

**In Pursuit of a  
Better Payment  
System**



**Secure Payments Task Force  
Payment Lifecycles and Security Profiles  
*DMF Vote Results Addendum:  
Vote and Comment Record***

Published March 16, 2018

# Executive Summary

In January 2015, the Federal Reserve published the *Strategies for Improving the U.S. Payment System*, a multi-faceted plan for collaborating with payment system stakeholders to enhance the speed, safety, and efficiency of the U.S. payment system. As a result, the Secure Payments Task Force (SPTF) was established to advise the Federal Reserve on payment security matters, coordinate with the Faster Payments Task Force and determine payment security priorities for future action. The task force has produced the Payment Lifecycles and Security Profiles as one of their key deliverables, and is now being asked to officially approve this deliverable.

The task force vote was conducted from January 11 to January 26 to approve the Payment Lifecycles and Security Profiles. This document (*Vote Results Addendum: Vote and Comment Record*) provides the votes of each Secure Payments Task Force member as well as comments. The *Vote Results*, which can be found in a separate document, includes numerical results of the vote, at both the task force and voting segment level. In accordance with the Decision-Making Framework, these documents will be published on FedPaymentsImprovement.org.

## Approval of the Payment Lifecycles and Security Profiles

Approval of the Payment Lifecycles and Security Profiles was achieved in accordance with the Decision-Making Framework, which is applied to task force work products requiring a super majority consensus. Task force members who voted were asked to: (1) “Consent,” with an option to provide comments; (2) “Stand Aside,” with an option to provide comments; or (3) “Object,” with a required declaration of concerns and a proposal for an alternative approach that addresses those concerns. With 63% of task force members participating in the vote, the framework achieved a decisive 90% consent rate as well as the consent of all eight industry segments. (Details can be found in the *Vote Results*.) On February 21, 2018, the Secure Payments Task Force chair recorded the Payment Lifecycles and Security Profiles as approved based on the results of the task force vote.

# Payment Lifecycles and Security Profiles

## *Task Force Vote Record*

| Last Name | First Name  | Organization  | Voting Segment                | Vote*       | Comments* (Y/N) |
|-----------|-------------|---|-------------------------------|-------------|-----------------|
| Ahlstrom  | Paul        | Alta Ventures   | Other Stakeholders            | Consent     | Y               |
| Alvarez   | Troy        | Intel Corporation   | Non-Bank Providers            | Consent     | N               |
| Anand     | Vijay       | Infosys Limited   | Non-Bank Providers            | Consent     | N               |
| Anderson  | Adam        | Bank of Commerce  | Small Financial Institutions  | Consent     | N               |
| Arminio   | Maria       | Avenue B Consulting, Inc.                                   | Other Stakeholders            | Consent     | N               |
| Aubol     | Larry       | TASCET Inc.   | Non-Bank Providers            | Consent     | Y               |
| Avena     | Sherry      | Interactive Financial Services Group, Inc.                  | Non-Bank Providers            | Consent     | N               |
| Barouski  | William     | The Northern Trust Company                                  | Large Financial Institutions  | Consent     | N               |
| Barrows   | Becky       | TTCU The Credit Union                                       | Medium Financial Institutions | Consent     | Y               |
| Beckman   | Michelle    | American Express  | Non-Bank Providers            | Object      | Y               |
| Benardo   | Michael     | Federal Deposit Insurance Corporation (FDIC)                | Other Stakeholders            | Stand aside | N               |
| Bland III | Andrew R.   | Harland Clarke  | Non-Bank Providers            | Consent     | N               |
| Boden     | Kim         | Western Union   | Non-Bank Providers            | Consent     | N               |
| Bradfute  | Richard     | James Polk Stone Community Bank                             | Small Financial Institutions  | Consent     | N               |
| Brungardt | Jill        | Commerce Bank   | Medium Financial Institutions | Object      | Y               |
| Burchess  | Danna       | Five Points Bank  | Small Financial Institutions  | Consent     | N               |
| Byrne     | Brian       | EMVCo   | Other Stakeholders            | Object      | Y               |
| Callahan  | Mary Ann    | Paxos Trust Company, LLC                                    | Non-Bank Providers            | Consent     | N               |
| Campbell  | Angela      | UMB Bank, N.A.  | Medium Financial Institutions | Stand aside | Y               |
| Canino    | Carla       | Sunlight Commerce Consulting                                | Other Stakeholders            | Consent     | N               |
| Chadwick  | Laura       | National Restaurant Association                             | Other Stakeholders            | Consent     | N               |
| Colvin    | Ben         | MasterCard  | Non-Bank Providers            | Object      | Y               |
| Cortedano | Jose        | Rosetta Technologies  | Non-Bank Providers            | Consent     | N               |
| Danvers   | Christopher | American Airlines Federal Credit Union                      | Medium Financial Institutions | Consent     | N               |
| Dickerson | Kelly       | Shore United Bank   | Medium Financial Institutions | Consent     | Y               |
| Dooley    | Terry       | SHAZAM Network  | Non-Bank Providers            | Consent     | Y               |
| Dresner   | Andrew      | JPMorgan Chase & Co.  | Large Financial Institutions  | Consent     | Y               |
| Drohman   | Jason       | Western State Bank  | Small Financial Institutions  | Consent     | N               |
| Duke      | Jim         | Woodforest National Bank                                    | Medium Financial Institutions | Stand aside | N               |
| Dulaney   | Travis      | Push Payments   | Non-Bank Providers            | Consent     | N               |
| Evans     | Frazier     | Individual Participant                                      | Other Stakeholders            | Consent     | Y               |
| Faoro     | Dave        | Verifone, Inc.  | Non-Bank Providers            | Consent     | N               |
| Farren    | Angi        | Upper Midwest Automated Clearing House Association (UMACHA) | Other Stakeholders            | Consent     | N               |
| Fialkov   | David       | NATSO   | Other Stakeholders            | Consent     | N               |
| Fields    | Anne        | Crutchfield Corporation                                     | Business End-Users            | Consent     | N               |
| Fors      | Terry       | Deluxe Corporation  | Non-Bank Providers            | Consent     | N               |
| Gilbert   | Chris       | Bankers' Bank of Kansas                                     | Small Financial Institutions  | Consent     | N               |

