CHAPTER 4: PAYMENT SERVICES

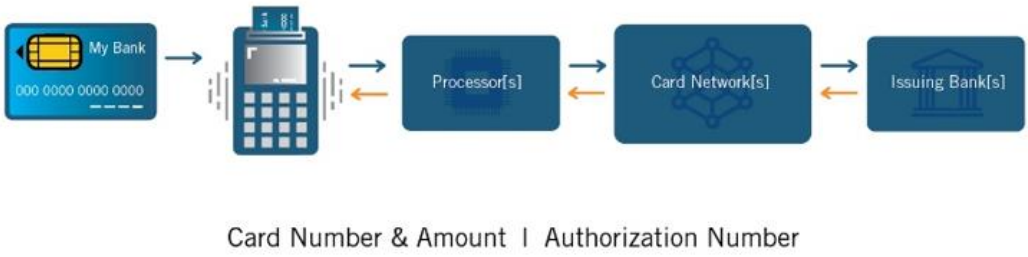
4.1. Sector overview

Technological innovation has dramatically changed the payment services sector. Established firms are developing and adapting new technology in order to defend and grow their existing business. For example, traditional banks are providing end-to-end services across the banking and payments value chain, including through new collaborative payments ecosystems with different industry stakeholders (Capgemini, 2017). Meanwhile, new market entrants (such as fintech firms) are competing to provide new means of payments, often as part of a broader set of digital services (McQuinn et al, 2016). Chinese payment companies offer the best examples of how payment fintechs are using consumer data in ways that differ significantly from established players (Chorzempa, 2018). At one end of the spectrum of new firms is the Chinese firm Tencent, which leverages a complete view of a consumer's behaviour from a broad ecosystem of services (including social, entertainment, news, literature, gaming, sports, and other fields). This gives its integrated payment service a considerable advantage as, on average, 55 percent of a typical Chinese consumer's mobile time is spent interacting with Tencent's services (Whitler, 2018). At the other end are many fintech payment providers (e.g., Stripe, Ayden, Square, etc.) that have developed a niche within the current system (i.e., hardware provider, acquiring services, gateway services, etc.) that have a much different view and use of data for payment services (as compared to Tencent).

Payments are no longer about physical interactions at the point-of-sale (POS). For example, by creating a wholly digital self-checkout, Amazon's physical stores allow customers to skip the traditional point-of-sale completely. Customers expect greater flexibility, functionality, and control over the point-of-sale, especially via smart phones. Overall, there is a clear trend in the payments space toward new partnerships and the use of agile technologies (such as application programming interfaces and web-based tools) and data analytics so that firms are able to provide a more personalized, secure, and seamless service to customers, who are using a growing range of devices and methods to manage payments.

Payment cards (debit, credit, and prepaid cards) continue to play a central role in digital trade given their wide acceptance and use for online payments. Basically, for payments to occur within a card network, an interbank processing platform connects payment card issuers and acquirers (typically banks), which allows the exchange of payment card transactions by a bank's cardholder with another bank's merchant, ATM, or other card-accepting device. Interbank settlement of cross-border transactions typically involves traditional banks relying on an international payment network establishing a multi-bank net/debit position (BIS, 2018). With payment cards, the business model is generally defined as being either a three- or four-party model, in terms of describing the relationship between card providers and banks, cardholders, merchants, and the payment networks. In the case of the four-party model (see Figure 8), the issuer (a payment service firm) provides the consumer with an account (debit, credit, or prepaid), which can operate via a physical card, a smart phone, or online only. The consumer selects products to buy from a retailer, who submits the transaction to the acquirer (mainly banks). The acquirer submits the transaction to the issuer for approval, who (if it approves) remits the retail price to the acquirer, less an interchange fee, who pays the retailer (less a merchant service charge). Finally, the consumer's account is debited the transaction amount.

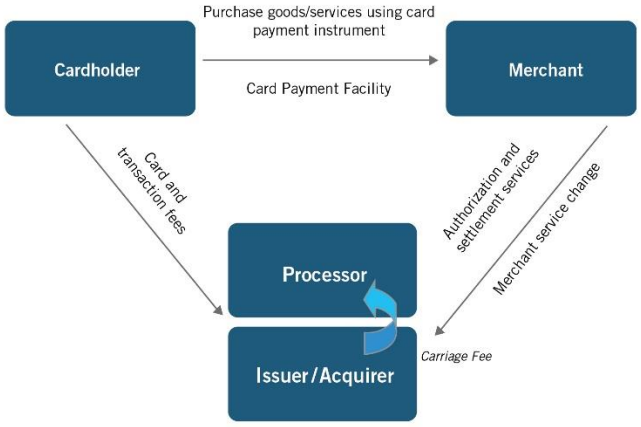
Figure 8. How a typical transaction flows through the four-party model for payment services, which involves merchants, acquirers, issuers, and schemes



Source: Firm A

In a three-party model, the payment service firm acts as both the issuer and the acquirer (see Figure 9). In both models, payment services data flows between these stakeholders as each seeks to play a specific role in facilitating a purchase. However, the sector is undergoing significant change. For example, many banks that issue cards are becoming more digital by offering virtual prepaid, debit, and credit cards for the first time, in order to give customer access to e-commerce solutions.

