# Data Sharing Options – U.S. Payments Forum Payments Ecosystem View

| # | Option | Description | Technology | Liability Shift | Benefits | Opportunities | Network Dependent? | Usage / Business Case |
|---|---|---|---|---|---|---|---|---|
| 1 | 3D Secure | Merchant flags online transaction for 3DS treatment to be applied by Card issuer who:<br>1) Declines authentication<br>2) Steps up through pre-authorization authentication<br>3) Approves authentication and proceeds to authorization<br><br>Merchant provides additional data and data or derived score is shared with Card Issuer | Merchant's Payment Gateway to Access Control Server (ACS) to Card Issuer | Yes | • Established protocol<br>• Avoids fraud losses for all parties<br>• Merchant has chargeback protection for online transaction | • Client friction may result in cart abandonment or servicing challenges for issuer<br>• May results in higher # of false/positive issuer declines<br>• ACS provider may/may not include data elements, versus score (model risk management required)<br>• Data not always clean<br>• Work required to share data elements to downstream applications at issuer<br>• Additional fees for merchants | Yes – Not available for US Debit Networks | Limited to merchant's with larger ticket sizes and / or high reported fraud<br><br>Need widespread merchant adoption to maximize value |
| 2 | 3D Secure Data Only | Merchant sends pre-authorization message to Card Issuer with data fields populated<br><br>Issuer utilizes data to make authorization decision with no step up requirement | Same as above | No | • Improves approval rates<br>• Data can also be leveraged in fraud prevention strategies and dispute process<br>• Frictionless customer experience | • Expensive to build<br>• Data elements are limited –not always as defined<br>• Additional fees for merchants | Yes – Not available for US Debit Networks | Pilot activity / one large processor only<br><br>Need widespread merchant adoption to gain value from build |
| 3 | Trusted Transaction / Merchant ID | Merchant identifies population of "trusted" transactions and sends to Card Issuer to be considered as part of the issuing decision strategy | Leverages auth flow: either MID or unused data field | No | • Reduction in false positives / fraud declines leading to improvement of authorization rates<br>• Easy to measure success and adjust strategy if needed<br>• Limited / no tech development | • MID structure or unused data element may not be available for use<br>• Merchants may need to add new 'trusted' MID(s)<br>• Merchants required to connect to multiple issuers | No | Growing – most large issuers support<br><br>Lift in approvals drive positive business case |

# Data Sharing Options – U.S. Payments Forum Payments Ecosystem View

| # | Option | Description | Technology | Liability Shift | Benefits | Opportunities | Network Dependent? | Usage / Business Case |
|---|---|---|---|---|---|---|---|---|
| 4 | Issuer Led Connections to Merchant / Processor | Issuers receive data directly from Merchants, Fraud Risk Providers and Processors pre-authorization and utilize that data in their decisioning models | API | No | • Reduction in false positives / fraud declines leading to improvement of authorization rates<br>• Data can also be leveraged in Operations and dispute process<br>• Merchants can share declines, allowing Issuer to service calls from customer. | • Build required for users<br>• Vendor registration / agreements required<br>• Merchants need to build connections to multiple issuers | No | One large issuer supporting today, use growing<br><br>Need adoption by processors and merchants to maximize value |
| 5 | Fraud Risk Providers Connections to Issuers | Fraud Risk Providers connect merchants to card issuers; share data or a score as part of authorization request. Issuers incorporate data into authorization strategies | API | Dependent on agreement | • Improved approval rates<br>• Data can also be leveraged in fraud prevention and dispute process | • Vendor registration / agreements required<br>• Issuers have to connect to multiple providers<br>• Some solutions are only model based / model risk management required | No | Many large merchants participate in services<br><br>Value dependent on contract with provider |
| 6 | Network Adds Data to Auth Message | Networks Add Data from Merchants and / or Fraud Risk Providers into the Auth Stream. Issuers incorporate data into authorization strategies and send to downstream applications for servicing and dispute processing. | API | No | • Networks do majority of work<br>• Merchants / Issuers don't have to connect with additional providers<br>• Consistent approach across the industry | • Payment ecosystem members may not want to share data with networks<br>• Merchant and Issuer fees | Yes | Development underway<br><br>Value dependent on fee structure |
| 7 | Wallet Provider Score Solution | Wallet providers provide a score for transaction via authorization. Issuers incorporate score into authorization strategies.<br>Emerging: Wallet providers share data directly with issuers pre-authorization. | API or via Auth | No | • Wallet providers have device insights across merchants<br>• Wallet provider scoring layered on top of other risk management capabilities | • Model risk management required for Auth or API<br>• Direct API – issuer integration with multiple wallets required<br>• Wallet provider privacy concerns with sharing data with networks | Yes – Auth<br>No - API | Limited<br><br>Value to be determined as solution evolves |