customer-centre/setting-up-your-account/Understanding_Your_Statement_vs2.pdf	Unable to find fees information

Some ISOs will also charge PCI DSS related fees:

- **PaymentSense** https://support.paymentsense.com/hc/en-us/articles/201239471-What-is-PCI-compliance-and-why-does-it-matter-

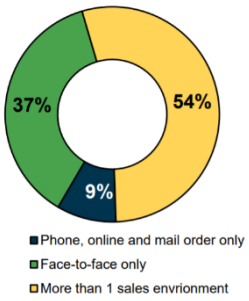
Some ISOs leave that to the acquirers:

- **RMS**: https://www.retailmerchantservices.co.uk/help-support/support-detail-pages/pci-compliance/how-do-i-become-compliant/

To my knowledge no payment facilitators, other merchant aggregators or merchants of records charge any PCI DSS related fees. This beggars the question as to why new entrants and smaller players see no need to charge these fees, yet the established players with the greatest knowledge and extensive resources do.

CONSIDERATION FOR FINAL REPORT:

It is fair to say that acquirers roughly charge similar levels of fees, with the notable exception of Global Payments who are substantially more expensive.



It also must be understood that the charges stated are levied per merchant ID (MID).

This means there will be a **multiplier effect** if a merchant operates in more than one sales environment (i.e. each channel requires at least one separate MID, and PCI DSS fees are applied per MID).

Even confining ourselves to the PSR study data, this will affect 54% of the merchants that replied to the survey.

From the data on the previous pages, it will be apparent that, with the exception of Barclaycard, **there is a general lack of transparency in terms of PCI DSS related fees**. If I can't find them (and I know where to look), what chances do merchants have?

Whether such fees should be applied in the first place, and the conditions under which they could be legitimately applied should also be reviewed.

FURTHER CONSIDERATIONS

Underwriting

The Final Terms of Reference highlight Barriers to entry (sections 3.7 and subsequent of the original terms of reference) as an area in scope of the study.

It is a well understood fact that the time is takes to obtain payment facilities varies widely depending on the type of provider selected.

For example, getting a merchant account directly from an acquirer can take weeks, whereas getting a payment facility from a payment facilitator or aggregators can take less than an hour. This is primarily due to the structure of the commercial agreements explained in the previous sections.

However, there are some underwriting practices that are worthy of further examination.

For example, there has been an increased popularity of digital banks business accounts amongst the SME population because these seem to be more flexible and certainly more efficient than traditional incumbent banks.

However, SMEs (level 4 and level 3 merchants) seem to be penalised at underwriting stage because they use a digital only bank, such as Starling Bank or Monzo, as they are asked to provide substantially more information than those banking with traditional high street banks. Examples of extra information required include:

- Exterior photos of business premises
- Photos of stock
- Invoices for stock
- Advertising/social media links
- Order book, etc.

CONSIDERATION FOR FINAL REPORT:

Generally, **digital banks are classified as "high risk" by some acquirers**. Because digital banks have more efficient underwriting processes shouldn't mean that their business customers should be penalised for using them. Digital banks are regulated by the FCA just like any other bank and the practice of penalising their customers should be investigated.

In addition, **collateral requirements and settlement periods** should be further examined for consistency, fairness and competition.

GDPR Compliance

Whilst not directly related to the provision of card acquiring services, it should be noted that some providers include the implied consent to their privacy policy in their Merchant Service Agreement. This is a breach of the General Data Protection regulation, which specifies that consent to a privacy policy should be separate from any other consent given[30].

[30] https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/general/merchant-services-agreement-standard-tscs.pdf?la=en-gb

CONCLUSION

Given the PSR's remit around improving **competition**, supporting **innovation** and **promoting end user interests** in payment systems a thorough review of the card market is welcomed. Reenforcing why the supply of card acquiring services is important to the economy and identifying what the industry and regulators need to do to ensure an effective market is key.

The card payments ecosystem is a complex one. In my response, I have taken great care to present an unbiased view of the card acquiring market and all references are from public sources. My aim is to highlight the issues that SMEs face in our constantly evolving and challenging world. It is my belief that the regulators are ideally placed to help them achieve better outcomes, ultimately to the benefits of the end customer. I also wish to highlight the challenges that other ecosystem players (e.g. PSPs, acquirers, issuers, schemes) are faced with, with the intention to advocate for more transparency in an ecosystem that is so fundamental to the economy.

This document provides a list of clear recommendations (highlighted in grey throughout) after the various problem statements and explanations. I appreciate that, bearing in mind the amount of change that is happening within the industry, any regulatory intervention has to be proportionate and prioritised appropriately. But it also needs to recognise that accelerating societal change is changing the shape of the market currently dominated by cards.

With this in mind, the PSR may wish to consider **establishing a working group of experts** to help prioritise and establish a plan of activities to implement findings of the current review and to monitor the need for further action. I would be delighted to help.

I hope you find this report of use, and I remain at your disposal should you have any further queries.

Neira Jones

December 2020

neira.jones@phoenixedge.co.uk

ACKNOWLEDGEMENTS

My sincere thanks go to the following people, who have freely given their time and expertise to review this document, and helped me make the final version as digestible and valuable as I hope it to be:

Tony Craddock, Director General, Emerging Payments Association emergingpayments.org

Andrea Dunlop, Co-Founder InvestFem investfem.com

Anne Pieckielon, Independent

Ian Rutland, Managing Director, TwentyTwenty Payments Ltd

Gert Scholts, Managing Director, The Best Sales Coach

Nigel Tanner, CEO Blue Scorpion Limited www.bluescorpion.co.uk

Appendix 1: Merchant Validation Requirements

MERCHANT LEVEL	CRITERIA	VALIDATION REQUIREMENTS
LEVEL 1	(1). Any merchant, regardless of acceptance channel, processing more than 6,000,000 Visa transactions per year. (2). Any merchant that has had a data breach or attack that resulted in an account data compromise. (3). Any merchant identified by any card scheme as Level 1.	(1). Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") – also commonly known as a Level 1 onsite assessment – or internal auditor if signed by officer of the company. (2). Quarterly network scan by Approved Scan Vendor ("ASV"). (3). Attestation of Compliance Form
LEVEL 2	1 million – 6 million Visa or MasterCard transactions annually (all channels).	(1). Annual Self-Assessment Questionnaire ("SAQ"). (2). Quarterly network scan by ASV. (3). Attestation of Compliance Form.
LEVEL 3	Merchants processing 20,000 to 1 million Visa or MasterCard e-commerce transactions annually	(1). Annual Self-Assessment Questionnaire ("SAQ"). (2). Quarterly network scan by ASV. (3). Attestation of Compliance Form.
LEVEL 4	Less than 20,000 Visa or MasterCard e-commerce transactions annually, and all other merchants processing up to 1 million Visa or MasterCard transactions annually.	(1). Annual Self-Assessment Questionnaire ("SAQ"). (2). Quarterly network scan by ASV. (3). Attestation of Compliance Form. **Note: Ultimately, compliance validation requirements are set by the acquirer.**