# Cyber Security and Cloud Outsourcing of Payments

Ciet Noé, Verdier Marianne

*First version: December 2022*

**Abstract**

We study the incentives of competing banks to outsource their payment services to a cloud-based common infrastructure, managed by a private third-party provider (TPP). The TPP provider stores depositors' information in the cloud and offers compatibility services, but is exposed to cyber risk. If the market is unregulated, without cyber risk, banks outsource excessively to the TPP compared to the first-best because network effects soften competition for deposits. However, we show that cyber risk and the costs of security may reduce banks' incentives to join the third-party infrastructure, which may result in an inefficiently low level of interoperability of their payment systems. We examine how the liability regime for cyber incidents may improve the players' investment in security. We show that increasing the TPP's liability towards depositors has a higher impact on payment system security than increasing its liability towards banks. We discuss how several regulatory options impact the security and compatibility of banks' payment systems: the supervision of outsourcing agreements, a shared responsibility model, the public provision of payment services.

**Keywords: payment systems, banks, cyber risk, cloud outsourcing, financial stability, compatibility, critical infrastructure.**

**JEL classifications: E42, E58, G21, L51, O31.**

## 1 Introduction

For decades, banks have outsourced the management of payment services to third-party providers. With the recent development of digital innovations in payments, the importance of cloud-based third-party providers in the banking sector has been growing rapidly.[1] According to the Financial Stability Board (2019), cloud computing is defined as an innovation that allows for the use of an online network of hosting processors, so as to increase the scale and flexibility of computing capacity.[2] Regulators are concerned that the outsourcing of payment systems to third-party providers could pose new risks for the security of retail banking activities and financial stability. For example, in 2022, the European Commission has reached a provisional agreement on a Digital Operational Resilience Act for financial services (DORA), which designs a regulation of Critical Third-Party Providers, including cloud service providers.[3]

In this paper, we study the optimal architecture of a retail payment system in the presence of cyber risk. We analyze banks' incentives to outsource their payment services to a cloud-based third-party provider (TPP), and the level of security of their payment systems. We obtain the following results. Without cyber risk, banks tend to outsource excessively their payment systems compared to the first-best because of network effects. However, the presence of cyber risk implies that banks may sometimes choose not to outsource enough their payment services when depositors benefit from interoperability. We compare various regulatory options in terms of cyber security and efficiency: a liability regime for cyber incidents, the supervision of cloud outsourcing agreements, the shared responsibility model, the building of a public infrastructure.

Banks' partnerships with cloud service providers for payments may entail several benefits that can be ultimately passed on the depositors, such as the ability to deliver up-to-date services without supporting important innovation and storage costs.[4] In addition, the technical solutions offered by cloud service providers are often standardized and may scale-up rapidly. This implies that competing banks may easily rely on compatible solutions. In payments, banks often rely on a third-party cloud-based infrastructure (either privately or publicly managed) to develop interoperable payment solutions. For example, in the United-States, the private service provider Modo offers a platform that enables bank to achieve technical interoperability.[5]

Yet, the use of third-party service providers in banking generates new con-

[1] A study by the International Data Corporation (2018) shows that banks' spending on public cloud services has been growing at a rate of 23 percent per year over the last five years. In 2020 only, major partnerships of banks with cloud companies include Deutsche Bank with Google Cloud, Standard Chartered with Microsoft, and Bank of America with IBM.

[2] Cloud services model can be deployed either through a public cloud on the Internet, or by a private cloud that is only accessible by a single organization, or by a combination of the two.

[3] The latter would be supervised by one of the European Supervisory Authorities, who would have the power to request information, conduct inspections, issue recommendations, and impose fines in certain circumstances.

[4] Banks are able to deliver better mobile banking experiences or to use AI to make personalized recommendations of services to their clients, (see Lam and Seifert, 2021).