Figure 9. How a typical transaction works within a three-party payment model for payment services, where the payment firm is both the issuer and acquirer



Source: Firm A

Established payment service providers are coming up with new relationships with merchants in order to access a greater range of data. At the heart of payment providers' traditional business model was the basic service involved in facilitating payments, for which they earned interchange fees. However, the types of firms engaged in payment services, and what services they offer, is changing. A broad range of non-bank and fintech start-ups have entered the sector. This includes, for example, mobile money and financial services like Paytm in India, Stripe in the United States, Go-Pay in Indonesia, True Money in Thailand, Mynt in the Philippines, Toss in Korea, and Alipay in China (and beyond). Also critical for these payment/financial services providers is their integration within the broader digital ecosystem, especially e-commerce marketplaces, email platforms, and mobile apps and app stores. These services also go beyond payments and money transfers, to include a financial dashboard, credit score management, customized loan/insurance plans, and investment services. For example, Go-Pay, (part of ride sharing and on-demand services platform Go-Jek) in Indonesia, provides cashless payments via in-app services, peer-to-peer transfers, and QR code payments at brick-and-mortar stores (Fintech Ranking, 2018). At the same time, established firms are seeking to seize the opportunities through

innovation or partnerships with startups, which is happening all over the world and is seen as a win-win for both sides (Global Payment Innovation Jury, 2017).

Payment services and digital trade

Electronic payment services and digital trade have an intertwined, mutually supportive relationship as consumers want payment services to seamlessly handle the considerable challenges of managing cross-border payments across a diverse range of e-commerce marketplaces, while maintaining a high level of security and privacy (Gefferie, 2018). Payment services represent a critical part of the suite of online services (such as two-sided marketplaces, search functions, or customer review processes) that together make it much easier and cheaper for firms of all sizes to access customers and business partners from around the world, which in turn provides customers with greater convenience and choice. Ensuring that local firms have easy and cheap access to new, low-cost, and innovative electronic payment options is critical to connecting domestic firms with foreign customers. Innovation continues to change how this intermediary process takes place. While digital payments can be made via one of the established card networks (e.g., Visa, Mastercard, or American Express) and card-based point-of-sale devices, they are increasingly being made via mobile apps and devices provided by a growing range of online service providers, such as non-banking institutions and fintech start-ups (Marchetti, 2018).

Quantifying the growth of payment services and their impact on digital trade is difficult. Comprehensive and comparable data on cross-border payments are challenging to compile due to the absence of a common terminology and methodology and an absence of coordinated, large-scale data collection efforts (Marchetti, 2018). Regardless, a number of indirect measures which suggest the rapid global growth in international digital trade and e-commerce (and international remittances and other processes) indicate that the payments sector plays a large and growing role. In 2017, eMarketer estimated that global retail e-commerce sales reached USD2.3 trillion, a 24.8 percent increase from 2016. Of this, mobile-based e-commerce comprises an estimated 58.9 percent of all digital sales[69]. This is further supported by a surge in parcel volumes around the world, which increased 48 percent between 2011 and 2014 (WTO, 2015). There remains considerable room for payment services to drive further digital trade and e-commerce growth. An increasing number of developing economies are moving large numbers of people over to digital payments from their traditional use of cash. For example, formal banking reaches only about 40 percent of the population in emerging markets, compared with a 90 percent penetration rate for mobile phones (Beshouri and Gravrak, 2010).

4.2. Profile of firms interviewed

Firm A

Firm A is a U.S.-based, multinational financial services company involved in facilitating a significant number of transactions annually. Firm A has data centers in multiple regions around the world. Firm A's electronic payments services provide consumers with convenient and secure access to their funds, reduces cash and check handling for merchants, and expands the pool of customers able to engage in domestic and international transactions. Consumers can use Firm A to make electronic payments with credit, debit, and prepaid cards—and other devices, including smart phones.

[69] "Mobile Is Driving Retail Ecommerce Sales Worldwide," eMarketer Retail website, January 29, 2018, https://retail.emarketer.com/article/global-ecommerce-topped-23-trillion-2017-emarketer-estimates/5a6f89f5ebd40008bc791221.

Firm A's services are part of the changes that are blurring the lines between digital and physical commerce, with omni-channel experiences becoming the norm. Firm A is involved in data-driven innovation as payment services continue to change. For example, real-time payments are one part of the next wave of digital payments growth as on-demand services and new ecommerce platforms integrate sellers, hosts, drivers, freelancers, and developers needing fast, convenient and secure access to funds.

4.3. Role of data in firms' business models

Data is critical to each step in capturing, processing, and authorizing a transaction as electronic information (e.g., about the customer, the merchant, the purchase, etc.) is exchanged between the various stakeholders. Although the core function of the data is ensuring that a customer's funds are transferred to the merchant in exchange for a good or service, this is only one role of data in today's digital economy. Every interaction that Firm A's services are involved with generates data, which when analysed in aggregate can yield significant insights. This process at Firm A is indicative of the value chain associated with "big data," which can be generally described as: raw data, aggregated data, intelligence, insights, decisions, operational impact, financial outcomes, and finally, value creation.

For payment service firms, the first few steps of this process come from the traditional and structured data they provide to merchants that aggregates and summarizes their transactions (from a particular day or time period). Other common data used by financial institutions include: identity and demographic data (e.g., ID, age, nationality, address, education, professional details), transactional data (e.g., payment account movement (credits and debits)), payment obligations (e.g., to evaluate the debt service ratio and the remaining net income), behavioural performance data (e.g., credit incidents, debt falling due, potential debt), website, device, and mobile app usage, and the perception of the financial institution's service level (e.g., customer expectations and satisfaction/complaints) (Papp, 2019).

In the middle and final steps of this data analytics process, firms bring artificial intelligence and data science tools to bear in combining and analysing this traditional data with alternative and unstructured data sources, such as voice and message service usage data, social media, satellite imagery, emails, mobile applications, and personal devices. These data analytics processes also highlight the fact that for payment providers to be competitive, itis not enough to focus on lowering the cost of each transaction, but rather using the full spectrum of data and advanced data analytics to provide value-added services to customers, merchants, and others.

