



## The Role of the EMV<sup>®</sup> Specifications

This paper shares an insight into the worldwide success and flexibility of the EMV Specifications.<sup>1</sup>

EMVCo is the global technical body that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV<sup>®</sup> Specifications and related testing processes. This provides consumers with the ability to make card-based payments regardless of location, and for merchants to accept them.

EMVCo engages with payments industry stakeholders, including card issuers, technology vendors and merchants, from around the world to develop specifications designed to: support interoperability, security and innovation, fuel and simplify product development, and accelerate speed to market.

EMVCo was formed in 1999 to enable the development and management of specifications to address the challenge of creating global interoperability amongst different countries and to deliver the adoption of secure technology to combat card fraud, while enabling innovation in the payments industry. Today:



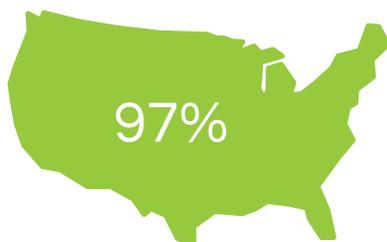
There are **8.23bn** EMV chip payment cards in global circulation.



**58.7%** of cards issued globally are interoperable utilizing EMV Specifications.



**76.7%** of all card-present transactions conducted globally used EMV chip technology.<sup>2</sup>



In the United States, the Federal Reserve Bank of Atlanta reports that “the majority of general-purpose credit and debit cards issued in the United States today contain a chip, with nearly all (97%) of the country’s payment value occurring on these cards.”<sup>3</sup>

<sup>1</sup> For further information on how EMVCo operates, please read the Operating Principles at [www.emvco.com](http://www.emvco.com).

<sup>2</sup> Data reported is for a twelve-month period. In regions where EMV is newly deployed and/or being actively rolled out, the twelve-month reporting figure may lag or under-represent the current transaction percentage.

<sup>3</sup> Federal Reserve Bank of Atlanta, *The Future of U.S. Fraud in a Post-EMV Environment*, June 2019

The EMV Chip Specifications were designed to facilitate the reduction of fraud at retail store locations, as the payment information stored on an embedded microchip is very difficult to counterfeit. The EMV Chip Specifications support seven types of cardholder verification methods (including online and offline PIN) and any combination of them, as well as ten biometric verification types.

- Chip cards offer transaction security that traditional magnetic stripe cards cannot provide, while also promoting global interoperability.
- Counterfeit card fraud is the "leading danger for traditional magnetic stripe cards."<sup>4</sup>
- While the EMV Specifications form part of a layered security approach, the Nilson Report confirms that "EMV technology provides the best protection against losses from counterfeit cards."<sup>5</sup>
- According to Deutsche Bank, "EMV chips have helped to considerably reduce fraud from card-present transactions, as the chip technology has rendered copying the magnetic stripe obsolete."<sup>6</sup>
- In the United States, the Federal Reserve Bank of Atlanta has reported that 'counterfeit card fraud is dropping [...] in a trend that is consistent with other countries' that have migrated to EMV Chip.<sup>7</sup>
- A variety of cardholder verification methods (CVMs) are supported by the EMV Specifications.



Counterfeit card fraud in the United Kingdom has reduced by **90%** since 2008.<sup>8</sup>

Counterfeit card fraud in Canada has reduced by **76%** since 2008.<sup>9</sup>



<sup>4</sup> Javelin Strategy, 'From Application to Transaction: Card Fraud Trends, Threats and Tactics', April 2018

<sup>5</sup> Nilson Report, 'Issue 1068', July 2015

<sup>6</sup> Deutsche Bank, 'Card fraud in Germany', December 2018

<sup>7</sup> Federal Reserve Bank of Atlanta, 'The Future of U.S. Fraud in a Post-EMV Environment', June 2019

<sup>8</sup> UK Finance, 'Fraud the Facts 2019', March 2019

<sup>9</sup> Canadian Bankers Association, 'Learn how to protect yourself from credit card fraud', 2019

The EMV Specifications have evolved beyond EMV chip and now provide a comprehensive technology toolbox that industry participants may use to develop and implement new, innovative, secure, and globally interoperable payment methods for both physical and digital commerce.

