Issue 2 | 2021

EDPS

TECH DISPATCH

Card-based payments

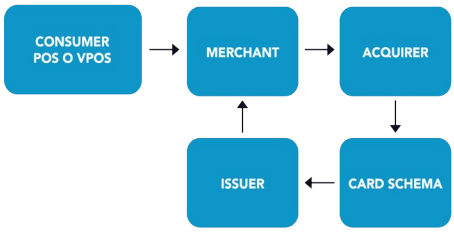
In the last years, **citizens have been using many new technologies that facilitate payments**; such increase has also accelerated due to the COVID-19 pandemic. Consumers and businesses are looking for a more simple, personalised, and economically feasible way of conducting their day-to-day transactions. **Cash payments are are being replaced by *cashless* payments** via an ever-growing landscape of emerging solutions: beyond debit cards or credit cards, *contactless* payments using Near Field Communication (NFC) or Quick Response (QR) technologies and *cardless* payments via smartphone apps are just a few examples of new card-based payment methods.

I. What is a card-based payment?

Card-based payments are the most common cashless means of payment in the European Union[1]. **A card payment is a process where a payer uses a credit or debit card to pay for goods or services offered by a merchant**. Due to the diversity of national and international consumer banks and the complexity of payment standards and regulations, a number of actors support the handling of digital retail transaction. To pay the ***merchant***, ***consumers*** provide their physical or virtual payment card to the ***point of sale*** **(POS)** or in the case of e-commerce to the virtual POS. Whether it is a prepaid, a debit or a credit card, the POS needs to authenticate the user to initiate the payment process. The user data is stored on-card through three different technologies. Magnetic stripe is the oldest form and is rarely used nowadays. User data is also stored on a chip with a microprocessor that offers more security and features. Finally, some cards equip this chip with a tiny antenna for contactless transactions (also called Near Field Communication - NFC). For a transaction, the chip and the POS create together a unique, encrypted code, a so-called *cryptogram* or *token*. Sometimes, the card holder's signature, PIN or biometrics are involved for additional security. This token is unique to each transaction.

The bank of the merchant, the so-called ***acquirer***, provides the *point of sale* (POS) to the merchant, meaning the digital instrument that initiates a transaction through the use of a payment card.

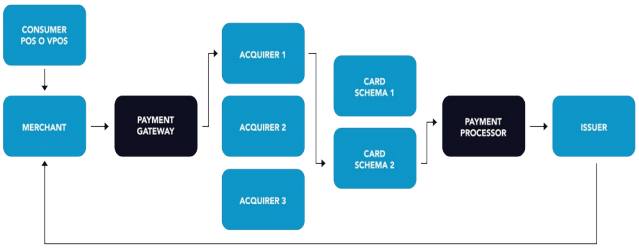
The acquirer provides technical and commercial services to accept, process and settle card transactions on behalf of the merchant. For this reason, it transfers payment information to the so-called *issuer*, i.e. the bank of the payer that issued the payment card, through the ***card schema***. A card schema executes card-based payment transactions, allowing communications between issuers and acquirers involved. It describes rules, practices and standards to exchange payment information among acquirers and issuers. Some countries have their domestic schemas (e.g., PagoBancomat in Italy, Bancontact in Belgium or Girocard in Germany), that also support payments through international schemas such



1 In 2021, the number of credit card issued increased by 6.5% to 609.3 million that represented around 1.8 payment cards per euro area inhabitant.

as VISA or MasterCard (called co-badging) for cross-border payments. When payment is authorised, the issuer will withdraw money from the consumer's bank account and the acquirer will transfer money to the merchant's account. Within this process – also called "***four party payment card scheme***", the *merchant* and the *issuer* have a direct business relationship with the consumer and must implement *know-your-customer* (KYC) rules and comply with the EU's Payment Services Directive 2 (PSD2), which requires, for example, strong customer authentication with multiple factors.

Due to the growing complexity of the payment ecosystem, many payments involve two additional actors that simplify the process for the merchants and absorb operational costs as software connection between different actors in the process.



The ***payment gateway*** is a software that facilitates the payment transaction giving merchants access to various acquirers and helps to reduce their costs by selecting the schema with the lowest transaction fee for each payment of all schemas supported by the consumer's card. Some payment gateways also offer additional services to the merchant, such as reporting, as well as fraud and payment acceptance management. Usually, the acquirer that provides the POS to the merchant also provides payment gateway services.