In the case of Firm A, it uses aggregated, anonymized data to help retailers understand a consumer's experience before and after visiting a retailer so as to better understand what needs are clearly being met and where the retailer may be missing opportunities. Firm A's use of AI is indicative of the broader trends in the financial services sector. For example, an estimated 53 percent of large merchants and banks in Latin America use artificial intelligence and machine learning technologies (Visa, 2019). Alibaba (which has extensive payment service operations) also provides an example that applies to Firm A's general approach in working with merchants to use technology and payment services to add value for their business. In exchange for a signup fee and a commitment to buy their inventory through Alibaba, the firm gives Chinese retail store owners extensive data collection infrastructure. For one local corner store merchant in China, it led to a 30 percent increase in revenue for the year. Alibaba has achieved a similar transformation, with over one million other small stores and a growing number of larger, "superstores."[70]

[70] Levine, Steve. "China's AI-infused corner store of the future," Axios, June 17, 2018, https://www.axios.com/china-alibaba-tencent-jd-com-artificial-intelligence-corner-store-df90517e-befb-40ca-82d5-f37caa738d54.html.

Personal data is central to data analytics and payments services at Firm A and throughout the sector. Payment services firms like Firm A may use personal data for a number of purposes, including to process payment transactions; to protect against and prevent fraud; and to provide the customer with personalized services and recommendations. Personal data is also shared, for instance, with third parties for fraud monitoring and prevention purposes, as well as those who provide auxiliary services with the customer's consent.

In a way, consumers' concerns over data privacy and protection affect the payment sector's use of data and hence service offerings. A survey for one of the world's leading payment providers showed that 27 percent of respondents stated that privacy and personal data protection was a key driver in trying a new payment method (Visa, 2019). What this highlights is that while consumers appreciate the ability to tailor every experience to suit their individual preferences, their concerns about personal data influence their decisions about whether to take advantage of these data-driven conveniences.

4.4. How policies and regulations are impacting firms' business models

Payment services are affected by several types of data-related laws and regulations:

- Regulations and restrictions about payment services data and its processing, transfer, and storage;
- Regulations about the collection and use of certain categories of data, including personal data;
- Regulations regarding government access to payment services data;
- Market entry requirements (e.g., licensing).

While the Internet may be global, domestic laws and regulations can seriously affect the role of payment services in digital trade. The cross-border payments process is complex, involving many different parties and underlying arrangements that all differ by jurisdiction. This is made all the more difficult as the financial services sector, which includes payments, is typically among the most heavily regulated areas of an economy. Divergent, restrictive and burdensome regulatory frameworks translate into costs, complexity, and lost economic opportunities for firms and customers to use cutting-edge payment services to access the global digital economy.

Rules and laws pertaining to data are critical to payment services, as the collection, processing, storage, and transfer of data is central to the delivery of the service itself and to the analytic processes firms use to improve customer service, drive market insights, and, ultimately, to extract economic value from data (IFC, 2017). This is evident in the fact that payment networks clear and settle transaction information, not funds. A central issue for payment services and global digital trade is that while technological innovation and changes in consumer preferences mean that payment services are rapidly changing, economies are at different stages in updating regulatory frameworks. Understandably, regulatory agencies that are responsible for consumer protection, financial stability, and other public interests are grappling with the legitimate challenge of updating policy frameworks to account for technological innovation and changes in consumer behaviour. For the purpose of this chapter, economies can generally be categorized into three main groups: those undertaking reforms which support the development, deployment, and use of payment services at home and across borders; those leaving legacy frameworks in place; and those undertaking reforms which may inadvertently undermine cross-border payment services and digital trade.

When economies do not update regulatory frameworks (i.e., legacy frameworks), this can potentially become a barrier to the development, deployment, and adoption of new payment services. Many modern barriers to payment services are due to institutions and regulatory frameworks which need to be updated, such as those pertaining to consumer protection, those restricting the establishment and operation of non-bank payment providers, and those which skewed playing fields towards certain participants in the payments system (WEF, 2018). For example, ensuring mobile money interoperability with the financial

system can be difficult when legacy policy frameworks discourage or complicate the use of new payment methods (WEF, 2018).

Data is already a major reason for existing bottlenecks in digital trade. As part of a Committee on Payment and Settlement Systems (CPSS) survey, respondents noted legal, regulatory, and compliance considerations as the most significant cost and challenge to their business, especially for cross-border payments. In particular, payment service providers cited anti-money laundering, know-your-customer, risk mitigation, and consumer protection requirements (BIS, 2018). Given the cost and complexity of cross-border transactions, respondents cited corresponding "de-risking" by some firms, particularly smaller firms, as they seek to reduce their exposure to certain types of customers and transactions. Furthermore, in terms of compliance costs, respondents confirmed that complying with several sets of rules and regulations as opposed to one added costs. The greatest challenge arose from conflicting jurisdiction rules and when the cooperation among authorities to resolve issues or areas of conflicting interpretation can be further improved (BIS, 2018). This highlights the more "traditional" data-related laws that payment service providers face when engaging in digital trade.

Data-related laws and regulations that support the role and flow of data

Depending on how they are implemented, regulations designed to allow government's access to payments data, especially by financial regulatory authorities, can be a significant impediment to the global provision of payment services. In particular, data localization requirements impede the free flow of data, with implications for the development of integrated, secure, and efficient payments systems worldwide, with consequences for innovation, competition, and economic growth.

At the heart of the issue is that many economies need to update domestic and trade policy tools to ensure that financial regulatory authorities have the confidence that payment firms are managing and protecting data in a responsible manner, and if needed by regulatory authorities, can provide data on request. The issue is that policymakers in many economies are focusing on the location of where payment service firms store data, rather than on the legal framework for ensuring that firms provide access to data in a timely manner (which is an example of regulatory best practice). In many cases, regulatory authorities are requiring local data storage because they believe that this is necessary to ensure government's access to the data. In the era of cloud computing, however, data can be provided with a few clicks of a mouse button.