\* Comments associated with votes are included in the second section of this report.

| Last Name     | First Name  | Organization  | Voting Segment                  | Vote*       | Comments* (Y/N) |
|---------------|-------------|---|---------------------------------|-------------|-----------------|
| Gimello       | Sarah       | Paychex, Inc.   | Non-Bank Providers              | Consent     | N               |
| Giorgio       | Tina        | ICBA Bancard & TCM Bank   | Small Financial Institutions    | Stand aside | N               |
| Gobeyn        | Gina        | Discover Financial Services                                     | Large Financial Institutions    | Object      | Y               |
| Guerrier      | Amma        | Xenith Bank   | Medium Financial Institutions   | Consent     | N               |
| Hallowell     | Curtis      | Cummins-Allison Corp.   | Non-Bank Providers              | Consent     | N               |
| Hardison      | Clint       | SunTrust Bank   | Large Financial Institutions    | Consent     | N               |
| Hart          | Annmarie    | Mag-Tek Inc.  | Non-Bank Providers              | Consent     | N               |
| Hartridge     | Andrew      | M&T Bank  | Large Financial Institutions    | Stand aside | N               |
| Helms         | Jarrett     | The Clearing House (TCH)  | Non-Bank Providers              | Consent     | N               |
| Hennessy      | Jane        | G2 Web Services   | Non-Bank Providers              | Consent     | N               |
| Hill          | Christopher | Bankers' Bank of the West                                       | Small Financial Institutions    | Consent     | Y               |
| Holloway      | Lauren      | PCI Security Standards Council                                  | Other Stakeholders              | Object      | Y               |
| Horwedel      | Mark        | Merchant Advisory Group (MAG)                                   | Other Stakeholders              | Consent     | N               |
| Hunt          | Carrie      | National Association of Federally-Insured Credit Unions (NAFCU) | Other Stakeholders              | Consent     | Y               |
| Jackson       | David       | Marketcy  | Other Stakeholders              | Consent     | N               |
| Jenkins       | Rue         | Costco Wholesale Corporation                                    | Business End-Users              | Consent     | N               |
| Jensen        | Austen      | Retail Industry Leaders Association (RILA)                      | Other Stakeholders              | Consent     | N               |
| Jewell        | Linda       | Navy Federal Credit Union                                       | Medium Financial Institutions   | Object      | Y               |
| Jones         | Dewayne     | Regions Bank  | Large Financial Institutions    | Object      | Y               |
| Kendall       | Russell     | Bank of America   | Large Financial Institutions    | Consent     | N               |
| King          | Thaddeus    | The Pew Charitable Trusts                                       | Consumer Interest Organizations | Consent     | N               |
| Kozlowski III | Theodore    | Individual Participant  | Other Stakeholders              | Consent     | N               |
| Kratovil      | Jason       | Financial Services Roundtable                                   | Other Stakeholders              | Object      | Y               |
| Lafferty      | Tracy       | Alloya Corporate Federal Credit Union                           | Medium Financial Institutions   | Consent     | N               |
| Larimer       | Jane        | NACHA - The Electronic Payments Association                     | Other Stakeholders              | Consent     | N               |
| Lees          | Sharon      | Macon-Atlanta State Bank  | Small Financial Institutions    | Consent     | N               |
| Lindgren      | Stephen     | Cornhusker Bank   | Small Financial Institutions    | Consent     | N               |
| Love          | Paul        | CO-OP Financial Services  | Non-Bank Providers              | Stand aside | N               |
| Lucas         | Joyce       | Kacil Business & Technology Consulting Firm                     | Other Stakeholders              | Stand aside | Y               |
| Luhtanen      | Reed        | Wal-Mart Stores, Inc.   | Business End-Users              | Consent     | Y               |
| Mares         | Brad        | Target Corporation  | Business End-Users              | Consent     | N               |
| Martindale    | Suzanne     | Consumers Union   | Consumer Interest Organizations | Consent     | Y               |
| Martz         | Stephanie   | National Retail Federation                                      | Other Stakeholders              | Consent     | N               |
| McNaughton    | Ryan        | North American Banking Company                                  | Small Financial Institutions    | Consent     | N               |
| Mention       | Cedric      | Killeen Independent School District                             | Government-End User             | Consent     | N               |
| Merlet        | Janet       | NEACH   | Other Stakeholders              | Consent     | N               |
| Miller        | Mary Ann    | Actimize, Inc.  | Non-Bank Providers              | Consent     | N               |

\* Comments associated with votes are included in the second section of this report.

