PAYMENT INSECURITY: HOW VISA AND MASTERCARD USE STANDARD-SETTING TO RESTRICT COMPETITION AND THWART PAYMENT INNOVATION

Card payments have experienced explosive growth over the last ten years. As of 2017, debit and credit card payments accounted for 54% of all U.S. consumer purchase payments by count and 55% by value, dwarfing even cash (at 35% and 15% respectively), according to a report from the Federal Reserve Bank of Atlanta. The same report states that card payments are seeing robust growth, increasing 10.1% by number and 8.4% by value from 2016 to 2017.

But as card usage has increased, so also have real concerns about fraud, particularly in the United States. The U.S. alone accounts for nearly half of all fraud in the world, but only for about one-quarter of all transactions. Given this, it is especially important to examine the roles and practices of U.S. payment standards setting bodies, particularly EMVCo.

KEY TAKEAWAYS

- EMVCo is a vehicle for collusion among the card companies on payment standards.
- EMVco has sacrificed payment security for the convenience of the card companies and for retaining or increasing those companies' transaction volume. Its standards constantly limit merchant choice for transaction routing, in violation of U.S. federal law.
- The U.S. payments industry's competitive landscape is harmed by allowing EMVCo to set standards, lagging behind many countries when it comes to payments.

WHY STANDARDS SETTING IS IMPORTANT

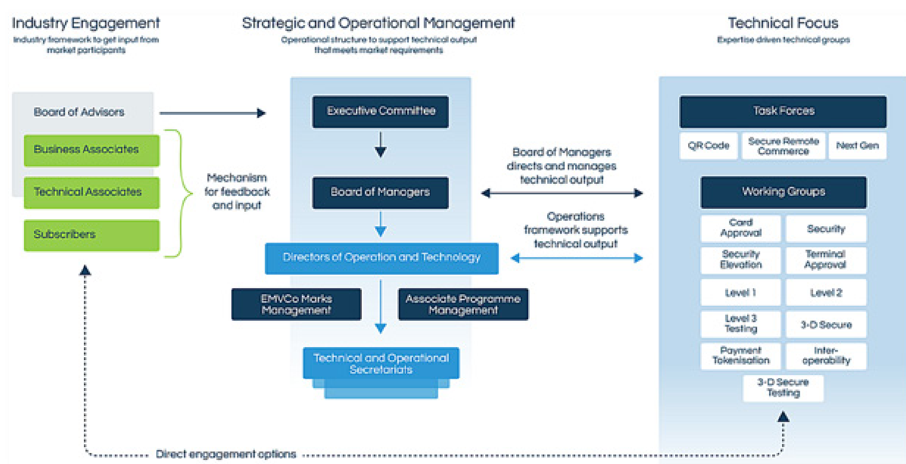
How security standards are produced and who produces them is a critical consideration in modern economies. Any standards that give advantage to certain companies over their competitors are a valid source of concern as this impacts the welfare and competitiveness of the U.S. payments system. Such practices are ultimately detrimental to security, as particular companies' interests are naturally prioritized at the expense of better and safer technologies. Open standards setting is key to ensuring that no one industry dominates the standards setting process.

HOW DOES EMVCO COMPARE TO OTHER STANDARDS SETTING BODIES?

	W3C	ANSI	EMVCO
Is active membership (i.e. not just in an advisory capacity) open to all?	Y	Y	N
Is mission and work defined and agreed to by all participating members?	Y	Y	N
Are decision making roles available to all participating members?	Y	Y	N
Are meetings and proceeds documented and open to public review?	Y	Y	N
Are members specialized in the specific technical areas where they contribute to standard development?	Y	Y	Primarily Chip Cards
Appeals process open to all members to resolve differences in standard?	Y	Y	N

EMVCO'S ORGANIZATIONAL STRUCTURE

In contrast with recognized standards-setting organizations, which advocate openness and inclusivity, EMVCo decisions are effectively made by its six owners – Visa, Mastercard, Discover, American Express, JCB, and China Union Pay. There is no consumer group, merchant, unaffiliated network, or US financial institution that has a final voting voice in EMVCo's standard setting process.