The European Commission's (EC) efforts provide a useful example. As part of its efforts to build a digital single market, the EC is working to remove barriers to the transfer of company, tax, bookkeeping, and financial data, and asking that member states focus on mandating access[71]. For example, in 2015, Denmark changed its local data storage requirement for accounting data such that firms could store their data anywhere, as long as Danish authorities were given easy access to data on request[72]. This is where the focus should be: putting in place the legal framework to ensure firms provide data to regulatory authorities in a timely manner.

Similarly, the United States' experience with ensuring regulatory oversight of financial firms' IT systems and ability to provide data could serve as a good example for other economies dealing with concerns over access to data. The U.S. Treasury and financial regulators recently reconsidered a policy

[71] Julia Fioretti, "EU looks to remove national barriers to data flows," Reuters, September 29, 2016, http://www.reuters.com/article/us-eu-data/eu-looks-to-remove-national-barriers-to-data-flows-idUSKCN11Z19Q.

[72] "Requirements for Exemption to Store Electronic Accounting Records Abroad Will Be Abolished," Horten website, accessed November 9, 2017, http://en.horten.dk/News/2015/February/Requirement-for-exemption-to-store-electronic-accounting-records-abroad-will-be-abolished.

that would have allowed data localization for financial data, but instead enacted a policy framework that focuses on maintaining access to data. U.S. regulators' concerns were based on their experiences in the global financial crisis when they had issues getting access to data in key banks' (such as Lehman Brothers') IT systems during bankruptcy proceedings. The U.S. Federal Reserve and Federal Deposit Insurance Corporation's (FDIC) ability to use and analyze Lehman's IT systems and data was reportedly hindered as the bank's network became fragmented, overseas subsidiaries were sold off, some IT systems in overseas subsidiaries were turned off, some key IT staff departed, and restrictions on data flows were imposed due to insolvency filings in other economies—as was the case when the United Kingdom's financial regulator took over Lehman Brothers' European division[73]. This made it difficult for the regulators to access the data needed to unwind positions and ascertain what money was owed to whom[74]. However, subsequent legal reforms (e.g., the Dodd-Frank Act, enacted in 2010) have addressed these concerns by focusing on how companies disclose to regulators the way they manage their IT and data as part of regular prudential compliance activities..[75]

As it relates to trade policy, the United States-Mexico-Canada Trade Agreement's (USMCA) provisions on financial data flows and regulatory access to data show how economies can address legitimate issues raised by cross-border data flows while allowing the free flow of data as the default and predominant policy approach. In the USMCA, the opening section on the location of computing facilities for financial services (article 17.20.1) focuses on the underlying issue that financial regulators are worried about—access to data, not the location of data storage. USMCA parties agreed to recognize "that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on such access." Modern cloud computing, which allows transfers of data with the click of a button, enables firms to provide such access, while still allowing firms to move financial data freely in order to provide secure, innovative, globally deliverable services.

---

[73] Rosalind Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy: The Effect of Lehman's U.S. Broker Dealer" (Yale Program on Financial Stability Case Study 2014-3E-V1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588556; Administrative Office of the United States Courts, "Report Pursuant to Section 202(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010" (Washington, D.C., July 2011); Lemieux, "Financial Records and Their Discontents"; "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009," PricewaterhouseCoopers, accessed April 4, 2016, http://www.pwc.co.uk/en_uk/uk/assets/pdf/lbie-progress-report-140409.pdf.

[74] "Lehman Brothers International (Europe)."

[75] "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm.These "living wills" are required to provide a broad range of information relevant to resolution planning and implementation including, for example, detailed descriptions of organizational structures, credit exposures and cross-guarantees, and supporting data. The relevant section on IT and data states: "Management Information Systems; Software Licenses; Intellectual Property. Provide a detailed inventory and description of the key management information systems and applications, including systems and applications for risk management, accounting, and financial and regulatory reporting, used by the covered insured depository institution (CIDI) and its subsidiaries. Identify the legal owner or licensor of the systems identified above; describe the use and function of the system or application, and provide a listing of service level agreements and any software and systems licenses or associated intellectual property related thereto. Identify and discuss any disaster recovery or other backup plans. Identify common or shared facilities and systems, as well as personnel necessary to operate such facilities and systems. Describe the capabilities of the CIDI's processes and systems to collect, maintain, and report the information and other data underlying the resolution plan to management of the CIDI and, upon request, to the FDIC. Describe any deficiencies, gaps, or weaknesses in such capabilities and the actions the CIDI intends to take to promptly address such deficiencies, gaps, or weaknesses, and the time frame for implementing such actions."

The USMCA's central focus on ensuring access for legitimate financial oversight objectives is made clear (through partial repetition) with the subsequent balancing provision that prohibits parties from requiring financial firms to use local computing facilities as a condition of doing business "so long as the economy's financial regulatory authorities have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory." This extends to third-party suppliers of cloud storage or other related services. Each economy also agreed to provide financial firms with a reasonable opportunity to make changes to their IT systems (i.e., shifting data storage from one jurisdiction or another) if they find that they are not able to provide regulators with immediate and ongoing access to data. Such a commitment makes sense if firms realize they are not able to assure access as part of prudential reporting requirements, such as in "living wills" (where firms have to detail how they manage their IT systems and data) which systemically important financial institutions in the United States need to prepare under the Dodd-Frank Act (Cory and Atkinson, 2016). Finally, highlighting the central focus on access to data, the USMCA details that even in the final resort whereby a financial regulator requires a firm to change where it stores data, it does not necessarily mean shifting it to computing facilities in the United States (for example), just to another (third-economy) jurisdiction where regulators know they would have requisite access.