| Last Name   | First Name | Organization                                  | Voting Segment                | Vote*       | Comments* (Y/N) |
|-------------|------------|---|-------------------------------|-------------|-----------------|
| Mirajkar    | Rakesh     | Capital One, N.A.                             | Large Financial Institutions  | Stand aside | N               |
| Montis      | Will       | AgriBank, FCB                                 | Large Financial Institutions  | Consent     | N               |
| Mott        | Steve      | BetterBuyDesign                               | Other Stakeholders            | Consent     | Y               |
| Neustifter  | Manfred    | CFPS Technology Group                         | Non-Bank Providers            | Consent     | N               |
| Newton      | Sherry     | Transwestern                                  | Other Stakeholders            | Consent     | N               |
| Noggle      | Lance      | Credit Union National Association (CUNA)      | Other Stakeholders            | Object      | Y               |
| O'Brien     | Richard    | Payment Pathways, Inc.                        | Non-Bank Providers            | Consent     | N               |
| Parks       | Justin     | BB&T  | Large Financial Institutions  | Consent     | N               |
| Penny       | Bryan      | Nordstrom, Inc.                               | Business End-Users            | Consent     | N               |
| Peretti     | Brian      | Department of the Treasury - OCIP             | Other Stakeholders            | Consent     | N               |
| Perrelli    | Frank      | BNY Mellon                                    | Large Financial Institutions  | Consent     | N               |
| Petrini     | Brooke     | CGI   | Non-Bank Providers            | Consent     | N               |
| Piazza      | John       | MB Financial                                  | Medium Financial Institutions | Consent     | N               |
| Picillo     | Philip     | Webster Bank                                  | Medium Financial Institutions | Consent     | Y               |
| Press       | Aaron      | LexisNexis Risk Solutions                     | Non-Bank Providers            | Consent     | N               |
| Pudmanabhan | Suchitra   | CBW Bank                                      | Small Financial Institutions  | Consent     | N               |
| Ranzini     | Stephen    | University Bank                               | Small Financial Institutions  | Consent     | N               |
| Ready       | Anna       | National Association of Convenience Stores    | Other Stakeholders            | Consent     | N               |
| Rogers      | Paul       | United Bankers' Bank                          | Medium Financial Institutions | Consent     | N               |
| Ruden       | Seth       | ACI Worldwide                                 | Non-Bank Providers            | Consent     | N               |
| Russell     | Brian      | Individual Participant                        | Other Stakeholders            | Consent     | Y               |
| Sandqvist   | Niklas     | Aera Payments Identification AS               | Non-Bank Providers            | Consent     | Y               |
| Scanio      | Salvatore  | Ludwig & Robinson PLLC                        | Other Stakeholders            | Consent     | N               |
| Scheidt     | Edward     | Accredited Standards Committee (ASC) X9, Inc. | Other Stakeholders            | Consent     | N               |
| Schmidt     | Tim        | Great Western Bank                            | Medium Financial Institutions | Consent     | N               |
| Shafquat    | Shoaib     | QCheque LLC                                   | Non-Bank Providers            | Consent     | Y               |
| Sparrow     | Jeff       | GeoCommerce Inc                               | Non-Bank Providers            | Consent     | N               |
| Srinivasan  | Ganesh     | Volante Technologies, Inc.                    | Non-Bank Providers            | Consent     | N               |
| Stoltz      | Rochelle   | Coulee Bank                                   | Small Financial Institutions  | Consent     | N               |
| Story       | Jeff       | The Bankers Bank                              | Small Financial Institutions  | Consent     | N               |
| Strayer     | Victoria   | TSYS  | Non-Bank Providers            | Consent     | N               |
| Tapling     | Peter      | Individual Participant                        | Other Stakeholders            | Consent     | N               |
| Tassey      | Jeffrey    | Tassey & Associates                           | Other Stakeholders            | Object      | Y               |
| Tatge       | David      | r4 Technologies                               | Non-Bank Providers            | Consent     | N               |
| Tonne       | Cary       | Affinity Plus Federal Credit Union            | Medium Financial Institutions | Consent     | N               |
| Tran-Trong  | Ky         | Visa Inc.                                     | Non-Bank Providers            | Consent     | Y               |
| Ulrich      | Glen       | U.S. Bank                                     | Large Financial Institutions  | Consent     | N               |

\* Comments associated with votes are included in the second section of this report.

| Last Name         | First Name  | Organization                                     | Voting Segment                | Vote*   | Comments* (Y/N) |
|-------------------|-------------|--|-------------------------------|---------|-----------------|
| Vanderhoof        | Randy       | Smart Card Alliance/EMV Migration Forum          | Other Stakeholders            | Consent | N               |
| Vinogradov        | Victor      | Western Alliance Bank                            | Medium Financial Institutions | Consent | N               |
| Volmar            | Scott       | InterComputer Corporation                        | Non-Bank Providers            | Consent | Y               |
| Walker            | Hannah      | Food Marketing Institute                         | Other Stakeholders            | Consent | N               |
| Wallen            | Charles     | Spectrum   | Non-Bank Providers            | Consent | N               |
| Weaver            | Michelle    | Extraco Banks, N.A.                              | Small Financial Institutions  | Consent | N               |
| Welch             | Bruce       | Gilbarco Inc.                                    | Non-Bank Providers            | Consent | N               |
| Whaley            | Cary        | Independent Community Bankers of American (ICBA) | Other Stakeholders            | Consent | Y               |
| Wilkes            | Bradley     | WingCash, LLC                                    | Non-Bank Providers            | Consent | N               |
| Williams          | Christopher | Exponent, Inc.                                   | Other Stakeholders            | Consent | N               |
| Williquette       | Joel        | Capital Credit Union                             | Medium Financial Institutions | Consent | N               |
| Wyson-Constantine | Heather     | American Bankers Association                     | Other Stakeholders            | Object  | Y               |
| Zelazny           | Frances     | BioCatch   | Non-Bank Providers            | Consent | N               |
| Zhang             | Yuemei      | Wells Fargo & Company                            | Large Financial Institutions  | Consent | Y               |
| Zietlow           | Robert      | Bankers' Bank                                    | Small Financial Institutions  | Consent | N               |
| Zirkle            | Amy         | Electronic Transactions Association (ETA)        | Other Stakeholders            | Consent | N               |