[5] https://modopayments.com/wp-content/docs/Modo-Overview-eBook.pdf

cerns for regulators.[6] For example, in December 2021, a five-hour outage of Amazon Web Service (AWS) impacted the access of consumers to many services, including banks' call centers and websites. In addition, banks migrate sensitive data outside their IT systems when they join the cloud, which increases the risks of data breaches. In 2019, 106 million credit card applications of Capital One Financial have been stolen from the AWS. Ongoing civil lawsuit against both AWS and Capital One suggest Capital One failed to implement security procedures available on its cloud platform (Covert, 2021).[7] Supervisors insist that banks are responsible for monitoring their service providers, while third-party companies have started to face transparency requirements towards their clients.[8] Several Central Banks have expressed the concern that the outsourcing of banking services to common third-party providers could increase the cyber risks in the financial sector (e.g., the Financial System Review of the Central Bank of Canada, 2019, the Reserve Bank of New Zealand, 2020, in a consultation paper).[9] On the other hand, cloud service providers contend that their services improve the security and the reliance of their payment systems.[10]

The presence of cloud service providers in the banking industry is related to the broader debate on public intervention in payment systems. The main research question is whether the government should build a common infrastructure to maximize the benefits of inter-operability and payment system security (as is the case in Brazil with Pix or in India with UPI).[11] In our paper, we aim at understanding whether there is an excessive (or under) provision of third-party services when outsourcing to a cloud-based infrastructure implies different costs and benefits of managing cyber risk.

We build a model to analyze banks' incentives to join a common payment infrastructure managed by a private operator (the cloud service provider) in the presence of cyber risk. The cloud service provider offers to banks two different services: storage capacity and a payment app. There is a fee for each service. Banks compete in the downstream market of deposits on the Hotelling line and offer payment services to their consumers, which quality depends on the security of their payment systems. If the banks' depositors are equipped with the same payment app, they are able to send payments to one another. Some depositors are naive, while other are sophisticated and choose their banks according to the

[6] In 2021, the Federal Reserve, the FDIC and the OCC launched a first interagency guidance to financial institutions related to their third-party relationships (see Federal Reserve System, 2021)

[7] The bank supervisor (the Office of the Comptroller of the Currency) found the bank liable of poor risk assessment when considering its cloud migration, as well as insufficient safeguards practices afterwards.

[8] US banking agencies introduced in 2022 customer notification requirements for a broad scope of third party service providers to banks. The equivalent measure in Europe is the DORA regulation.

[9] See the financial system review of the Bank of Canada (2019), the consultation paper of the Reserve Bank of New Zealand (2020) on cyber resilience.

[10] See the response of AWS to the consultation Reserve Bank of New Zealand.

[11] See D'Sliva et al., 2019.

level of risk of its payment system. Since banks are unable to price discriminate between consumers, the price of deposits reflects banks' horizontal differentiation on the Hotelling line and banks' vertical differentiation in terms of payment system security.

Banks decide whether or not to join the cloud by comparing their benefits and costs of outsourcing their payment services. On the one hand, if both banks join the cloud and become interoperable, their depositors may enjoy the benefits of network effects. On the other hand, the security of their payment system changes and depends on the cloud service provider's investment. Banks also lose the benefits of security differentiation, which they obtain if they compete with independent payment solutions. Two other inefficiencies may arise when banks join the cloud: additional damage and moral hazard. Indeed, the cloud service provider may under-report cyber incidents, which reduces the banks' and the depositors' ability to claim compensation.

We start by analyzing the social optimum. The outsourcing decision benefits the society if and only if the marginal social benefits of interoperability are sufficiently high with respect to the potential marginal social costs in terms of risk. In the first-best allocation, there is no moral hazard, which implies that the cloud service provider does not hide any information when a cyber incident occurs. We show that the welfare-maximizing level of security of the payment system is higher if both banks join the cloud (than if they remain independent) if and only if the marginal benefit of delegating the investments in security to a third-party provider exceeds the marginal costs. This happens if the cloud service provider incurs a sufficiently low cost of investing in cyber security, compared to the banks. For example, if there are no additional losses with cloud outsourcing, and if banks do not contribute to payment system security, cloud outsourcing increases the level of security of the payment system if the investment cost of the cloud service provider is lower than the sum of the banks' investment costs. This result is caused by the efficiency gains that arise if there is no duplication of investment costs.