Data-related laws and regulations that limit the role of data: Restrictions as to the analysis, storage, and transfer of payment services data

A growing number of economies are using data-related restrictions as a barrier to market entry and operations for payment service providers. Local data storage, processing, and transfer/routing requirements have a significant impact on payment services firms, especially foreign ones. Barriers that make it costlier, more complex, and/or illegal for payment service firms to export and use data as part of centralized data analytics platforms limit the ability of payment services firms to use data from the broadest range of sources to provide secure, innovative, and standardized services to customers around the world. This was a major impact of laws that have been enacted or considered in several economies including a few APEC members. At the same time, one APEC economy indicated that data localization should be a legitimate policy tool given the absence of global rules on privacy. The economy further added that it is necessary to protect its citizens' privacy and data as well as promote trust in the digital economy.

As an example, one APEC economy has put in place local data storage, processing and routing restrictions for payment services data, along with other market entry restrictions that make operations difficult for international networks. About five years ago, the economy enacted a new payment systems law that requires international payment providers to transfer their processing capabilities with respect to their domestic operations to a local state-owned operator.[76] Requiring firms to use a new, state-owned process raises a number of issues including data processing and security concerns considering that the operator is relatively new and may lack the technical and institutional capabilities to securely connect to and work with payment providers. At the same time, the economy explains that this measure is a response to the fact that the neutrality of international payment providers and their ability to deliver services irrespective of international political climate are called into question.

[76] Federal Law No. 161-FZ "On the National Payment System" dated June 2011 (the NPS Law) as amended in October 2014 by the Federal Law No. 319-FZ "On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation."
https://www.dentons.com/en/insights/alerts/2017/march/2/major-russian-legislation-changes-for-2016-banking-and-finance#4

Another APEC economy is considering a law that would require payment services firms to route data through a local, state-owned, payment provider, hence forfeiting their role in delivering value-added services (ITI, 2017). Other economies also do this for certain types of transactions, such as debit card transactions. On the latter, these economies target debit transactions as this category of payment is often supported as part of broader efforts to improve the uptake of payment services.

Other examples of data-focused laws and restrictions that target payment services data include:

- The Law on Payments and Security Settlement Systems, Payment Services, and Electronic Money Institutions requires firms to maintain documents, records, data storage, and processing facilities in Turkey (Fefer et al, 2018).
- The Central Bank of Brazil proposed a cybersecurity policy that would require the local storage of financial data. The cybersecurity proposal would force firms to store their data locally (article 11). The law raises other concerns about the security of data given it required firms to indicate where the actual data centers are located (article 12:1) and that it included a requirement for cloud companies to provide the Brazilian Central Bank with physical access to the data centers (article 12:7) (Atkinson and Cory, 2017).

Some economies are indirectly creating local data processing requirements by using laws and regulations to require all transactions through a single, local "payment gateway," which is often a state-owned or connected firm. Payment gateways are essentially the stage of the e-commerce process where customers enter their personal and payment details to make a payment online (such as during the checkout process). It is equivalent to a physical point-of-sale POS terminal, where customers swipe or dip their chip-embedded card to complete a transaction. Economies are increasingly affecting this step in the processing of cross-border payments as they see it as a critical value-added step from a data analytics perspective which they want a local and/or state-owned firm to control.

Cases shared by Firm A include:

- One APEC economy is implementing a plan to develop its own local electronic payments industry by requiring that all credit and debit payment transactions be processed by a government-owned monopoly[77]. This makes the state-owned firm a direct competitor in the payments sector, while precluding foreign market access[78].
- About a year ago, another APEC economy enacted new rules that effectively prohibit foreign firms from playing a role in domestic payments, as part of its initiative to launch a domestic payment gateway[79]. The new rules require all domestic electronic (i.e., non-cash) transactions to be processed through the domestic gateway. Critical players in the payment network must be appointed or approved by the central bank, must store data locally, and must be 80 percent domestically owned. This includes the "standards institution," which is in charge of creating, developing, and managing the technical and operational specifications (including security and data protection) of the domestic gateway. It also includes the "switching" institution, which is in charge of processing domestic payment transaction data. Prior to this restriction, the economy allowed 100 percent foreign ownership. This is in addition to the Regulation on

[77] "National Payment Corporation of Vietnam," Banking Vietnam website, http://banking.org.vn/2016/national-payment-corporation-of-vietnam/.
[78] "Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses ," *The Information Technology Industry Council,* 2017, https://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf
[79] "Regulation of Bank Indonesia No. 19/8/PBI/2017 on National Payment Gateway," Bank Indonesia website, November 1, 2017, https://www.bi.go.id/en/peraturan/sistem-pembayaran/Pages/pbi_190817.aspx

Information Technology Risk Management which requires foreign banks and payments networks to locate data centers and process payments in the economy[80].

The impact on data analytics

Firm A generally described how local data storage, processing, and transfer/routing requirements undermine data analytic processes. Furthermore, Firm A outlined how restrictions on payment processes have a similar impact to data localization given that such restrictions act as a de facto market entry and data processing restriction given they prevent foreign firms from accessing and processing payments data. Local data processing or routing restrictions have a significant impact as both policies effectively prohibit foreign firms from bringing to bear a key part of their competitive offering—their globally distributed data analytics platforms. The non-exhaustive description below is indicative of the general impact on data analytics.