\* Comments associated with votes are included in the second section of this report.

# Payment Lifecycles and Security Profiles

## *Task Force Comment Record*



# Payment Lifecycles and Security Profiles – Vote and Comment Record

| Last Name | First Name | Voting Segment                | Comment Type | Comment  |
|-----------|------------|-------------------------------|--------------|--|
| Ahlstrom  | Paul       | Other Stakeholders            | Consent      | I like the positioning of open standards. I believe the world we are heading into will lean towards adoption of tokenization, user authentication and encryption approach leveraging open standards for security. These open standards could be de jure or de facto as long as they are available and widely accepted.   |
| Aubol     | Larry      | Non-Bank Providers            | Consent      | The profile is tightening up. Good work.<br>LA-  |
| Barrows   | Becky      | Medium Financial Institutions | Consent      | While choosing consent, I also understand these are living documents to which changes can be made if and when needed.  |
| Beckman   | Michelle   | Non-Bank Providers            | Object       | <p>First, we acknowledge the substantial degree of change made to the document since the last vote. Clearly the input from a wide array of stakeholders expressed prior to and during the most recent task force meeting has been both heard and largely incorporated, resulting in a product we believe much more accurately, completely, and objectively portrays the current industry landscape. As such, we have had a strong desire to provide an unqualified "consent" vote of endorsement.</p> <p>However, we remain sufficiently concerned about unchanged language concerning "open standards" and the implications of it to register an object vote. We feel compelled to voice advocacy for approaches that guide consistent, scalable, and interoperable deployment in a global marketplace for many key payment technologies. Explicit use of "open standards" language is potentially exclusionary and subject to misinterpretation. We support decisions to deploy technologies being made based on a pragmatic approach on when suitable for use for relevant use cases, allowing the best tools to combat fraud to come to emerge and grow. Open standards screening criteria is subjective and could inhibit freedom of choice of tools that may be the most effective at achieving fraud reduction.</p> <p>Amend "open standards" language that has been the source of much debate from wide array of stakeholders to simply "standards" OR remove such terminology altogether.</p> |
| Brungardt | Jill       | Medium Financial Institutions | Object       | As context for my vote, I wish to register that the deployment of technologies like encryption, tokenization, and user authentication should be made on a pragmatic, non-mandated basis. The benefits of these particular technologies are situation-dependent and no single static solution can be generalized to the entire payments system. The knowable security case for these technologies exists independently of standards or any governance structure (or absence of such a structure). In order to avoid confusion between security and non-security governance issues, I would suggest broadening the language around standards to simply read "standards" instead of "open standards" or remove the reference to "standards" entirely. Given that consumers deserve the most responsive security approach, it is important that non-security issues do not become an obstacle to the rapid deployment of needed technologies in their proper contexts.   |
| Byrne     | Brian      | Other Stakeholders            | Object       | <p>Unfortunately, the term "open standards" has become a proxy for challenging the governance model of EMVCo. Different stakeholders have different views, on the most effective way to facilitate global reliability in the acceptance of card based payments. The EMVCo position is that the SPTF Payment Lifecycles and Security Profiles are not the appropriate forum to introduce such a politically charged discussion.</p> <p>That the "open standards" phrase used multiple times in Section 5 of multiple profiles, be replaced with the phrase "industry standards" or simply the word "standards."</p>   |
| Campbell  | Angela     | Medium Financial Institutions | Stand aside  | As context for my vote, I wish to register that the deployment of technologies like encryption, tokenization, and user authentication should be made on a pragmatic, non-mandated basis. The benefits of these particular technologies are situation-dependent and no single static solution can be generalized to the entire payments system. The knowable security case for these technologies exists independently of standards or any governance structure (or absence of such a structure). In order to avoid confusion between security and non-security governance issues, I would suggest broadening the language around standards to simply read "standards" instead of "open standards" or remove the reference to "standards" entirely. Given that consumers deserve the most responsive security approach, it is important that non-security issues do not become an obstacle to the rapid deployment of needed technologies in their proper contexts.   |