Then, we analyze the game in which banks decide whether or not to join the cloud after investing in payment system security. The cloud service provider commits to offer a given level of investment in payment system security and chooses the access and compatibility fees that banks need to pay when they outsource their payment systems. When there is a cyber incident, the liability regime allocates the total loss between the cloud service provider, the banks and the depositors. At the last stage of the game, if a cyber incident occurs, the cloud service provider does not disclose it perfectly to the banks, to avoid becoming liable. Moral hazard generates some benefits and some costs for banks. On the one hand, if a cyber incident is not discovered by anyone, banks avoid compensating their depositors, which reduces their respective marginal cost. On the other hand, the cloud service provider's under-provision of information increases the amount of the losses when a cyber incident occurs. This implies that banks expect to incur higher losses when they decide to join the cloud. Banks trade off between relying on the cloud's infrastructure to increase the compatibility of their payment systems and remaining independent to enjoy the benefits of security differentiation. We show that at a symmetric equilibrium, both banks outsource their payment services if the cloud service provider earns a positive profit, and they both remain independent otherwise. Even if an asymmetric equilibrium does not exist in our setting, the possibility that a bank may deviate from the situation in which both banks join the cloud to enjoy the benefits of a higher security differentiation constrains the cloud service provider's pricing strategy.

Unlike the conventional wisdom, which often assumes that banks tend to outsource excessively their payment services to the cloud, we show that banks may sometimes choose not to outsource enough to the cloud service provider, with respect to the welfare-maximizing situation. We identify the market conditions such that banks under-outsource their payment services (resp., over-outsource). Banks tend to choose excessive levels of interoperability to soften competition for deposits. This result is standard in the literature on compatibility in networks (see Foros and Hansen, 2001). However, we show that cyber risk reduces banks' incentives to outsource excessively and may even imply that banks sometimes do not outsource enough their payment systems with respect to the social optimum. This result is caused by several distortions with respect to the first-best. The vertical structure of the market adds several layers of inefficiencies caused by the timing of the investment and pricing decisions and the presence of moral hazard. Some effects reinforce the bias towards excessive outsourcing caused by network externalities, while other may compensate for it, and even reverse it, such that banks may sometimes under-outsource their payment services.

The vertical market structure implies the following distortions. First, the cloud service provider chooses its prices after banks choose their investments in security. This implies that it does not internalize the impact of its pricing strategy on banks' investment incentives. Therefore, it may under-estimate banks' rents of outsourcing, and offer its services too rarely compared to the first-best. This effect weakens the bias towards excessive outsourcing. Second, banks' investment incentives are distorted by the presence of moral hazard. However, in our paper, the effect of moral hazard on banks' investment in cyber security is ambiguous. On the one hand, banks have incentives to over-invest to protect themselves from the additional damage caused by under-reporting of cyber incidents. On the other hand, banks also benefit from the under-reporting of cyber incidents, as this enables them to avoid becoming liable towards their depositors. Thus, the moral hazard effect may either reinforce or weaken the bias towards excessive outsourcing caused by network externalities. Third, the cloud service provider does not internalize the impact of banks' expected damage on competition for depositors. In addition, neither the banks nor the cloud service provider internalize the expected losses incurred by the naive depositors. We conclude the paper by analyzing how the liability regime for cyber incidents impacts payment system security and banks' outsourcing decisions.

The rest of the paper is organized as follows. In Section 2, we survey the literature that is related to our work. In Section 3, we present the model and the assumptions. In Section 4, we present the first-best benchmark, in which the social planner chooses how much to invest in cyber security, and decides whether or not it is socially optimal that banks share a common payment system. In Section 5, we solve for the game in which firms decide how much to invest in cyber security, and banks decide whether or not to join the third-party provider. We identify the distortions that arise with respect to the first-best. In section 6, we apply our model to compare various remedies to the distortions that occur when banks make their outsourcing decisions. We discuss how moral hazard impacts investments in security and outsourcing decisions. Finally, we conclude.

## 2 Related Literature

Our paper is connected to five strands of the literature: the research on investment in cyber security, the role of cyber security in payments, the literature studying product liability and product compatibility, respectively, and the literature on the optimal market structure in network industries.