- 🌀 Fighting fraud across the payments industry is an ongoing battle. Global trends show that as card-present fraud reduces in a specific marketplace following migration to EMV Chip, card-not-present (CNP) fraud increases as fraudsters target other areas.<sup>10</sup>
- 🌀 EMV Specifications for remote payments include EMV 3-D Secure (EMV 3DS), EMV Secure Remote Commerce (EMV SRC) and EMV Payment Tokenisation.
- 🌀 The Federal Reserve Bank of Atlanta has stated that the availability of these technologies means the “industry is undoubtedly in a much better position today to mitigate CNP fraud than it was in the early days of EMV adoption in other countries.”<sup>11</sup>
- 🌀 EMV 3DS deployments are still in their early years which make published data limited, but it is widely recognised by the industry as a solution to address CNP fraud:
  - *The European Banking Authority has issued an opinion confirming that EMV 3DS “should enable the application of the full range of SCA [strong customer authentication] exemptions specified in the RTS and the out-of-scope of SCA transactions.”*<sup>12</sup>
  - *Banque de France reported that the fraud rate declined for remote transactions in 2018, attributing the improvement as the result of “issuers’ merchants’ and companies’ efforts to improve customer protection by rolling out strong customer authentication solutions such as [EMV 3-D Secure].”*<sup>13</sup>
- 🌀 Deutsche Bank reports that, according to retailers and financial services providers, EMV 3-D Secure and EMV Payment Tokenisation have “yielded good results” reducing card-not-present fraud.<sup>14</sup>
- 🌀 The Federal Reserve Bank of Atlanta states that EMV SRC could “enhance the security of e-commerce transactions through [EMV Payment Tokenisation] and dynamic data.”<sup>15</sup>

**Adoption of EMV Specifications and associated approval and certification processes promotes an interoperable international payments framework, which supports an advancing and diverse range of payment methods, technologies and acceptance environments.**

- 🌀 EMVCo supports various testing and certification programmes.
- 🌀 EMVCo continually seeks ways to support the broader industry and streamline processes.



<sup>10</sup> Federal Reserve Bank of Atlanta, *The Future of U.S. Fraud in a Post-EMV Environment*, June 2019

<sup>11</sup> *ibid.*

<sup>12</sup> RTS refers to the ‘regulatory technical standards on SCA and common and secure communication’, which specifies certain transactions to which an SCA exemption can be applied to balance security and convenience. It also identifies transactions which are considered out-of-scope of the mandate.

<sup>13</sup> Banque de France, *Annual Report*, 2018

<sup>14</sup> Deutsche Bank, *Card fraud in Germany*, December 2018

<sup>15</sup> Federal Reserve Bank of Atlanta, *The Future of U.S. Fraud in a Post-EMV Environment*, June 2019

<sup>16</sup> Interac, *Statistics*, January 2020

The EMV Specifications are available royalty free, designed to be flexible, and can be adapted regionally to meet national payment requirements and accommodate local regulations. Domestic networks across the world have widely implemented EMV Specifications.

- 🌀 The EMV Chip Specifications have been implemented by various domestic debit networks. For example, Interac in Canada reported over 6 billion EMV-enabled transactions in 2018 with a value of \$251.3 billion.<sup>16</sup>
- 🌀 Domestic debit networks, including eftpos (Australia), MIR (Russia), Cartes Bancaires (France), ELO (Brazil), have implemented EMV 3DS solutions.
- 🌀 The EMV SRC Specifications enable all payment networks (including domestic debit networks) to develop an SRC system and provide a means for merchants to promote their brand / logo equally alongside global payment system brands within the EMV SRC payment icon requirements to the extent the merchant chooses to do so.
- 🌀 The EMV Payment Tokenisation Specification - Technical Framework provides a level of commonality across the payment ecosystem to support token adoption while enabling levels of differentiation that promote innovation. Many domestic debit networks are EMVCo-registered Token Service Providers, along with The Clearing House and PayPal.

Implementation of EMV Specifications enables participants in the payment ecosystem to have confidence that the products they issue will interoperate on global secure infrastructures, regardless of where their customers make or receive a payment.

🌀 EMV Specifications are supported by independent, accredited testing laboratories and certified test tool providers. This helps the deployment of approved and evaluated products in the marketplace.

- 74 Approved Testing Laboratories
- 164 Qualified Test Tools
- 7,544 Approved / Evaluated products



EMVCo actively engages the payment community in shaping specifications.

- 🌀 Industry stakeholders from across the world have significant influence on the work of EMVCo, actively participating in regular EMVCo advisory and technical meetings to develop, enhance and evolve EMV Specifications.
- 🌀 During the development of EMV Specifications, EMVCo receives input from its community of over 100 Associates, including merchants, issuers, acquirers, domestic payment networks, technology providers and testing laboratories.
- 🌀 EMVCo engages with regional and global organisations to receive input and share perspective on areas of respective interest.
  - For example, EMVCo, The FIDO Alliance, and the World Wide Web Consortium (W3C) have created a new Web Payment Special Interest Group for organisations to collaborate on a vision for web payment security and interoperability.

➔ Looking to the future, EMVCo continues to evolve the EMV Specifications to support innovation, interoperability and security.

For more information on EMVCo please visit: [www.emvco.com](http://www.emvco.com)