A major impact is that these restrictions prevent Firm A from working with global datasets and providing quicker and more effective data-driven services. For example, Firm A outlined how these restrictive policies limit its ability to use data analytics to combat credit card fraud, which is a global problem for consumers, financial institutions, and regulators. Data analytics use behavioural, temporal, and spatial techniques to assess a consumer's behaviour and whether a transaction is out of the normal or not. When a transaction is initiated, hundreds of pieces of information (for example, about the customer, merchant, place, and time, all compared against years' worth of data about prior transactions) are gathered and sent for analysis by the payment processor's predictive model to determine if it is likely a genuine or fraudulent transaction. For Firm A and other large payment providers, this process happens tens-of-thousands of times daily, which ultimately involves billions of pieces of data. These data-driven systems are powerful and fast enough to detect fraud in real time by using models based on historical data (and deep learning) to proactively identify risks. Critically, these data analytic processes improve fraud detection without increasing the number of "false positives," which not only means that firms prevent more fraud, but that they spend less time and money doing it. Similarly, big data analytics is used to detect money laundering disguised as legitimate payments. Ultimately, requiring payment service firms like Firm A to use an artificially altered database for analysis means that they may not be providing the most accurate prediction for customers as it relates to fraud and other activities.

Quantifying the impact of these policies on Firm A and similar payment firms' data analytics in terms of cost is difficult given the diffuse nature of the processes and services affected. Firm A itself struggles to put a figure on the impact or even components of it, even though it can see the myriad ways these restrictions affect its preferred operational arrangements. It is difficult for firms to identify, isolate, quantify, and aggregate the financial (in terms of specifying extra labour, investment in IT systems) and non-financial costs associated with specific data-related regulations (in terms of indirect impact on operations and the provision and development of services). However, the impact of restrictions on data analytics differs from explicit local data storage (to a degree) in that differential costs between local and preferred data storage services provide a clear marker. However, the impact of data-related restrictions on data analytics for payments firms is clearly present. Furthermore, it is comparatively easy to see (from a conceptual basis) that the impact Firm A is grappling with would represent an even larger and costlier challenge for a small or medium-sized firm that does not have the resources or technical

[80] "Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses ," *The Information Technology Industry Council*, 2017, https://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf

expertise to make the type of technical and operational changes, across multiple markets, that these restrictions entail.

The impact on digital trade

Firm A made the broader point that data-related laws discriminate against and potentially prevent market entry by foreign payment service providers as they affect the IT services used by foreign firms, but less likely to be used by local firms. Local mirroring or data storage requirements create costly and duplicative services, but requirements for local processing raise the cost and complexity to another level.

The impact can be described a sliding scale of restrictiveness and impact (from least to worst)[81]:

- Local "mirroring" requirements require foreign firms to either setup their own local data storage facilities and data processing services or pay a third-party provider for these services. In this scenario, foreign firms capture a first copy of the transaction data for local storage, before transferring it out of the economy for storage and processing in its global IT systems. Such mirroring requirements also affect data analytics processes depending on specific requirements, as they can extend to how firms are/are not able to use and update this local copy.
- Full and only local data storage requirements require foreign firms to either setup their own local data storage facility and data processing services or pay a third-party provider for these services.
- Local data processing or routing requirements (requiring firms to send transaction data to a designated firm) completely cuts off foreign firms from using data that is critical to providing modern services, such as global fraud monitoring and prevention. This can effectively be done in two key ways: when an economy designates a local firm (often state-owned) to be the only payment processor or when they require firms to route all payments through a local (often state-owned) firm. These requirements essentially act as a de facto barrier to market entry as they prevent firms from conducting core, value-added activities as part of their general service offering to customers.

Each of these categories provide an advantage for local payment service firms. As a service that relies on data and digital technologies, these requirements pose significant issues for payment service firms, especially foreign ones, which rely on the Internet to operate centralized, low-cost, and highly sophisticated IT systems. Payment providers leverage data analytics and cross-border data flows to be as cost competitive as possible and to help make transactions safer, more convenient, and overall, more valuable for the customer and the merchant, including through innovations such as contactless payments and electronic wallets.

In the scenario that an economy requires a payment services firm to only process data locally, it requires the firm to deal with the challenge (which may not be fully feasible) of seeing if it can download and replicate (to some extent) its global data analytics platforms into a local ecosystem (i.e., an IT system within an economy's borders). Such a scenario raises ongoing operational challenges as to the relationship between the local analytics platform and the global one and how to keep the former as updated (secure and effective) as possible (even though it will not benefit from the insights derived from a broader, global data set). These problems are compounded if the firm has to manage this issue across multiple economies.

These requirements tend to be discriminatory as local firms are more likely be only operating in their home economy and are therefore happy to comply with local data storage measures. Local firms are

[81] Based on information obtained during an interview with an industry expert.

also less likely to be concerned with the impact that local data storage and processing may have on business efficiency (e.g., spending more for IT services) as to their primary goal only be to capture local market share (rather than be globally competitive and innovative).

Local data storage and processing requirements act as a barrier to entry as payment service firms have to assess whether it is worthwhile for them to enter a market given the cost and complexity involved in making potentially costly and complex changes to global IT platforms and services. In some cases, a foreign payment firm may decide to enter or continue operations, but decide that data-related restrictions mean it cannot provide its full suite of services. For example, local data storage may mean that it cannot provide global fraud prevention services to a local market, as it is not able to integrate data from around the world to a local market. In other cases, a foreign technology firm may decide to not enter (or to exit, if already present) a market, as the initial and ongoing technical and operational costs simply outweigh the potential benefits. For many foreign firms, this type of regulatory assessment is becoming increasingly common, as they need to weigh up the aggregate cost and complexity that comes from making a number of iterative changes across individual economies.

