	Best Practice:	Why is it important?	Priority	Timeline
	Fundamentals:			
F.1	Consistently engage merchants in concept phase for new rules and technologies.	Networks and issuers that allow meaningful merchant participation in business plans and policy decisions will ensure a mutually agreeable customer experience, adequate time to market, equitable sharing of investment and risk, and adequate competition are achieved.	High	Near Term
F.2	Process reversals & release open-to-buy holds in real-time.	Merchants typically submit real-time credits to cardholders who return items purchased previously as well as for voided and cancelled sales. Merchants need issuers to process these credits on a real-time basis in order for the cardholder to continue shopping. This is a critical customer service issue for merchants.	High	Near Term
F.3	Implement a standard lead time between an acquirer-to-merchant implementation of spec changes to allow sufficient time for merchant implementations. Ideally, this would include a 3-month stakeholders feedback period (inclusive of merchants) of future network spec changes followed by a 6-month lead time for acquirer compliance and a 12-month lead time for merchant compliance based on the date final (postfeedback) requirements are formally announced.	Merchants desire consistent and adequate timelines to incorporate technical, operational, and other business changes into their environments for payments which compete for funding and resources with other incremental profit initiatives. There is an understanding some changes may require a faster timeline while others may require longer timelines. However, the intent is to provide consistency among the networks and reasonable expectations. Merchants have capital planning and project timelines for internal business efforts that cannot just be superceded because of a timeline that is communicated without adequate time to factor into the overall business/techincal implications for the merchant community	High	Near Term
F.4	Ensure stakeholder investments in effective fraud prevention tools are factored into liability rules.	Merchants invest heavily in fraud mitigation tools (EMV for face-to-face and 3rd party fraud tool for digital commerce) and practices, yet merchants bear the greatest amount of risk with regards to liability shift rules especially in the case of digital commerce transactions (traditionally 100% liability to merchant). In addition, the merchant pays higher transaction fees for digital commerce transactions where they incur higher ongoing costs of acceptance, despite their investments in fraud prevention. This best practice is foundational to ensure that costs and risks are balanced among stakeholders.	High	Med-Long Term

	Best Practice:	Why is it important?	Priority	Timeline
F.5	Ensure all stakeholders have equal participation on all new or changed industry standards which will become binding for US payments. This would include both participation in working groups discussions.	Card brands and issuers need to allow meaningful merchant participation in brand and issuer-led organizations such as PCI, EMVCo, and NACHA to ensure merchant input is taken into account on important updates to payments standards.	High	Long Term
F.6	Support rules regarding authorizations for split shipments that are consistent across networks to improve the customer experience.	The networks have differing requirements for how split shipments are handled in the authorization and settlement transactions. Consistency across networks would simplify merchant development and support processes and improve the customer experience.	Medium	Near Term
F.7	Implement Network Quarterly Updates.	Offering timely and direct access of coming changes to network rules, programs, and requirements will enable merchants the opportunity to be informed and take action sooner than the current acquirer pass-thru model.	Low	Near Term
F.8	Ensure no merchant is inhibited from requiring the entry of any form of multi-factor authentication (i.e. PIN or password) enabled on a financial account product.	PIN entry is an effective means of verifying cardholders especially for high-value high-risk transactions, but some networks feel that requiring a PIN causes undue friction, consumers cannot remember PINs for multiple credit cards. However, the volume of PIN fraud compared to Signature based fraud proves PIN is more effective at customer authentication.	Low	Near Term
F.9	Develop a better and consistent process for EMV certification that is more efficient and effective.	There are varied test cases by network for EMV certification that do not always identify coding issues or are interpreted by acquirers differently yet the risk upon deployment after “successful” certification is passed to the merchant for such issues or misinterpretations. Merchants should have some level of confidence and protections with large-scale deployments of payment technologies such as EMV. Additionally, there are longer-term technical changes that would streamline the EMV certification process. As one example, each network has their own kernel for EMV with various expiration dates. A single kernel would streamline certification across all networks reducing costs to the merchant, acquirer, and overall ecosystem.	Low	Med-Long Term

