MERCHANT ADVISORY GROUP ®
4248 Park Glen Road
Minneapolis, MN 55416
952.928.4648
merchantadvisorygroup.org

January 25, 2016

Mr. Robert deV. Frierson
Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue N.W.
Washington, DC 20551.

Submitted via email at regs.comments@federalreserve.gov
OMB Control # 7100-0351

Re: Federal Reserve Payments Study – Surveys FR 3066a, 3066b, and 3066d (80 FR 73760)

The Merchant Advisory Group (MAG)® greatly appreciates the opportunity to provide comments on the collection surveys for the triennial Federal Reserve Payments Study. The study is a tremendous tool for capturing United States payment trends, and we are pleased to see the collection surveys indicate more focus on gathering payments-related fraud and security information.

By way of background, the Merchant Advisory Group (MAG) was founded in 2008 by a small visionary group of merchants in the payments field dedicated to driving positive change in payments through multi-stakeholder collaboration. Today, the MAG represents over 100 of the largest U.S. merchants who account for nearly $2.6 Trillion in annual sales at over 430,000 locations across the U.S. and online. Roughly $1.5 Trillion

of those sales are electronic representing over 41 Billion card payments. MAG members employ nearly 11.5 million associates.

First, we would like to express a willingness from the merchant community to work with the Federal Reserve on 3066d ad-hoc Retail Payments Survey Supplement now and in the future.

Second, we would like to briefly comment on 3066a - The Depository and Financial Institutions Payments Survey. We would encourage the Federal Reserve to add a "Near Real-Time" line item under #12.a in the ACH payments section as that is the true direction the U.S. needs to be heading to remain competitive with the rest of the world in ACH payments. Under the General-Purpose and Debit Prepaid section, we would encourage the addition of a question related to items #3 and #4 regarding whether or not regulated debit cards provide at least two accessible routing options for every mobile wallet into which they are provisioned. Lastly, it seems the instructions could be a bit clearer under the final section – Unauthorized Third Party Payment Card Fraud – especially as it pertains to signature card losses. For example, it is unclear how issuers should account for unresolved chargebacks between the merchant and issuer.

Third, we would like to focus the majority of our comments on survey form 3066b. MAG would highlight and recommend the following items for further consideration:

In the General-purpose credit card transactions section:

In general, collecting additional information on fraud will help shed more light on the current fraud landscape in the United States. This is particularly important following the migration to EMV as any overall reduction in U.S. related payment card fraud, should lead to a reduction in the 5 basis points allowance on regulated debit interchange rates, and should result in a decrease in the fraud prevention adjustment, especially with the estimated costs of investment in EMV being roughly one to four for issuers and merchants respectively.

Under question #2, we would encourage the Federal Reserve to add a data point to capture net chargebacks. In other words, more detailed information on the number, value, and percentage of issuer-won chargebacks would be valuable information, especially given the recent EMV transition, which shifts counterfeit liability toward merchants who have not activated EMV card acceptance at their terminals. MAG is very concerned issuers may be inappropriately initiating EMV chargeback reason codes, and that card networks are refusing to mitigate such erroneous behavior. The Fed may even consider expanding the question to include a stand-alone section on EMV chargebacks. For example, some of our merchants have seen EMV counterfeit chargebacks outside at their fuel pumps even though the liability shift date for those transactions is not until October 2017.

Under question #4, we are pleased to see the Federal Reserve using new terminology by saying "person" present instead of card present. Card-present and Card-not-present (CP & CNP) paradigms are shifting, as they should. MAG does not believe the existing labels, rates, or liability structures are appropriate given the advent of mobile and e-commerce where there are much better security tools and mechanisms available to authenticate transactions well beyond the capacity of magnetic stripe credit cards. As the Federal Reserve is likely aware, merchants bear the vast majority of all card-not-present fraud losses while also paying a premium in fees to process those transactions. It is vital that the study look both at how authentication is advancing, and also provide a window into ways the existing assignment of liability might be preventing further enhancements from coming to market.

Under question 4b.2.a, we would encourage the Federal Reserve to omit the reference to "via 3-D Secure," and/or further breakout the category to include: authenticated via 3DS, PIN, biometrics, and other vs. not authenticated at all. The 3-D Secure platform is only one of a handful of platforms that enables authentication on e-commerce transactions. The Pay Secure platform is another example of an online authentication tool. This platform uses PIN authentication online so perhaps PIN should be considered as another subset of e-commerce authentication methods included in the survey.

4248 Park Glen Road, Minneapolis, MN 55416
952.928.4648

Under question 4b, we would also recommend line-items for collecting data on In-App wallet purchase, as well as clarification on how an e-commerce purchase that's initiated online, but picked up in the store would be classified for purposes of the data collection survey.