The impact on local economies: cost and availability of best-in-class data services

The increased digitalization of organizations, driven by the rapid adoption of technologies such as cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well. Beyond the impact on trade, localisation requirements which affect a key data-dependent service—such as payments—will ripple throughout a local economy in several ways[82].

Given their central role in facilitating economic activity, the effects of a less-efficient, competitive, and secure payments services sector will ripple through an economy in the form of reduced firm competitiveness and economic productivity. Local data storage and processing requirements are likely to result in some foreign firms not entering a market, not offering their full suite of innovative services, or inhibiting their ability to provide their best products/services given their inability to transfer or process data on centralized IT platforms (the section below examines cases involving fraud detection and cybersecurity). Companies may also be compelled to spend more on compliance activities, such as hiring a data-protection officer, or putting in place software and systems to get individuals' or the government's approval to transfer data.

Furthermore, localization requirements for payments data further complicates a service that firms in many economies already rank as a major challenge in terms of engaging in digital trade. For example, an International Trade Center survey identified international e-payments as the largest bottleneck in the process chain for e-services exporters, as compared with other elements such as establishing an online business (ITC, 2017). Furthermore, 23 percent of 2,200 micro, small, and medium-sized enterprise respondents engaging in e-commerce in more than 100 economies identified inadequate "links between third-party e-payment service providers and local banks" as a top e-payment obstacle (ITC, 2016 and 2017). Another recent survey of merchants in 15 emerging economies in Latin America, Asia, and Africa identified e-payments as a moderate obstacle to e-commerce, and one that was more problematic for small firms (Suominen, 2017).

[82] Based on information from discussions with an industry representative.

Measures that restrict payment services data may lead to digital platforms, such as e-commerce marketplaces, not entering certain markets as it prevents them from using their preferred payment service(s) they include as part of their broad suite of services, such as advertising and logistics. It is not hard to see the potential complications that arise for digital platforms that bring buyers and sellers together across dozens of economies having to re-evaluate their local operations if they have restrictions as to if/who they can use for payments in each and every market. Depending on the platform's decision to enter or not, this would mean local firms would be potentially prevented from accessing the enormous benefits that come from using platforms to easily and cheaply access customers around the world.

These additional costs are either borne by the customer or the firm, which undermines the firm's competitiveness (especially for foreign firms which are at some disadvantage vis-a-vis domestic firms) by cutting into profit margins. It also means that the broader economy will likely suffer as the local payments sector will be less competitive (in terms of price and service offerings) if foreign firms decide not to enter, as local firms will face less pressure. The cost to firms of complying with restrictive data governance arrangements are not limited to money, but extend to broader growth and expansion, as implementing operations to comply with local data storage requirements often requires lead time of months, even years. In addition to disrupting the broad shift from paper-based payments to electronic payments in economies around the world, these policies may undermine the significant economic benefits that research shows comes from this transition in payment methods[83]. For example, McKinsey & Company has estimated that the shift from cash to digital payments could increase GDP across developing economies by 6 percent before 2025, adding $3.7 trillion and some 95 million jobs (McKinsey Global Institute, 2016).

Firm-level competitiveness is also affected as local data storage and processing requirements may prevent local firms from accessing and using best-in-class data analytic services (wherever these may be based and whatever broader platform they may be part of, such as e-commerce marketplaces). For example, it may prevent firms from using data analytics to increase customer activity, such as through targeted marketing programs, predictive modelling of consumer behaviour, and other new customer targeting techniques. For example, at its broadest level, big data analytics allow payments providers to create a more detailed, comprehensive, and single view of a customer. For example, it can help firms improve their customer segmentation, targeting, and sentiment analysis. China's Ping An established a big data analytics platform in 2013 to improve cross-selling and customer migration, with the goal of "one customer, one account, multiple services, and multiple products."[84]

As the chapter on data analytics outlines, today's economy is increasingly dependent on how firms use data, and if local firms are prevented from using the best services, this will affect their success in today's increasingly data- and artificial intelligence-based economy (New, 2018). In a similar way, local data storage and processing requirements may also undermine data-driven innovation. Organizations use data to create better insights, which, in turn, lead to innovation. Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches (Reimsbach-

[83] For a literature review of the research which shows the economic benefits of electronic payments: Wilko Bolt and Sujit Chakravorti. Digitization of Retail Payments. (Amsterdam, De Nederlandsche Bank, December, 2010), https://www.dnb.nl/binaries/Working%20paper%20270_tcm46-243674.pdf.

[84] "Seven critical changes to payments industry as FinTech matures," Payments Cards and Mobile website, January 17, 2017, https://www.paymentscardsandmobile.com/seven-critical-changes-payments-industry-fintech-matures/.

Kounatze and Van Alsenoy, 2013). By making it harder and more expensive to access and use cutting edge data-driven services, economies may prevent local firms from extracting valuable insights from their data. Furthermore, it may affect the number and cost of data analytics services available in an economy, which may lead to fewer firms using such services (as cost is a key determinant of ICT adoption and deployment), which will affect data-driven innovation across an economy. In line with this, the OECD has found that the probability of innovation increases with the intensity of ICT use (OECD, 2010).

Similarly, by inhibiting competitiveness at home, economies may inadvertently cause their firms will be less competitive and innovative than those companies that compete without protection and at scale. Economies of scale for payment services, like many parts of the digital economy, are critical, as payment systems require considerable up-front investments in processing infrastructures, highly secure telecommunication facilities and data storage, and apply complex operational standards and protocols. As a consequence, it is critical for firms to achieve a large volume of payment transactions in order to reduce per unit costs (Bolt and Chakravorti, 2010). The Global Payments Innovation Jury Report of 2017 (a survey of 70 industry executives from around the world) shows how this is already a major issue in that it cites the inability to scale as the biggest reason payments start-ups fail (26 percent of respondents), followed by regulation (in third place with 15 percent). For policymakers who want to support local payment providers, it is critical they implement a policy environment that makes their firms competitive at home while also facilitating economies of scale by ensuring they are able to enter into and compete in foreign markets. Local firms in economies enacting local data storage and processing requirements will inevitably face the same disadvantages as foreign firms do in their local market if local data storage and processing rules for payments data become the norm around the world.