# Payment Lifecycles and Security Profiles – Vote and Comment Record

| Last Name | First Name  | Voting Segment                | Comment Type | Comment   |
|-----------|-------------|-------------------------------|--------------|---|
| Colvin    | Ben         | Non-Bank Providers            | Object       | <p>Mastercard objects to the Payment Lifecycle and Security Profiles because of the continued use of the term “open standards” as it is in section 5 of many of the different profiles. Mastercard believes, based on the dialogue that has occurred in SPTF related forums that the term ‘open standards’ is vague, not well defined and has a different meaning to the various stakeholders in the payments ecosystem. Therefore the term is subject to broad interpretation by the stakeholders about the most effective way to enable ‘greater deployment of tokenization, user authentication and encryption’ to enable secure and reliable card payments.</p> <p>Mastercard recommends that the ‘open standards’ phrase be replaced with the phrase “industry standards” or simply the word “standards” to ensure the most expedient close to this work effort.</p> |
| Dickerson | Kelly       | Medium Financial Institutions | Consent      | <p>As context for my vote, I wish to register that the deployment of technologies like encryption, tokenization, and user authentication should be made on a pragmatic, non-mandated basis. The benefits of these particular technologies are situation-dependent and no single static solution can be generalized to the entire payments system. The knowable security case for these technologies exists independently of standards or any governance structure (or absence of such a structure). In order to avoid confusion between security and non-security governance issues, I would suggest broadening the language around standards to simply read “standards” instead of “open standards” or remove the reference to “standards” entirely.</p>   |
| Dooley    | Terry       | Non-Bank Providers            | Consent      | <p>A next step to address the risks, gaps, and challenges and to improve security, interoperability, transparency as well as the consumer experience would be for payments to be based on Open and Accredited standards created and managed by recognized Open and Accredited standards organizations like ANSI and ISO instead of proprietary framework bodies like PCI and EMVCo.</p> <p>Great job to the team who spent countless hours on these work products and I congratulate the Federal Reserve for facilitating and bringing the industry together in an incredibly open and transparent process.</p>   |
| Dresner   | Andrew      | Large Financial Institutions  | Consent      | <p>While we consent to the overall document, we disagree with the use of the term “Open standards” within the text. We would have agreed with the term “standards”, but the current language is not consistent with many of the core standards in use by the industry today and would slow down the adoption of new standards going forward. Further, we would emphasize that this is a document of the Task Force and not the Fed itself and should always be presented that way in public forums.</p>   |
| Evans     | Frazier     | Other Stakeholders            | Consent      | <p>I believe there is still work to be done but this is a great foundational document to build from.</p>  |
| Gobeyn    | Gina        | Large Financial Institutions  | Object       | <p>Good progress, however remaining stakeholder concerns on items not critical to the intended purpose of the Payment Lifecycle &amp; Security Profiles deliverable remain. The term “open standards” remains in several of the use cases; it term is a point of conflict/concern of stakeholders across the taskforce. The conflict distracts from the intention of the Payment Lifecycle and Security Profiles deliverable and not relevant to its intended purpose.</p> <p>Remove the term “open standards” and replace with the term “standards.”</p>   |
| Hill      | Christopher | Small Financial Institutions  | Consent      | <p>I know there is concern among some organizations involved about the phrase “open standards” when it comes to tokenization, user authentication and encryption as well as risk-based cybersecurity. While I think that is a loaded phrase that could be misused, I don’t want that to deny moving the entire initiative forward. I do hope the task force / subgroup / steering committee / etc. reopen discussion about this particular point in the Challenges and Improvement Opportunities in all of the Payment Lifecycles and Security Profiles.</p>  |

# Payment Lifecycles and Security Profiles – Vote and Comment Record

| Last Name | First Name | Voting Segment     | Comment Type | Comment   |
|-----------|------------|--------------------|--------------|---|
| Holloway  | Lauren     | Other Stakeholders | Object       | <p>We object to the statement in several of the profiles that “Greater deployment of tokenization, user authentication and encryption based on open standards could enhance payment security.” Standards development occurs in thousands of individual organizations that vary significantly in many ways as regards their technical processes, costs and requirements of participation, intellectual property regimes and more. PCI SSC is involved in a variety of these standards development organizations, and has evolved its own rules and procedures to best accomplish its important goals in the context of the rapidly evolving threat landscape in which it operates.</p> <p>The challenges presented by this landscape require the ability to address cybersecurity threats quickly, sometimes within confidential settings, when vulnerabilities are identified or new threats emerge. It also requires a degree of coordination of purpose and approach that is seldom possible where standards are developed among multiple “siloeed” standards organizations, each of which concerns itself with only one or a few technical areas or business domains. In contrast, the holistic, “end to end” approach adopted by PCI SSC provides a comprehensive approach to payment card security with proven efficacy.</p> <p>While it is true that the process employed by PCI SSC therefore necessarily varies in some respects to those of some other standards development organizations, it is well recognized that there is no single definition of “openness” in standards development, and that practices vary, both within and across industries. Indeed, while the U.S. government’s OMB Circular A-119 does express a preference for the use of “voluntary consensus body” standards in government procurement, it goes on to state that there is no objection to the use of standards developed by entities that do not match that particular definition, or even to the use of proprietary standards, where the non-voluntary consensus body standard is superior, has been more widely adopted, or may have any of a long list of other enumerated benefits.</p> <p>In addition, under World Trade Organization rules barring the erection of technical barriers to trade, signatory nations (of which the U.S. is one) are barred from requiring compliance with unique domestic standards where existing, internationally acknowledged standards are already available and in broad use.</p> <p>Given the wide implementation of PCI SSC’s holistic suite of cybersecurity standards and supporting materials and services, and the broad state and foreign governmental endorsement of these standards, it would be a step backwards, rather than forwards, in securing payment card data not to encourage the use of PCI SSC standards in service of meeting a designation (“open standards”) which is neither necessary, or even universally understood in the same way.</p> <p>In summary, we request that all standards, including those developed by PCI SSC, that have proven to be useful in protecting the confidentiality of payment data be included rather than limiting them through the uses of an unnecessary and undefined filter, especially where the materials in question are defined as “educational” and intended as “best practices” for a broad audience.</p> <p>Suggested solution: Remove the word “open” altogether or replace it with “industry” so that it reads either:</p> <ul style="list-style-type: none"> <li>• Greater deployment of tokenization, user authentication and encryption based on standards could enhance payment security. OR</li> <li>• Greater deployment of tokenization, user authentication and encryption based on broadly adopted industry standards could enhance payment security.</li> </ul> |
| Hunt      | Carrie     | Other Stakeholders | Consent      | <p>I will note that there is still some ambiguity concerning the meaning of open standards in the document, and NAFCU wants to ensure that this ambiguity could never serve as an opportunity to direct criticism at credit unions for failing to use any one particular security method.</p>   |