HOW ARE EMVCO'S STANDARDS DETRIMENTAL TO PAYMENT SECURITY, INNOVATION, AND COMPETITION?

The impact the lack of multi-stakeholder representation in EMVCo has on the payment system is real and measurable. In the United States, the payments industry spends millions of dollars every year complying with standards set by EMVCo and implemented by the card companies as de facto standards. This high level of investment prevents the use of capital to innovate or develop other alternative payment methods. This paper examined a few examples of how EMVCo standards negatively impacted security and/or prioritized the competitive interests of its executive committee members over that of security and innovation.

> "EMVCo's ownership by the credit card companies has put profits ahead of security, driven up costs for businesses and consumers alike, and has left the United States with a fraud-prone payments card system even as fraud has been reduced in the rest of the world."

In much of the rest of the world, when chip cards have been introduced, they have been used with personal identification numbers (PIN). The chip authenticates that the card is valid, and the PIN authenticates the user. PIN is a valuable security tool in reducing lost or stolen card fraud. But in the United States EMVCo introduced the less-secure chip-and-signature, limiting the competition that Visa and Mastercard could face from unaffiliated networks.

EMVCo adopted expensive, complex and difficult-to-implement technology such as NFC which helped preserved the status quo for the card companies and protected their market share.

EMVCo established tokenization standards that excluded non-card payments, ignoring the work of other standards-setting organizations such as the American National Standards Institute or The Clearing House. EMVCo pushed aside calls for open standards and instead issued a tokenization standard that discriminates against unaffiliated debit networks.

EMVCo ignored the work of other standards-setting organizations such as the Fast Identity Online (FIDO) Alliance and World Wide Web Consortium (popularly known as W3C) that were developing open authentication standards for both card and non-card systems. Instead, EMVCo is regressing to 3-D Secure, an old standard inherited from the card companies and that EMVCo is trying to position as a global authentication standard. 3-D Secure 2.0, as this new standard is being called, is likely to introduce much friction during the checkout process and create obstacles for routing of debit transaction through unaffiliated debit networks.

EMVCo has introduced the Secure Remote Commerce standard, which purports to become a new integrated checkout platform for online payment. Neither EMVCo nor the card companies have fully explained and justified the reason for this standard. Secure Remote Commerce has the potential to be leveraged as competitive pre-emption tool that may limit participation from non-card company payment methods and to hinder merchants' ability to route transactions through unaffiliated debit networks, creating higher dependencies on the card companies and increasing merchants' payment processing costs, as well as potentially violating federal law for debit transactions.

EMVCo portrays itself as a technical specification development organization with no enforcement power over the card companies. Yet, the card companies are EMVCo. Both EMVCo's executive committee and its management board are composed of long-term card company employees. Accordingly, it is of little surprise that its specifications and ensuing de facto standards are designed to meet the needs of the card companies rather than the U.S. payments system as a whole.

EMVCo's current structure is not designed to develop, nor capable of developing, open standards. Its "closed" standards have repeatedly failed to properly address ongoing challenges to payment security and inclusivity at a time when collaborative and competitive standards will be needed to innovate, and most immediately, keep up with upcoming industry developments such as open banking or "push" payments. Given its current organization, staffing, areas of expertise, internal policies and inclinations, EMVCo is not a neutral technology standards body let alone "the common voice of the payments industry."

IN CONCLUSION

It is our conclusion that the U.S. payments industry is being harmed by the card companies and EMVCo. The setting of payments standards for topics such as authentication and tokenization should be migrated away from EMVCo to independent and neutral national or international standards-setting bodies. EMVCo's ownership by the credit card companies has put profits ahead of security, driven up costs for businesses and consumers alike, and has left the United States with a fraud-prone payments card system even as fraud has been reduced in the rest of the world.

READ THE FULL WHITE PAPER AT
SECUREPAYMENTSPARTNERSHIP.COM

SECURE PAYMENTS PARTNERSHIP