Secure Remote Payment Council (SRPc)
Position Paper #4 – Discussion Document
User Authentication: Barriers to Adoption and Success Criteria for Market Implementation
December 3, 2015

Position Statement

Identity theft is a gnawing and growing problem. It is a concern for consumers who have or might become victims, and for the financial institutions and merchants who strive to protect them from this crime.

Most common forms of identity theft include (1) existing card account fraud, when a card or its data is lost, stolen, skimmed or breached, and a criminal uses the card itself or creates a counterfeit card to make a purchase either on the Internet or in the physical world; or (2) account takeover, when a criminal obtains the customer's personal information and impersonates the individual to create a new payment or credit account. The latter is a more arduous recovery for the victim, while the former is more prevalent because payment credentials can be readily exposed. One potential solution to existing account fraud is the concept of User Authentication. It should be noted that authentication of the user may not have a material impact on account takeover, an area that lies outside the purview of the card issuing entities, but it has been heralded as the best defense against Internet and Point of Sale fraud.

What is User Authentication?

The Federal Financial Institutions Examination Council (FFIEC) provides the following definition:

> *"Authentication is the verification of identity by a system based on the presentation of unique credentials to that system. The unique credentials are in the form of something the user knows, something the user has, or something the user is. Those forms exist as shared secrets, tokens, or biometrics. More than one form can be used in any authentication process. Authentication that relies on more than one form is called multi-factor authentication and is generally stronger than any single-factor authentication method. Authentication contributes to the confidentiality of data and the accountability of actions performed on the system by verifying the unique identity of the system user."*

Given the ever increasing amount of personally identifiable information (PII) that is readily available on the Internet, Financial Institutions and Merchants are looking for identity management solutions that are safe and secure. There are a myriad of authentication solutions available in the marketplace, including one-time passwords; device ID; physical tokens and fobs; push notifications; biometrics, such as fingerprints, voice recognition, iris scan, etc.; behavior patterns; database lookup; and social media analysis, just to name a few. They all share common ingredients: something you know, have or are, and there is general agreement that two or more is better than a single authentication vector.

Implementation of user authentication solutions has taken a back seat to the deployment of other security technologies (e.g., end-to-end encryption, tokenization, EMV, etc.) as the industry has been more focused on protection against card fraud rather than identity theft. Yet, from the consumer perspective, identity theft and the ensuing hassle is more important than the actual card fraud.

What have been the barriers to entry in deployment of User Authentication?

- Lack of ease of use for consumers or perception of consumer reluctance to adopt
- Friction of user authentication increases shopping cart abandonment
- Costs of authentication schemes compared to benefits
- Focus on the implementation of other security technologies before user authentication
- Resistance of Issuers to change or modify legacy systems
- Tremendous uncertainty and lack of financial incentive surrounding mobile commerce impacting liability and cost, e.g., will those transactions be treated as card present or card not present?

Are there misperceptions in the marketplace?

Consumer willingness to use authentication technology

Increased incidences of identity theft, account takeover and the never-ending high-profile breaches have caused an outcry from consumers for protection. The industry needs to manage to consumer concerns about false denials due to fear of fraud. Like shopping cart abandonment, false denials can have a significant adverse impact on revenues and the willingness to shop with that Merchant again.

A recent study conducted by MasterCard found that 86 percent of all consumers are willing to take additional steps to be personally involved in fraud prevention.[1] The use of password-locking of tablets and smartphones is a good example of this.

Still, consumers haven't been asking for user authentication solutions. In fact, only a very small percentage of consumers have adopted them. One concern we've heard expressed is the intrusiveness of some proposed schemes. Consumers are wary of giving up the very personal biometric data. It's one thing to lose a password or a Primary Account Number; it's another thing entirely to lose your fingerprints or vein patterns. Biometrics may be too personal a form of user identification for the payments environment. Once biometric forms of identification have been relinquished they cannot be taken back. Can consumers actually trust the custodian of that personal information?

User authentication solutions must become more sophisticated but easier to use and remain friction free, for consumer willingness to grow. A protective balance will need to be struck between the sharing of additional attributes such as biometrics with authenticators and a near frictionless experience for the consumer. Financial Institutions have historically been in an ideal position to fill the role of trusted authenticator.

Most likely the best way for consumers to adopt authentication is to create "consumer choice." Consumers given a choice, albeit from a qualified list of certified technologies, would improve adoption. Some consumers may prefer a "selfie biometric" while others a dynamic PIN pad, one-time-password (OTP) or others. The thought that "we" know the best solution may be a bit pretentious, but sometimes the market and individuals know more about what works.

Even if layered authentication is used, the advantage of a consumer choice authentication world invites consumers to participate and reduces if not eliminates systematic risks. Imagine if any given BIN range had seven or eight different authentication technologies certified for consumers to choose. That adds another dimension of complexity for nefarious forces to deal with and attempt to defeat. Even if one of the certified authentication technologies was compromised only a small portion of the BIN range is at risk.