# Payment Lifecycles and Security Profiles – Vote and Comment Record

| Last Name | First Name | Voting Segment                | Comment Type | Comment  |
|-----------|------------|-------------------------------|--------------|--|
| Jewell    | Linda      | Medium Financial Institutions | Object       | <p>As context for my vote, I wish to register that the deployment of technologies like encryption, tokenization, and user authentication should be made on a pragmatic, non-mandated basis. The benefits of these particular technologies are situation-dependent and no single static solution can be generalized to the entire payments system. The knowable security case for these technologies exists independently of standards or any governance structure (or absence of such a structure).</p> <p>In order to avoid confusion between security and non-security governance issues, I would suggest broadening the language around standards to simply read "standards" instead of "open standards" or remove the reference to "standards" entirely. Given that consumers deserve the most responsive security approach, it is important that non-security issues do not become an obstacle to the rapid deployment of needed technologies in their proper contexts.</p> <p>Thank you</p>  |
| Jones     | Dewayne    | Large Financial Institutions  | Object       | <p>As context for my vote, I wish to register that the deployment of technologies like encryption, tokenization, and user authentication should be made on a pragmatic, non-mandated basis. The benefits of these particular technologies are situation-dependent and no single static solution can be generalized to the entire payments system. The knowable security case for these technologies exists independently of standards or any governance structure (or absence of such a structure).</p> <p>In order to avoid confusion between security and non-security governance issues, I would suggest broadening the language around standards to simply read "standards" instead of "open standards" or remove the reference to "standards" entirely. Given that consumers deserve the most responsive security approach, it is important that non-security issues do not become an obstacle to the rapid deployment of needed technologies in their proper contexts.</p>   |
| Kratovil  | Jason      | Other Stakeholders            | Object       | <p>While the Payment Lifecycles and Security Profiles have evolved in very significant and positive ways -- and the Fed team is to be applauded for their efforts -- I cannot consent to these documents on behalf of my members so long as they contain the unnecessary, superfluous, and blatantly political use of the term "open standards."</p> <p>Were the word "open" dropped from these documents, or replaced by a more accurate term such as "industry," I would be excited to vote to provide my consent to this process. However, the inclusion of the word "open" is an overt attempt by some to bias this collaborative process against certain parties. It is such a shame that, despite such tremendous progress made elsewhere in these documents, that the use of this single word -- which will be used to politicize this entire effort once it is finalized -- has been allowed to proceed. From a purely objective standpoint -- are there lots of "closed" standards out there? Are there many standards-setting bodies that brag about their "closed" standards? If so, I'm not aware of any. So why continue to use the word? Moreover, why continue to use the word without providing a definition of the phrase "open standards?" Given an appropriate definition elsewhere, it's conceivable that "open standards" could be acceptable.</p> <p>Yet despite these recommendations and arguments being made by many participants over the last few months, nothing on this issue has changed. For this reason, and in the best interest of my members, I must object.</p> <p>Remove the word "open" from "open standards." Alternatively, replace with "industry," as in "industry standards."</p> |
| Lucas     | Joyce      | Other Stakeholders            | Stand aside  | <p>At our last DMF vote - I voted positively - read the changes - and don't see any real concerns.</p>   |