	Best Practice:	Why is it important?	Priority	Timeline
F.10	Ensure issuers are required to enable multi-factor authentication on payment products for larger transactions, unattended terminals and AFDs (i.e. PIN, Biometric, etc.).	Merchants make decisions for step-up authentication in the event of higher risk transactions. It is important that issuers enable multi-factor authentication alternatives on their products in the event a merchant feels the need to perform step-up authentication based on fraud scores. At minimum, as a subset of that, merchants request networks adopt uniform policies to require issuers to support 2-factor authentication and cardholders to provide PIN, zip code, CVV or some other form of 2-factor authentication when conducting these types of higher risk purchases.	Low	Med-Long Term
F.11	Tech modernization: Migration of legacy payment switches / gateways to cloud-based API architecture .	Cloud architectures can provide a number of benefits including lower costs, scalability, flexibility and accessibility. APIs provide access to cloud-based services without the requestor of those services needing to know how the service providor operates. They are ideal for providing connectivity to services used by multiple applications and many users as with cloud-based services.	Low	Long Term
	Debit			
DB.1	Confirm debit routing is supported for all technologies including, but not limited to, tokenized and contactless transactions and in all channels including PINless capability.	By law, the merchant has choice on what network to route any payment transaction to according to swipe fee reforms. There should be no technology that prohibits a merchant's rights in this regard. Networks have clearly stated that their tokenized product does not offer debit routing and, therefore, merchants must choose between their tokenization or debit routing. This does not meet this best practice.	High	Near Term
DB.2	For transactions capable of routing to more than one network, ensure new CVMs are available to all networks on all devices in all acceptance channels (i.e. CDCVM availability on all US Common Debit).	Biometric authentication is not available for face-to-face payment domestic debit network transactions because the CDCVM is not licensed to those domestic debit networks. Both the acquirer and the issuer of the debit account have no knowledge if a biometric authentication was used for the payment transaction since they only see a "no CVM" cardholder verification. As a result, there is a higher risk that the issuer may choose to decline the transaction, negatively impacting the customer experience.	Medium	Near Term

	Best Practice:	Why is it important?	Priority	Timeline
	Digital			
DG.1	Ensure merchants have freedom of choice regarding which digital wallets to accept, based on security, data use provisions, marketing arrangements, cost, and consumer experience.	Networks should not mandate merchant acceptance of any digital container offered by a third party. There are operational, economical, performance, security, data, and other business considerations a merchant must consider for such acceptance.	High	Near Term
DG.2	Ensure contactless/digital acceptance remains optional for merchants (i.e. Merchants accepting physical card payments are not mandated to also accept contactless/digital card payments).	Merchants should not be required to accept all form factors of a network's payments including NFC/EMV contactless or other digital form factors, simply because they accept that network's branded payment products in the form of EMV contact or magnetic stripe. There are operational, economical, and other business considerations a merchant must consider for such acceptance.	High	Near Term
DG.3	Any merchant who accepts a digital wallet that utilizes the brand-owned EMVCo tokenization specification should get full liability protection for those transactions, and be able to reconcile those.	Network payment tokenization limits merchants' ability to mitigate fraud risk as the PAN is no longer available data to incorporate into merchant risk models and tools. Since merchants have no control over the authentication for payments using such proprietary network payment tokens and the network is taking full responsibility for the security surrounding the vaulting of PANs and de-tokenization protocols, merchants should assume no responsibility for liability of fraud or other chargeback risks.	High	Near-Med Term
DG.4	No premium rates, incremental or multiple security fees, or chargebacks on transactions processed via mandated network proprietary security solutions.	In the event a payment network requires a merchant to participate in a proprietary security solution or a product that uses such a solution by network rules, incremental fees charged for that mandated merchant participation appears to be non-competitive in nature offering no competitive choice for merchants to manage its own risks and acceptance costs. Elimination of such premium rates or incremental fees for network proprietary security solutions could still achieve any claim of improved security without passing those incremental fees or premium rates as a cost burden to the merchant who has no choice but to participate.	High	Med-Long Term
DG.5	Ensure that any payment and/or customer data received from merchants by networks or partners is used only for transaction processing.	Merchants do not want their customer or SKU data shared with competitors and monetized by the networks or their partners.	Medium	Near Term

	Best Practice:	Why is it important?	Priority	Timeline
DG.6	Provide PAR to merchants for all transactions (tokenized or clear text).	PAR enables merchants the ability to see a customer profile and payment behaviors across all analog and digital channels alongside payment tokenization where the Payment Account Number (PAN) is replaced with a token.	Medium	Near-Med Term
DG.7	Enable omni-channel commerce with supporting rules and relevant, modern, and effective tools for fraud mitigation.	Card brands need to recognize that many merchant verticals have channels that are beginning to coalesce. Merchants have pure brick and mortar transactions, call centers, Internet transactions, as well as, "mixed channel" transactions, such as order on-line and pick up in store or order in-store via a kiosk for home delivery. Another example is hotels and resorts, where many are moving to an online check-in process and not obtaining a signed registration card or swiping the credit card at check in. Card brand policies, procedures and costs need to reflect the changing retail environment.	Medium	Med-Long Term
DG.8	Ensure effective, open, and competitive data security provisions are required for all users of the network contactless/QR code specs.	As new wallet/contactless solutions are introduced, it is critical that merchants have assurance that the appropriate data security best practices have been applied to protect consumer data.	Low	Near-Med Term
DG.9	Ensure merchants have real-time insight into financial products inside a digital wallet to enable discounts or incentives.	Beyond the digital wallet identifier, merchants should also be made aware of the type of product within a digital wallet (e.g. credit, debit, prepaid) to enable their legal right to offer discounts or other incentives to consumers by payment type used based on the cost of acceptance or other criteria.	Low	Near-Med Term
DG.10	Require a Wallet ID in the authorization request when a device is presented as a payment instrument at the terminal and in settlement record (optional) for all mobile and in-app transactions.	Merchants want to know the wallet provider they are accepting at presentment so that they can: • verify it is secure • ensure there are data rules in place • address service level and operational issues that may arise • potentially pursue opportunities to market with that wallet provider	Low	Near-Med Term

