Secure Remote Payment Council (SRPc)
Authentication Work Group Position Paper 1
April 30, 2015

The mission statement of the SRPc Authentication Work Group is to collect, evaluate and comment upon common ideas, statements and positions promulgated in the payments industry related to transaction security, with a focus on authentication methods.

POSITION STATEMENT

For its inaugural effort, the Authentication Work Group set the foundation for subsequent evaluation by making the following position statement:

> "The payments industry must work collaboratively to endorse viable authentication methods that can be supported and used by all industry stakeholders. "

The SRPc Authentication Work Group agreed that authentication technology would be most successful in deterring fraud if it were used at every distribution channel including brick and mortar. However, the scope of this effort is focusing more narrowly on new authentication schemes and innovation as applied to the ecommerce and mobile channels only. The mobile channel, in particular, presents unique challenges because it operates both in the physical space and in the mobile application. To that end, the Authentication Work Group agreed to limit the review of authentication technologies to only those that can be remotely authenticated.

What are the success criteria for a viable cardholder authentication solution?

To meet the needs of all industry stakeholders, the SRPc's view is that the authentication solution must meet the following success criteria:

- Must be effective
- Must be ubiquitous and broadly adopted
- Must be easily federated
- Must not be exclusionary, e.g., it must comply with open standards
- Must support multi-factor authentication in accordance with FFIEC guidelines
- Must have a positive ROI, e.g., must not cost more than the fraud incurred
- Must not be too complicated such that it degrades the consumer experience or impedes their ability to pay
- Must provide a high degree of security for Customer credentials
- Must reduce end-to-end societal cost, and remove cost from the payment infrastructure

Effectiveness means to be able to validate the means of authentication in a digital or automated manner, as opposed to paper or manual. Return on investment goes hand-in-hand with effectiveness. In order to have value, any particular authentication scheme must be rationalized.

The authentication solution must be flexible in its application, enabling stakeholders with the choice to move to a less stringent type of authentication (e.g., based upon the transaction type, dollar amount, or point of origin), and bear the resultant liability. For example, a Merchant may choose to support a different form of user authentication for a small ticket purchase compared to that used for a purchase of a large dollar amount, but then must be prepared to assume some or all of the liability for the choice of authentication method that is used.

What constitutes a viable authentication solution?

One of the major attributes of a viable authentication solution is the degree of difficulty in compromising the solution. The earmark of a viable solution is that it represents an improvement on an existing methodology or solves a niche problem not provided by other solutions. For a solution to be viable, it also must be less expensive than the absence of authentication altogether. While the Authentication Work Group views that dynamic authentication is better than static, they also agreed that static is better than no authentication at all. Collecting signatures at the POS essentially provides no authentication at all unless signatures are digitalized and validated.

The most effective solutions for authentication in today's online environment are moving toward biometrics and dynamic PINs (i.e., one-time password or OTP). Cloud based solutions, priced on a per transaction basis, are making OTPs more affordable. Biometrics is still more expensive, but biometric functionality is being built into devices, such as phones and tablets, where the consumer fronts the cost for the technology.

The ultimate in payment security is best achieved when the authentication solution is used in combination with other security measures like tokenization and end-to-end encryption.

Stakeholder Requirements

Consumer Perception Drives Usage

The value in the authentication techniques available to support the ecommerce environment lies in Consumer perception. *Consumers need to have a predictable experience with authentication techniques.* The underlying principles for viable authentication solutions include:

- The authentication solutions should not lengthen the purchase process.
- The authentication solution should be simple and intuitive to use.
- The user should understand the implications of using the authentication solution including how the solution benefits them, or if use of the solution alters their rights or obligations relative to the payment being made. For instance, there have been cases where the use of a PIN in an ATM transaction has effectively reduced a cardholder's right to repudiate the transaction after the fact.
- The authentication solutions should be unobtrusive.
- The authentication solutions should ensure Consumer privacy.
- The authentication solutions should be cost effective for all stakeholders to implement.

Authentication methods must support the consumer's choice of payment option. Consumers want to perform PIN debit transaction online and therefore any authentication solution must support gateway routing to the PIN debit networks.