Ultimately, local data storage and processing requirements will likely lead to less efficient and less competitive local and regional payment markets. And this hurts all firms in an economy, because it raises their costs and/or forces them to use inferior services. In other words, when policymakers enact data localization laws to support one sector of their economy, they inadvertently end up affecting the other sectors of their economy. This issue is compounded by the fact that there are no significant regional initiatives to coordinate approaches to e-payments regulations (Cullen International, 2016). For example, in Latin America, e-payment solutions tend to be highly localized due to cross-border regulatory friction that in turn affects cross-border e-commerce. Likewise in South East Asia, cross-border bank payments among Association of Southeast Asian Nations (ASEAN) member economies remain complex due to reasons such as currency conversion costs, volatile exchange rates, significant variations in Internet speeds, and the absence of basic payments infrastructure systems in some economies and the lack of a common messaging standard[85].

The impact on local economies: detracting from foreign investment

In today's interconnected global economy, firms which have data at the center of their business model will take into account local data governance requirements as part of their regulatory due-diligence when considering global investment decisions. Local data storage or processing requirements signal to high-tech firms (whether in the payments sector or elsewhere) that an economy may not be truly committed

[85] HSBC. Payments in ASEAN post AEC. Available at: https://www. hsbc.com.my/1/PA_ES_Content_Mgmt/content/website/commercial/ cash_management/PDF_141107/5-Payments-in-ASEAN-post-AEC. pdf.

to supporting globally competitive and innovative data-driven firms[86]. Firms are less likely to commit the capital to invest in local research and development centers, global data processing centers, and other data-related facilities if they perceive that policymakers are likely to restrict the movement of data. Econometric modelling on the impact of data localization provides an indicative estimate as to the reduced level of investment that results from an economy that takes a restrictive approach to data flows. A study of potential data localization measures in several economies shows that the effects on GDP, investments, and welfare from data-related regulations are too considerable to be ignored in policy design (Bauer et al, 2014). If policymakers want to tap into foreign investment, technology, and know-how, they need to account for how their regulatory framework manages data-related issues, as these firms have the ability to setup operations in a broad range of economies to service foreign markets.

The impact on local economies: increased security risks

Economies requiring local data storage or processing affect the ability of payment service firms (and other tech firms) to use best-in-class technology and methods to protect and secure data and their IT systems[87].

Local data storage requirements means that all transaction data may only be stored in a single data center or only distributed over a small number of data centers. By requiring firms to use only local data services, economies enacting data localization may prevent firms from using best-in-class cybersecurity measures. This is a major potential issue, as cyber threats and fraud are on the rise with increased adoption of mobile payments and wearable devices leading to a loss of consumer trust as well as financial losses. Payment firms have to continuously invest in advanced authentication and enabling technologies (such as biometrics, secured element and tokenization, geo-location based authentication, and cryptographic keys) to stay ahead of hackers and cybercriminals (Capgemini, 2017). Local data storage and processing requirements may prevent firms from using modern techniques for storing data, such as "sharding," which involves breaking up data and storing it in multiple locations, or constantly moving it between different data centers in different economies.

Also, requiring firms to store data locally creates physical risks (and substantial costs) as firms may have to setup multiple data centers as part of a largely self-contained IT ecosystem within an economy in order to provide backup, redundancy capabilities to ensure data remains secure in the event of a natural disaster, power outage, or other such emergency which could take a data center offline.

Local data storage and processing requirements also prevent payment service firms from providing the best-possible fraud detection services to clients, as they are not able to feed local data into global systems that constantly monitor for fraudulent transactions, which are not limited by borders. It is now common for leading payment service accounts to have fraud management tools which score transactions based on insights from millions and billions of worldwide transactions. For example, if an odd transaction in New Delhi, India is found to be fraud, the global platform would learn from this. A similar transaction in Santiago, Chile the next day would be blocked (based on an assessment of a client's transaction history, it would lead to a higher fraud score that will cause the transaction to be declined). Firms use artificial intelligence to constantly assess transactions in real-time (Chakravorti et al, 2017). Firms are investing a growing amount of funds into developing machine learning solutions for fraud detection. Indicative of this, 68 percent of North American financial institutions (surveyed in a 2017

[86] Based on information from discussions with an industry representative.
[87] Based on information from discussions with an industry representative.

study) cite machine learning analytics as a high priority investment to help fight fraud. However, for firms to build fraud models and gain insights for fraud prevention, payment service firms need unimpeded access to their global platform and data sets from around the world. In a similar way, local data storage laws may prevent firms from being best prepared to defend against the full spectrum of cybersecurity attacks (in terms of being able to use data from global operations so that all systems reflect global best practices)[88].

4.5. Conclusion

Some data-related laws and regulations may add cost and complexity for payment services, which is a sector that already faces a significant compliance challenge from being subject to significant legal and regulatory requirements for financial services in multiple jurisdictions. This is why cross-border payments are generally more complicated and expensive than domestic payments. Adding data-specific issues adds a further distinction between domestic and foreign providers given that the latter tend to rely on centralized IT systems and data transfers to operate across multiple markets. By enacting policies which target cross-border providers as well as processing of payment data (including firms which are allowed to do so), these economies are affecting a key facilitator of digital and traditional trade.

[88] Based on information from discussions with an industry representative.