[1] http://www.pymnts.com/company-spotlight/2015/mastercards-report-on-consumers-and-data-security/#.Vg1cS_m6fq4

The consumer choice could even be extended to a layered approach. Consumers can determine their own layering, for example the consumer can allow a rules-based approach for transactions less than $100 and insist an authentication step such as an OTP for all other transactions. We have the technology to sensitize the payment ecosystem to enable consumers to choose the way they want to ensure their own payment security.

There is one last yet very important benefit to consumer choice. It creates a single experience for that consumer so that no matter where they are shopping, there is the same experience with regard to authentication.

Shopping Cart Abandonment

Data does suggest that this has been a problem. For example, 3D Secure takes measures to validate the user's identity and collect card information for online transactions. This service provides Merchants with a liability shift, and discounts in the form of lower interchange rates or discounts in those circumstances where user authentication has been attempted.

However, Merchants complain that they lose good sales due to the cumbersome enrollment process which causes shopping cart abandonment. The solution has not gotten traction in the US, as large Merchants have implemented their own sophisticated fraud detection tools instead.

The earlier version of 3D Secure redirected the customer from the Merchant site to the Third Party proving to be both time consuming and cumbersome. The latest version of this technology has created a more seamless approach to enrollment to avoid this problem.

Absolute vs. Risk Based Identity Verification

The assumption of "all or nothing" in authentication is not valid in a complex ecosystem where the required strength and certainty level of authentication can vary based upon the use case. Maybe some percentage less than 100 percent may be sufficient for some transaction types and/or dollar amounts. Same is true with customer credentials. When a service provider authenticates a customer, what degree of confidence is needed to determine that individual is who they claim to be. The answer may be different depending upon the reason that the authentication is being performed. Authentication to access a high security facility may need to be more absolute than that needed to make a purchase on the Internet. In fact almost every authentication scheme produces some type of score rather than a binary yes or no answer. The score provides guidance to the risk accepting party which can then assess the risk against the potential reward. The challenge is to balance the cost of user authentication solution to the risk. Authentication solutions should be risk-based, factoring the dollar amount of the transaction while gauging the level of confidence required to determine if the transaction is good. Remember, even low dollar transactions can be fraudulent and are often used by fraudsters to test the account

Who will assume the liability for fraud?

Who assumes the liability (and to what degree) for lost/stolen card holder data or personally identifiable information - Consumer, Merchant, or Issuer? The payment network operating rules are clear on who assumes liability for the misuse of card data, but proving who allowed the compromise to occur is where things get tricky. Currently there is no limited liability protection or insurance to protect against damages. Can transactions be "insured" or the liability laid off to other parties - perhaps for a fee? Would Financial Institutions and Merchants agree to share fraud data and fund an insurance pool?

Regulation E protects the consumer to a limited extent, but regardless of network liability rules, all parties lose. We have discussed that consumers face a significant hurdle repairing their payment credentials. But many consumers also blame either the Merchant or their Financial Institution – or both – for not securing the payment interaction. Not only does the Merchant lose sales, but there is documented evidence that consumers blame their Financial Institution, with many consumers switching from debit to credit, or closing their card account, or even leaving that financial institution entirely. A research study performed by the Identity Theft Resource Center, a not for-profit organization that assists victims and consumers with identity theft, substantiates this premise. Their survey results show that 38.9 percent of consumer changed their bank, credit union or credit card company when unauthorized activity occurred on their existing account.[2]

What we do know is that the value of what is being protected must be greater than the cost of protecting it.

Data, Data, Data

Fraud data must be reported and measured. To accomplish this, transparency within the four party payments system is needed. Currently, the payment system is opaque. There is no authoritative source for actual fraud data. In recent years, the Federal Reserve has attempted to quantify fraud but their results obtained from financial institutions do not align with media reports or Merchant numbers.

Fraud is a problem no one likes to admit and more often than not every victim attempts to downplay and minimize its impact. While all parties agree there are lots of direct and support costs, few parties can agree on actual cost. Additionally, the current interchange model assigns liability without a dynamic financial model and offers little incentive to report or reduce fraud.

Without good data, it is not possible to calculate risk or convince a third party of the benefits that could be obtained with a user authentication solution.

Use Case: Amazon Marketplace

Amazon Marketplace provides a good model for discussion on ways to mitigate fraud. A small, online Merchant joins Marketplace (and pays the fees) for three reasons:

1. "Rent" Amazon's brand to draw consumers to your products and reassure those consumers that they can buy safely because Amazon is in the middle of the process.
2. Layoff Merchant processing complexity, fraud monitoring, rules, etc., to someone who knows what they're doing.
3. Reduce risk of payment fraud.