A ***payment processor*** is a software that processes payments and executes them on behalf of an issuer, taking the money from the customer and depositing it into the merchant's account, as well as providing connections with different card schemas. Moreover, the processors maintain merchant accounts, provides additional services and facilitates settlement processes. The payment ecosystem also belongs to the third-party payment software and hardware vendors that develop POSs and computer systems for the merchants.

All around the world, **new payment methods are growing to enable frictionless and more secure payment experiences**. Most of them rely predominantly on the process illustrated so far.

II. What are the data protection issues?

Card-based payments rely a lot on data processing operations. The diversity of actors involved in the process and the intensity of these processing operations have many data protection implications.

II.1 Anonymity vs. traceability

Only cash payments do not inherently require the **processing of personal data**. Traceability is implicit to each card-based payments due to its functioning, exposing data subjects to a multitude of risks. Though proposals for digital anonymous payments such as GNU Taler are being developed, they see no relevant adoption so far.

II.2 Necessity and Proportionality

Different actors in the card payment ecosystem need to process different personal data based on the purposes they must achieve. For example, the merchant and the issuer are obliged to identify the customer to initiate the transaction and to meet the anti-money laundering legal requirements. While the other actors do not have to and can use anonymised or pseudonymised data, data subjects may face risks of misuse of personal data. In addition, the payment sector is one of the **most regulated sectors**. Actors in the payment ecosystem have to comply with sector-specific financial regulation that introduces many requirements with respect to the processing of personal data, such as specific data retention periods or reporting obligations.

II.3 Processing of special categories of data

A card-based payment transaction identifies at least the payer, the receiving merchant, the amount of the payment and the good or service paid for. If not provided from the outset, the location of the merchant can be inferred and, as such, the location of the consumer at the given date and time. The name and, if available, category of the merchant may give insights into the consumers' activities: €2 spent at the Central Station Coffee Shop, €20 spent at the lake-side boat rental service, €100 spent in an abortion clinic, €300 spent in a nightclub followed by a hotel reservation in the consumers' hometown. Under specific circumstances, transactions allow to

infer consumers' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and sexual life and orientation, and are therefore subject to elevated data protection requirements (see Art. 9 GDPR). What is more, many actors in the field observe the behaviour of the payer in order to recognise patterns and prevent fraud attempts as described in II.7. These processing activities generate the so-called *soft biometric* data[2] that might fall into the special categories of data.

II.4 Roles and Responsibilities

Due to the many and diverse actors within the card payment ecosystem, **recognising data protection roles is often difficult**. Understanding these roles is essential for a correct application of obligations and responsibilities of the GDPR. For example, understanding who decides which processing of data is essential to determine who will have to notify a possible data breach or to whom data subjects should refer to in case they would need to exercise their right of access. For example, a payment processor is usually a data processor of data controlled by the issuing bank.

II.5 Transparency and control

If consumers choose to pay electronically with their cards, the payment is processed according to the conditions set by the issuer, the acquirer and the card schema. Those conditions are often imposed to the merchant who usually lacks sector-specific knowledge and/or contractual power. The diverse actors and the underlying personal data processing operations presented in Section I remain **opaque** to the consumer with no further choice after having decided which card to use.

Some consumer banks (issuers) also collect consumers' consent to process payment data for other purposes that are not strictly related to the management of the payments. As described in II.7, data sharing with third parties for profiling activities might results grounded on **unfree consent,** that is, as such, invalid. Furthermore, they risk to lose control over their payment data regarding third parties.

II.6 Data Retention and Surveillance

Tracking payments of a person can describe the consumers' life in great detail. Credit cards can lead — and have led — law enforcement officers to suspects. This is also reinforced by the fact that applicable financial regulations prescribe retention periods between 3 to 30 years after termination of the bank account. While the fight against tax evasion, money laundering, international crime, etc., are important objectives for our societies and rely on data retention, this data collection relates to many aspects of the private lives of most citizens, with more and more details as they extend their use of digital payments. Repurposed in the future or leaked by accident, such a huge data collection presents a general risk of mass surveillance and unintended use.