# Payment Lifecycles and Security Profiles – Vote and Comment Record

| Last Name  | First Name | Voting Segment                  | Comment Type | Comment   |
|------------|------------|---------------------------------|--------------|---|
| Luhtanen   | Reed       | Business End-Users              | Consent      | <p>I would like to take this opportunity to praise the Federal Reserve staff, the steering committee, and our colleagues on the task force at large. The publication of this document will truly be a landmark achievement for the industry. The process that was undertaken ensured that every stakeholder who had a viewpoint was afforded ample opportunity to raise that viewpoint and engage in discussion with a cross-section of industry participants.</p> <p>While the document stops short of many recommendations we would make as business end users, I recognize that it is inevitable that any document published by such a group will fail to espouse the views of any particular segment. With that in mind, I consent to the publication of this document and urge the entire task force to continue to travel down the path to a more secure payments system.</p>   |
| Martindale | Suzanne    | Consumer Interest Organizations | Consent      | <p>Thanks to everyone for their hard work on this crucial foundational document for the Task Force. It will provide substantial value to the payments community and the general public.</p>   |
| Mott       | Steve      | Other Stakeholders              | Consent      | <p>This work represents a good start to shedding the light needed to fix what ails the payment system, laying the foundation for understanding the sources of fraud and inefficiency, and setting the stage for the next phase of the Task Force in drilling down to identify and address solutions. Bravo!</p>   |
| Noggle     | Lance      | Other Stakeholders              | Object       | <p>We appreciate the hard work by all who have worked on the payment lifecycles and security profiles. We continue to remain concerned by the continued use of "open standards." This takes a step beyond the principles of security that should be part of the profiles. Unfortunately we cannot partially support or partially object, which is why we object so that our concerns with the vote and process are on record.</p> <p>remove the word "open" when describing standards. The language should read "standards" instead of "open standards" or remove the reference to "standards" entirely.</p>  |
| Picillo    | Philip     | Medium Financial Institutions   | Consent      | <p>As context for my vote, I wish to register that the deployment of technologies like encryption, tokenization, and user authentication should be made on a pragmatic, non-mandated basis. The benefits of these particular technologies are situation-dependent and no single static solution can be generalized to the entire payments system. In fact our industry continues to message around a multi pronged approach related to security. It appears that much discussion has occurred between and among many stakeholders. The issue for some seems to be the use of the word "open" related to standards developed or in use today to achieve a secure, ubiquitous real time payment solution. It is this participants expectation that should the word "open" be part of the lexicon related to the lifecycle documents it is in no way indicative that the industry will be subject to further regulatory oversight. The knowable security case for these technologies exists independently of standards or any governance structure (or absence of such a structure). In order to avoid confusion between security and non-security governance issues, I would suggest one alternative would be to broaden the language around standards. Given that consumers deserve the most responsive security approach, it is important that non-security issues do not become an obstacle to the rapid deployment of needed technologies in their proper contexts.</p> |
| Russell    | Brian      | Other Stakeholders              | Consent      | <p>The team has worked extremely hard over the past year to assemble this excellent work package. I believe it will be received positively and help the market implement more efficient and effectively security solutions.</p>   |
| Sandqvist  | Niklas     | Non-Bank Providers              | Consent      | <p>To us these use cases seems to be a very comprehensive documentation of the different payment methods including security relevant information and risks.</p>   |
| Shafquat   | Shoaib     | Non-Bank Providers              | Consent      | <p>Thank you for all your hard work for keeping our payment systems safe</p>  |

# Payment Lifecycles and Security Profiles – Vote and Comment Record

| Last Name  | First Name | Voting Segment     | Comment Type | Comment   |
|------------|------------|--------------------|--------------|---|
| Tassey     | Jeffrey    | Other Stakeholders | Object       | <p>Despite all of the work that has occurred, and the desire to "consent", the retention of "open standards" is in my view inconsistent with an educational undertaking focused on security. "Open standards" or even "standards" in my view has become a proxy for a private sector governance process that could lead to a mandate of a particular security technology, and indeed, for example, individual task force participants have commented in favor of such concepts as a "PIN mandate", which in turn is a proxy for other issues that are even less consistent with an educational undertaking focused on security. The decision to apply a technology such as tokenization is made on a situational basis where, for instance, deployment of a static technology is completely inappropriate, and I do not see how a particular governance structure for a standard has any bearing on security; the security case for a particular technology is completely discernible independent of a standard or governance structure.</p> <p>Simply remove any reference to standards.</p>   |
| Tran-Trong | Ky         | Non-Bank Providers | Consent      | <p>We support the development of the Payment Life Cycle and Security Profiles and commend the Steering Committee members and Fed staff for their hard work in taking into account industry feedback and making significant improvements to the Profiles as they are presented in this DMF vote. To avoid potential confusion that may arise from the current references to "open standards" in the Profile documents and given the immense importance of securing the payment system through greater deployment of layered security including tokenization, encryption, and user authentication generally, we recommend that the language around standards to simply read "standards" rather than "open" standards or any other qualification. At a minimum, we recommend that the final Profiles clarify that the sentence regarding "greater deployment of tokenization, encryption, and user authentication" is not intended to suggest that current industry standards are not "open".</p>  |
| Volmar     | Scott      | Non-Bank Providers | Consent      | <p>I consent to the profiles as profiles. They have been deliberated as thoroughly as possible from a generic point of view, but not with respect to any specific implementation of any payment type. The rubber meets the road when evaluating/upgrading actual implementations and the variables associated with those implementation from end-to-end. End-to-end risk analysis must be done in the implementation/upgrade stage and analyzed in completeness. There are points of vulnerability which the profiles cannot address. The profile is an effective guide as it intended to be. But there are other security and secure messaging criteria to be considered implementation by implementation. I believe a qualified statement to this effect belongs in the publication. I give applause to the PIM and data Protection sub-workgroup and the Security Task Force at large for painstaking job well done.</p>   |
| Whaley     | Cary       | Other Stakeholders | Consent      | <p>ICBA consents to the publishing of The Payment Lifecycles and Security Profiles and expresses appreciation to the Federal Reserve and the Secure Payments Steering Committee for taking the time to consider all feedback and ensure a balanced picture of payments security without taking security principals out of their intended payments context.</p> <p>The Payment Lifecycles and Security Profiles will educate payments stakeholders and provide perspectives related to: the lifecycles of the most common payment types (enrollment, transaction flow and reconciliation); security methods, identity management controls and sensitive data occurring at each step in the payment lifecycles; relevant laws and regulations, and other references, as well as challenges and improvement opportunities related to each payment type.</p> <p>While ICBA consents to the document as a whole, we do express concern of the use of the term "open standards." ICBA regards the term as murky, at best. Standards can be open to the industry, openly owned, or openly maintained. Only the availability of the standard could pertain to security the other two are business issues. Since the document does not define "open standard" in the document, ICBA's consent is based on the term meaning open to the industry.</p> |