Amazon is that third-party that essentially allows a small Merchant to layoff several business functions to an organization with scale for a fee. That includes some level of payment risk mitigation. Amazon is in a position to do this as they have account and transaction history relationships with lots of consumers.

Banks (large ones) also have this scale, but strangely enough, they don't operate the same way. The "four-party model" actually puts them at odds with the Merchants. They might be able to use their knowledge of a consumer's transaction habits to lay off risk for a Merchant for a fee. This is the real tragedy of the oligopolistic national payment brand system. A Byzantine, one-size fits all pricing structure separates Issuers and Merchants, not allowing for a competitive market to drive new solutions that mitigate fraud in a mutually satisfactory way.

Of course, in the end, the biggest problem is the size of total fraud in ecommerce. It's too small! In the Amazon example above, for Merchants item #1 is many times more valuable than #2 or #3. Remember,

[2] Identity Theft Resource Center, Identity Theft: The Aftermath 2014 ™.

small ecommerce Merchants pay +25 percent of TOTAL REVENUE on getting consumers to their site or to see their products. Scenarios #2 and #3 are chump change by comparison.

Financial Institutions have allowed Amazon to take a big chunk of their business in fraud protection. There are some beneficial lessons learned from Amazon Marketplace about conducting business in the card-not-present environment.

Call to Action

The SRPc proposes the following guiding principles on the user authentication:

(1) **User authentication solutions must support a layered approach for security including multi-factor authentication**.

FFIEC provides guidelines for approved authentication techniques and endorses a layered approach to authentication entails using multiple factors – something you have, something you know and something you are. The strength of the authentication increases with each additional authentication factor that is used. The industry needs to phase out solutions like static passwords, site keys and challenge questions which are overused and easy to compromise, and replace them with stronger authentication methods.

Out-of-band authentication is a type of two-factor authentication that requires a secondary verification method through a separate communication channel along with the typical ID and password. This type of authentication helps to protect against man-in-the-middle attacks.

(2) Interoperability is key!

Financial Institutions and Merchants must be able to choose the technology they want for authenticating customers – whether that technology is one-time password, biometrics or other emerging solutions. Financial institution choice ensures the flexibility to add new parameters and/or swap out technology for alternate solutions, as the fraud landscape changes.

FFIEC provides guidelines for approved authentication techniques, which should be followed.

(3) The infrastructure framework for user authentication must connect Merchants and Financial Institutions.

User authentication framework should apply equally across all delivery channels, but may differ in methodology by channel based on the risk-weighting of a given transaction.

The industry must work cooperatively to promote better models. There are two approaches: (1) Merchant Authentication, a closed loop, proprietary solution like Amazon where the customer registers and authenticates their profile; or (2) Financial Institution Authentication, which ties the payment to the customer registered credential.

While some larger merchants have the capability and desire to handle authentication in their own systems, many Merchants without that level of expertise want the Issuer to take this responsibility, possibly facilitated by credential checking done by a switch or payment network.

(4) User authentication solutions must be easy for the consumer to use and must provide a high degree of protection against misuse of personally identifiable information (PII).

User authentication solutions must focus on ease of use and/or enhancing the customer experience to foster consumer adoption. While added security will not necessarily change consumer habits, the industry should focus on authentication solutions that enable customer convenience and simplicity.

For example, an authentication technology that could eliminate key strokes while speeding up the total transaction time when purchasing online would be well received by consumers and Merchants. Authentication technology must be developed such that it operates seamlessly across multiple consumer devices – PCs, tablets and mobile phones – so that it is readily accessible.

The solution should be minimally intrusive for consumers and should have an opt-out feature.

(5) The industry should use effective authentication methods appropriate to the level of risk.

FFIEC guidelines recommend selecting authentication mechanisms based on the risk associated with the particular application or services. Finding the proper balance between the level of risk protection and cost is tricky. What is "good enough?"

User authentication framework should apply equally across all delivery channels, but may differ in methodology by channel based on the risk-weighting of a given transaction.

The cost of the solution cannot be more than the amount of the fraud it seeks to eliminate. Also, the solution should raise the cost to the hacker to at a minimum the reward threshold. Put another way, it should be a disincentive to fraud.

(6) A balanced governance structure is needed as standards for authentication continue to unfold.

The industry must address the issue of liability in an equitable manner for all stakeholders. Currently, liability is determined by whichever entity sets the rules and is often a binary decision. All parties which are potentially liable must be able to participate in the framework.

A free and transparent marketplace will generally provide the correct balance between risk and reward without the need for government intervention.

Or, how about a "no fault" concept? Depending on the nature of the theft and loss, each party has statutory liability. This might spur an insurance market that would drive innovation. Car insurers have certainly had a major influence on automobile safety, for instance.

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 .