MAG

MERCHANT ADVISORY GROUP ®

Merchant Advisory Group Tokenization Recommendations

The Merchant Advisory Group (MAG) sets forth below recommendations regarding tokenization, which we believe will provide the greatest level of protection against fraud, enhance competition and provide the highest level of return on investment for commercial stakeholders. Given the existing unhealthy level of market concentration in the payments industry, we believe these recommendations will help avoid further concentration of market power due to the imposition of proprietary technology on the market by the payment networks that are already in a position of dominance.

Many merchants, particularly in the e-commerce space, have developed their own tokenization solutions and products. These products and solutions protect data that is much broader than just payments, and were created to fill a security void, in part, created by lack of innovation by the card industry. Adoption of narrow payment card-only tokenization schemes should not be required of any merchant or issuer by any network or processor unless the network or processor assumes all costs and liability associated with it.

It is critical that tokenization standards be developed in an open standards environment in order to ensure a competitive landscape under which the technology and payment stakeholders can evolve and deploy the most effective security measures for the benefit of U.S. businesses and consumers.

Open Standards Development & Interoperability

- Tokenization standards should be owned and managed by an accredited standards body, which enables democratic representation of all stakeholders.
- Tokenization standards should be developed with the objective of interoperability and practical application across multiple facets of commerce. For example, the same system that tokenizes payment card data should be able to tokenize other data points, such as a driver’s licenses, passports, or prescription numbers that may be sent as fields necessary for authorizing a transaction or for other purposes.

Deployment of Effective Security Solutions:

- Solutions should be focused on building a solution for a digitized economy instead of grandfathering in an old system and broken market into a new platform. This would likely be addressed by working in an open standards environment.
- Tokenization and encryption must be end-to-end. This implies that transactions, which originate at the merchant point of sale must be tokenized and/ or encrypted completely through to the party that issues the card.
- Today, merchants' fraud detection systems are highly reliant on the full card number. Tracking card registration, transaction velocity and general use are industry standard fraud mitigation techniques. This allows merchants to watch for card usage across accounts, catching fraud in advance of issuers knowing the card number has been compromised. Merchants are on the front lines of fraud detection and need to be able to have access to data to be able to identify fraud. While EMVCo's tokenization solution claims to improve security by including an authentication step, it puts merchants in a passive position when working to manage fraud out of the system.

Foster a Competitive Marketplace:

- Tokenization standards should enhance competition and promote a free market.
- Tokenization, like all technology, should be evolutionary, which is unlikely absent competition.
- The ability to generate and provide tokens must be done in an open, competitive, and interoperable environment allowing an open path for any capable party that wants to serve as a token provider and manager to do so. Such token service providers would agree to meet specific standards and undergo security audits based on accredited standards criteria.

Common Sense Operations & Data Management:

- Care should be given to existing tokenization products currently at market as many merchants and acquirers have been tokenizing data, including payment card data, for years. Layering solutions on top of one another – essentially tokenizing a token – is not the most common sense or efficient business solution.
- Data captured through tokenization should only be used for security purposes, and any secondary use of that data for marketing or other purposes by networks or issuers should be strictly prohibited and enforced.