Under question #5, we believe perhaps there should be some additional definition of "tokenized" payment. If the survey is intended only to collect data on a "payment token," which is the type of token supported by the EMVCo back-end solution to some of the new digital wallets, then that should perhaps be specified. Within that tokenization scheme, it would be helpful to delineate who is managing tokenization within the transaction (e.g. global network, domestic network, issuer, acquirer) as we have significant concerns the system is relatively closed to most parties outside of global payment card brands. Further, it would be useful to know whether the tokenization in use is "persistent" (meaning the same token is used for multiple transactions, or indefinitely) or "dynamic" (meaning a new token is generated for each transaction).

Separately, merchants work with our acquiring partners to deploy more extensive and product-inclusive tokenization systems for our internal systems, as well as payment transactions. Some of the acquirer tokenization solutions may look different to the bank than the "payment tokens" using the EMVCo payment tokenization process. The 3rd party acquirer solutions may also be more secure.

Under question 7.e, we would strongly encourage the Fed to break out counterfeit fraud into two subsections – one for card-present or person-present and one for card-not-present or person-not-present. This is a particularly important data point for an unbiased 3rd party to collect so that stakeholders can benchmark and evaluate how the EMV migration in the US impacts counterfeit fraud in different channels since EMV is rather limited in the type of fraud it protects against.

Under question #16, we are extremely supportive of the survey collecting the number and value of smaller dollar sales increments. We believe this is critically important as consumers continue to switch away from cash and other tender types toward electronic payments. This is even more critical in the debit card space where the dominant global card networks have greatly increased debit card fees beyond a reasonable and

proportional level even with the Federal Reserve's regulations in place. Our hope is that the Federal Reserve Board of Governors may utilize some of this data to recognize the need to lower the maximum allowable interchange transaction fee on debit cards as outlined in their existing rules pertaining to Section 920 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Under question #19, we might suggest adding a line item for cards that have been provisioned to multiple wallets. For example, I may have my credit card set-up in both ApplePay and CurrentC through the same hand-held device. This is particularly important for the Private Label Credits cards survey (Question #17 on pg. 11) because of numerous challenges merchants have reported in getting private label cards provisioned to certain mobile wallets.

Under question #20, we would suggest some clarification as to whether or not the question is referring to a terminal that they have deployed as an acquirer or a terminal where they have seen their cards used.

The majority of comments in this section also apply to the debit card section and the private label section.

Under the Private Label section:

We would encourage question #16 on chip card technology to include active cards broken down by how many cards have been issued with a multi-factor authentication mechanism (e.g. PIN) enabled on the product.

Under the EBT section:

We feel that gathering this data is very important as many of the programs continue to become modernized with some (i.e. SNAP) having regulatory authority to explore options for delivering the program through online/e-commerce channels. Since PIN customer authentication is required for SNAP and many other EBT program transactions, data will provide very interesting insight for policymakers going forward as

to how well multi-factor authentication works in deterring fraud both in-store and online.

We would suggest breaking out customer verification methods as separate line items in the majority of this data collection as different programs may have different authentication parameters and fraud landscapes, especially based on how funds are accessed (e.g. cash withdrawals vs. defined program packages vs. broader program qualified packages).

Under the Mobile Wallet section:

First, we believe the section could use clarity in the definition of a "remote" mobile commerce transaction. This is similar to our earlier comment that the survey could be clearer as to how in-store pick-up or some delivery environments should be categorized. For example, I may order pizza online through a mobile application and initiate a pre-authorization on a credit card for that sale, but I may actually pay in a different tender when I arrive at the restaurant for pick-up.

Additionally, we would suggest breaking out fraud into person-present mobile transactions, and person-not-present mobile commerce transactions. As with current CNP e-commerce dynamics, there are several security tools available in a mobile environment that should help reduce fraud losses and change current liability and fee dynamics, which are at a premium for merchants in the CNP space despite merchants' own significant fraud prevention investments for online and mobile environment.

We would recommend breaking out a fraud category to try to capture data on fraudulently provisioned card accounts.

Lastly, we would encourage the Federal Reserve to do a Mobile Wallet supplement survey annually for the next few years given the rapid growth and progress in the mobile wallet provider space, as well as the need for a third-party to gather data on the mobile commerce landscape and various technology providers.

Conclusion:

Thank you again for the opportunity to submit feedback on the data collection survey process. MAG is very grateful for the work the Federal Reserve puts into collecting detailed payment information trends as it provides tremendous value to U.S. businesses. We look forward to working with you all in the future.

Please do not hesitate to contact me at liz.garner@merchantadvisorygroup.org or at 202-488-1558 with any follow-up questions or concerns.

Sincerely,

/s/

Liz Garner
Vice President
Merchant Advisory Group