	Best Practice:	Why is it important?	Priority	Timeline
	Chargebacks & Fraud			
CF.1	Ensure issuers may not charge back over 5 fraudulent transactions on the same account nor any transaction after the first reported instance	Merchants should not be exposed to fraud on the same account beyond a consistent number of reasonable occurrences (e.g. 5 fraud transactions or other agreed upon number). In such cases, the issuer should be held accountable for card replacement or addressing accountholder abuse. In response to significant fraud chargebacks experienced by the merchants after the liability shift, the networks did implement temporary reductions for the number of fraudulent EMV transactions that expire in 2018. Consistency in this rule among networks would improve merchant payment operations and these parameters should continue in perpetuity vs. expiring in 2018.	High	Near-Med Term
CF.2	Allow for compelling evidence for all disputed transactions (for both retrievals and chargebacks).	Merchants should be provided a list of compelling evidence requirements for each transaction type which, if met, indemnifies the merchant from fraud liability. Additionally, compelling evidence requirements should be consistent across networks to improve merchant payment operations.	High	Med-Long Term
CF.3	Provide tools and align liability to the party who can best prevent the fraud.	More so lacking in the digital commerce space, transactions should leverage modern technology solutions and tools available to enable adequate authentication and verification of payment transactions. The party in the best position to prevent the fraud such as the party giving authorization should assume the liability for risk of fraud.	High	Long Term
CF.4	Provide transparency into fraud and chargebacks in the payment system.	Merchants need visibility of fraud and chargeback trends, so that they are able to appropriately prevent and combat fraud. These include things such as: • overall fraud and chargeback trends observed in the last 6 months, by channel • chargeback rates by merchant categories and by chargeback reason codes • detailed reporting of issuer-reported fraud and chargebacks at the issuer and BIN level (count and amount of transactions, count of accounts) • issuer chargeback to sales ratios overall, with a subtotal for fatal chargeback rates	Medium	Near Term
CF.5	Ensure the chargeback process and liabilities for a wallet provider is made available to and understood by the merchants.	The chargeback process involving a third-party provider of a digital container should be published and transparent to the merchant community.	Medium	Near-Med Term

	Best Practice:	Why is it important?	Priority	Timeline
CF.6	To the degree chargeback rules and procedures remain in place, align timeframes for initiating transaction disputes to legal requirements.	Networks should not supersede legal requirements for disputes. Merchants should follow one set of rules regarding disputes which should be law. Issuers must formally handle disputes from their consumers when such disputes are received within 60 days of the original billing date (Fair Credit Billing Act). However, the card association rules allow for chargebacks well beyond that time period. We need to align the allowable period for issuers to initiate a chargeback with federal law (and state laws that likely follow federal law most often).	Medium	Med-Long Term
CF.7	Provide holistic solutions to mitigate fraud in the ecommerce space, addressing all ways customers shop	Current network rules should support fraud mitigation solutions in cross-channel or omni-channel commerce experiences. For example, current rules don't support buy on line & pick up in store (BOPUS) commerce experience sufficiently to enable adequate fraud prevention practices leveraging modern technology solutions and equitable risk sharing among stakeholders.	Medium	Long Term
CF.8	Ensure an issuer abuse monitoring program exists and provides transparency to the merchants regarding issuer accountability	Card brands need to do a better job of monitoring issuers' compliance with the chargeback rules to ensure that they are not taking advantage of or creating loopholes to pass on fraud to merchants.	Medium	Long Term
CF.9	Ensure merchant excessive chargeback programs exclude chargebacks due to reported card accounts that have been breached and accommodate exceptions for locations in geographic markets with markedly higher than average fraud	Excessive chargeback programs do not currently limit exposure to merchants of chargeback liability due to circumstances in which the merchant has limited or no control. For example, if a merchant with a location in Florida where there is a higher crime rate implements every precaution possible to limit its exposure, they merchant may still be flagged under these excessive chargeback programs simply because of their geographic location and/or accounts that have been exposed to a breach.	Low	Near-Med Term