II.7 Automated Decision Making and Profiling

Card-based payments do not usually require automated decision making and/or profiling to take place. However, payment data is often used for purposes other than those strictly related to the payment execution. For example, some actors in the process could follow up on customer purchase patterns to avoid fraud, going beyond their legal obligations on fraud prevention. Moreover, payment providers may collaborate with private credit scoring companies that inform landlords, creditors and service providers about the individual trust score of their future clients. These kind of profiling activities could also produce special categories of data, as already described in Section II.3. Data obtained from the payment process is also used by merchants in tailoring their offering, using profiling techniques to understand a payer's spending capacity or their preferences to increase the effectiveness of certain marketing campaigns. When these activities happen, many risks can emerge. For example, consumers may suffer from non-transparent, unfair or biased decisions based on imperfect or opaque algorithms or inaccurate/incomplete data. In some countries, such as China, governments already use payment data to profile their citizens and to influence certain behaviours[3].

2 E. Kindt. *Privacy and Data Protection Issues of Biometric Applications*, p. 35. Springer (2013).

3 Wikipedia. *Social Credit System.* (2021). https://en.wikipedia.org/wiki/Social_Credit_System

II.8 Security

Even if security has always been considered a pressing need in the design of payment solutions, the complexity of the card payment process and the number of actors, software and hardware involved continue to produce a number of security risks ranging from card forgery to more sophisticated techniques. One of the biggest breaches of all times involved the payment processor Heartland Payment Systems in 2009[4]. Millions of credit card and debit card transactions were breached, including the information encoded in the magnetic stripe of cards, enabling criminals to potentially manufacture counterfeit cards. More recently, a security flaw in the payment software has been exploited against a supermarket chain in Sweden, leading to the suspension of the business for an entire weekend. As these examples show, ensuring the confidentiality, integrity and availability of the data processed within the card-based payment ecosystem is key to maintaining the trust of payers in the market and to ensuring business continuity. In previous decades, many security standards have increased in the payment field, mainly from the industry. In regard to on-card information, magnetic stripe has been deprecated because of its low security. An EVM (Europay, Visa and Mastercard) chip is nowadays installed in all payment cards because of its increased security. Another important aspect relates to verification of the identity of the payer. A secret PIN is going to be paired with biometric sensors installed on-card to improve security.

Moreover, the *Payment Card Industry Data Security Standard* (PCI-DSS) has been issued and maintained by the PCI Security Standards Council since 2004. It covers several different aspects of the electronic payment life-cycle, such as how to protect sensitive cardholder information or how to design software and hardware products. PCI-DSS was released when card-based payments were already widely adopted with a jeopardised set of technologies, some of which proved to be insecure. Deviations from current technologies would require a re-design of the payment process and would entail huge costs if implemented worldwide. As a result, PCI security standards are compensating for the vulnerabilities by building up additional layers of security controls around existing technologies. For this and other reasons, in recent years, many payment actors have failed to secure data and this resulted in large data breaches, triggering GDPR requirements on notifications, both regarding data protection authorities and data subjects. The European Commission has recently proposed the Digital Operational Resilience Directive[5] for improving resilience of the financial sector against cyberattacks and monitor third-party ICT providers.

III. Recommended Readings

European Central Bank. *Payments statistics 2020.* (2021).

S. Gomiz. *Hacking Point of Sale*. Wiley (2014).

S. Chishti, T Craddock. The PayTech Book: *The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*. Wiley (2020).

European Commission. *Study on the application of the Interchange Fee Regulation.* (2020).

European Central Bank. *Study on the payment attitudes of consumers in the euro area.* (2020).

N. Arvidsson. *Building a Cashless Society.* Springer (2019).

This publication is a brief report produced by the Technology and Privacy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Issue Authors: Stefano LEUCCI, Robert RIEMANN
Editor: Thomas ZERDICK
Contact: techdispatch@edps.europa.eu

To subscribe or unsubscribe to TechDispatch publications, please send a mail to techdispatch@edps.europa.eu. The data protection notice is online on the EDPS website.

ISSN 2599-932X
HTML: ISBN 978-92-9242-706-1
QT-AD-21-002-EN-Q
doi 10.2804/859230

PDF: ISSN 2599-932X
ISBN 978-92-9242-705-4
QT-AD-21-002-EN-N
doi 10.2804/661031

4 DartReading. Heartland Payment Systems Hit By Data Security Breach. (2009). https://www.darkreading.com/attacks-breaches/heartland-payment-systems-hit-by-data-security-breach

5 European Commission. Financial services – improving resilience against cyberattacks. (2021). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Financial-services-improving-resilience-against-cyberattacks-new-rules-_en