From the Consumer perspective, any authentication solution must be both easy and comfortable to use. Moreover, Consumers want limited risk exposure and/or hassle factor if fraud were to occur. The solution must be low or no cost to the Consumer, and must support an opt-out provision.

Additionally, Consumers want a trusted authority to be the gatekeeper of their authentication credentials. Consumers have demonstrated that they feel comfortable registering their payment credentials with Financial Institutions and Aggregators such as Amazon and PayPal. In turn, the Financial Institution Issuers and Merchants that are working with the Aggregators need to be comfortable with whoever is handling the authentication credentials on their behalf.

Consumers will gravitate toward solutions that are non-invasive, balancing the level of security with their privacy rights. Techniques such as behavioral scoring will be accepted by the Consumer, particularly when provided by a trusted Aggregator or Financial Institution.

Other Stakeholders

For the other stakeholders, the most viable solutions are those that can be supported across many distribution channels, and with multiple Issuer and Acquirer Processors, and Payment Networks. Authentication solutions must be readily adaptable at the front end so multiple parties can help to develop solutions. All stakeholders want a solution that can be easily integrated into the existing payment infrastructure, using standardized certification processes. Authentication solutions that support ubiquitous access and choice will be more readily adopted.

In particular, Merchants and some Payment Networks want authentication solutions that support least cost routing options for support of PIN debit on the Internet. While authentication solutions for the Internet have emerged, adoption has been slow due to the high degree of abandonment. Those solutions supporting PIN debit on the Internet must use standard message routing in accordance with BINs listed on the BIN routing table.

Merchants also contend that transactions that are authenticated through a consumer authentication solution should be eligible for lower interchange fees, because the transactions are more secure and less expensive for the bank to process. They also believe that some Merchant categories should be entitled to liability shift on chargebacks when they use Customer authentication for card-not-present transactions. However, the Consumers must be made aware of these alterations if it impacts their ability to repudiate a transaction after the fact.

Financial Institution Issuers want choice and flexibility in their preference for authentication solution as a point of competitive differentiation. This requires a delicate balance, however, because there are times when the Issuers' needs are in conflict with the solutions that are implemented at the point of purchase. This can result in Customer confusion at the POS, and cart abandonment in the ecommerce space.

All stakeholders must meet risk profile and regulatory agency requirements. Additionally they will have concerns about reputational risk if fraud were to occur.

CALL TO ACTION

Requirement for Common infrastructure

The online infrastructure must be designed to support a variety of authentication methods. There must be a broad set of solutions that compete, but within an infrastructure that enables interoperability of all authentication solutions. The payment industry wants a flexible market where the online message format or out of band channel enables the Financial Institution to select the type of authentication they want to perform, whether biometrics, one-time password or other option.

Authentication solutions that can be readily overlaid on the existing payment infrastructure are most likely to be readily adopted by the industry stakeholders.

Need for More Collaboration

More collaboration among the industry stakeholders is needed to determine best approaches for authentication. There is an acknowledged need in the market for better authentication solutions to protect against identity theft and counterfeit card fraud. These solutions must have benefits that outweigh the cost. Time to market must be accelerated or proprietary approaches with exclusionary provisions for stakeholders may emerge thereby limiting competition.

Industry collaboration means that all stakeholders sit at the table as equal partners and have equal voice in determining the outcome. To achieve the desired level of cooperation, the SRPc strongly recommends looking to models that have been successful in building collaboration in the payments industry. These include open-consensus standards bodies such as ANSI X9, ISO W3C, International Committee for Information Technology Standards (INCITS), FIDO Alliance and quasi-consortiums such as the Debit Network switches whose hallmark is working cooperatively to build enhanced functionality and capabilities, and reciprocating rules.

About the Secure Remote Payment Council

The Secure Remote Payment (SRPc) is a nonprofit, inter-industry trade association that supports the growth, development and market adoption of debit based internet eCommerce and mobile channel payment methods that meet or exceed the security standards for pinned based card present payments. It will accomplish this by encouraging and supporting those activities that accelerate the implementation, adoption and promotion of these payments. The SRPc's members include merchants, financial institutions, merchant processors, issuer processors, payment brand companies, payments authentication hardware providers, payments authentication software providers and payments consultants. This document does not necessarily express the views and opinions of every member of the SRPc. For additional information, visit www.SecureRemotePaymentCouncil.org .