# Payment Lifecycles and Security Profiles – Vote and Comment Record

| Last Name         | First Name | Voting Segment               | Comment Type | Comment   |
|-------------------|------------|------------------------------|--------------|---|
| Wyson-Constantine | Heather    | Other Stakeholders           | Object       | <p>Introduction<br/>The American Bankers Association is pleased to submit the following comments. Founded in 1875, the American Bankers Association is the united voice of America's hometown bankers—small, regional and large banks that together employ more than 2 million women and men, hold nearly \$17 trillion in assets, safeguard \$13 trillion in deposits and extend more than \$9 trillion in loans.</p> <p>America's regulated financial institutions believe strongly that consumers deserve a high level of security in their payment options and therefore invest significant resources in developing, deploying, and improving proactive measures to secure the elements of the payment system under their control. Banks and credit unions comply with robust physical and data security requirements provided by statute and regulation, and are regularly examined for their compliance. But they go further to protect their communities. Financial institutions strive for excellence by constantly innovating in the face of emerging threats and changing customer needs. Advances in tactics and technology mean that, increasingly, attempted fraud is intercepted and blocked before it is completed and losses occur. This constantly-evolving, dynamic landscape is why the financial services industry embraces a forward-looking approach to payment security issues.</p> <p>Security professionals at regulated financial institutions work closely with state and federal law enforcement agencies to anticipate threat trends and combat new methods of attack. They collaborate with industry colleagues and in other sectors, in forums such as the Federal Reserve's Secure Payments Task Force. The American Bankers Association fully supports the goals of the Task Force, and along with other financial services trade associations and their members, has contributed significant energy to ensuring its success. We thank the Federal Reserve System for their willingness to facilitate many of the improvements to these documents which our sector has contributed and their interest in tapping into the subject matter expertise residing in America's banks.</p> <p>Declaration of Objection<br/>Payments are best protected by multiple layers of security deployed using a dynamic strategy which anticipates and responds to emerging threats. There is no "standard" solution which solves payment fraud. Security is inhibited, not enhanced, by government mandates or near-mandates, which have failed when tried in other contexts. It is important to America's bankers that the freedom to innovate which many sectors rely on to improve consumer outcomes is preserved in the payments security arena, so that all stakeholders can reap the benefits of competition working towards a more secure payments system. Central planning directed towards a decentralized and shifting problem is unlikely to yield durable improvements for consumers.</p> <p>Technologies like encryption, tokenization, and user authentication are among the security layers which can protect payments integrity in appropriate contexts. No single technology is appropriate in every situation at any given time and the flexibility for the private sector to deploy, modify, and substitute measures quickly is essential to defeating emerging threats. Financial institutions and their partners have been the leaders in deploying the listed technologies and offering them to other sectors for their adoption. Financial institutions are the drivers of iterative improvements in these technologies. Today, America's banks are hard at work deploying them in creative ways, however there are areas of the economy where there remain opportunities for greater use.</p> <p>The current draft language around these technologies captures the accurate conclusion that these technologies could enhance security when pragmatically deployed in appropriate situations. However, the additional clause that conditions these benefits materializing if the technology is "based on open standards" is vague and could create confusion and delays in real-world implementation. This is especially true while there are existing standards efforts underway, many long-lived and some relatively recently begun.</p> <p>General statements that "open standards" could "enhance security" also create the impression that actual technologies are fundamentally dependent on governance structures if they are to reduce fraud. We are unaware of data to support this implication and believe that the objective evidence bears out the independent value of these technologies regardless of how their innovations evolve. Some of the most important innovations occur outside and prior to the establishment of formal "standards," and their potential contributions to payment security should not be derogated based simply on their administrative profile.</p> <p>Further, the governance structure of standards and an implied preference for one type is a non-security and private sector issue outside the scope of the Task Force. This is an area of competing views and a diversity of perspectives which should not be reduced to one view in a unity document.</p> <p>Our concern is rooted in the view that consumers should be afforded the best protection available and financial institutions should be comfortable making decisions to that end without the added obstacle of evaluating the private sector administrative governance model of any technology. In the absence of provable evidence for the assertions currently made around standards in the draft documents, we respectfully propose the following revisions in all affected sections:</p> <p>Greater deployment of tokenization, user authentication and encryption could enhance payment security.</p> <p>Greater focus on development and adoption of risk-based cybersecurity rules and frameworks could enhance security.</p> <p>Standards related to PIN capture need to be expanded to include new and evolving forms of PIN entry.</p> <p>The Task Force should prefer simplicity wherever possible and our suggestions are made in that vein. We hope that these proposed alternatives will receive consideration between the DMF and publication.</p> |
| Zhang             | Yuemei     | Large Financial Institutions | Consent      | <p>I would like to see our continued effort to improve those profiles, especially, I'd like to focus our effort on the technology or procedural standards, instead of standards related to regulations or rules. Also, we should avoid referring to "open standards" as this is a confusing term.</p>   |