We contribute to the emerging economic literature on investment in cyber security (see Anderson et al., 2009 for a survey). Our work is closely related to the research question of De Corniere and Taylor (2021), who study how both the liability regime for cyber incidents and firms' business model impact investments in cyber security. They compare firms' investment in security with price competition and with advertising-funded business models. As in their paper, we assume that a proportion of consumers is naive and study the optimal liability regime. In contrast to their work, we compare a business model with outsourcing to a cloud service provider to independent security provision. Therefore, we are interested in analyzing in a vertical relationship model the optimal liability regime with and without outsourcing to a third-party. In the context of software provision, Lam (2016) shows that a regime with full liability is inefficient because it implies overinvestment in attack prevention and damage control. Our paper differs from this work, as we model competition between firms and the role of a third-party provider.

Our paper also complements the literature on cyber security in payments. Several research papers analyze the optimal design of payment solutions when financial intermediaries trade off between security and convenience (see Kahn and Roberds, 2008, Kahn, Rivadeneyra and Wong, 2020, and Chiu and Wong, 2022) or security and the intensity of data usage (Garratt and Schilling, 2022). In our paper, the convenience benefit for consumers depends on banks' decision to outsource their services to a third-party, because outsourcing increases compatibility. In Kahn, Rivadeneyra and Wong (2020), the banks' choice of a technology impacts the consumers' incentives to protect their password and split their funds between several accounts. In Chiu and Wong (2022), cyber security impacts a platform's choice between issuing cash and accepting tokens. Several papers analyze how the liability regime affects the investment incentives of intermediaries (Kahn, Rivadeneyra and Wong, 2020, Creti and Verdier, 2014). We study shared responsibility between the cloud service provider, the banks and the consumers. By comparison, Kahn, Rivadeneyra and Wong (2020) consider the shared responsibility between the custodian of the funds and the consumers. Creti and Verdier (2014) analyze how the liability regime of a two-sided monopolistic payment platform impacts payment instrument pricing and consumer surplus. Garratt and Schilling (2022) study how the network pattern of data flows across firms affects the resiliency to various cyber risks (DDOS, leakage, corruption) and the incentives of firms to collect data. Unlike Garratt and Schilling (2022), we do not study banks' incentives to collect data and focus on the effect of cyber risk on security investments in a cloud-based business model.

Our work is also connected to the law and economics literature on product liability (see Daughety and Reinganum, 2013, for a survey). The novelty of our model consists in analyzing the optimal liability regime in a vertical relationship model with network effects. In a vertical relationship setting, Jacob and Lovat (2016) focus on the effect of the liability sharing rule on the ability of firms to pay for damages. In contrast to their paper, we study the consequences of the liability regime on downstream competition, as well as the effect of asymmetric information between firms on cyber security. The use of the upstream infrastructure offered by the cloud-service provider enables downstream firms to enjoy the benefits of compatibility, because end-users benefit from making transactions with a larger consumer base. To our knowledge, no theoretical paper has studied this specific issue.

Our work also contributes to the long-standing literature on product compatibility and interoperability of payment systems, surveyed by Bianci et al. (2022). We consider interoperability at the platform level, which refers to the extent to which the users of one payment system can make transactions with the users of another service provider. We analyze whether banks have incentives to buy services from a third-party if they enjoy higher benefits of compatibility when they outsource their payment services. Matutes and Padilla (1994) derive the conditions under which banks share their ATMs and find that sometimes total incompatibility may prevail. Unlike in Malueg and Schwartz (2006) who consider quantity competition and asymmetric firms, we consider symmetric banks with Hotelling competition as Doganoglu and Wright (2006). As in their papers, banks' incentives to make their services compatible depend on the degree of network effects. Doganoglu and Wright (2006) study how multi-homing affect private and social incentives for compatibility, whereas we consider only single-homing consumers. As in Malueg and Schwartz (2006), we find that banks prefer to outsource when the degree of network effects is sufficiently high.

Massoud and Bernhardt (2002) develop a model to study why banks may use inefficient pricing schemes in compatible ATM networks. Unlike in their work, we are interested in the inefficiencies caused by the liability for cyber incidents.

We also contribute to a literature studying the optimal market structure and firms' investment incentives, when upstream providers of a network infrastructure offer their services to downstream competitors (see Dogan, 2009). The upstream provider(s) may decide to invest in the quality of the interconnection offered to downstream firms. In our paper, the upstream firm is the cloud service provider, and the downstream firms are the banks, which compete for depositors. However, because we design a model that applies specifically to the banking industry, we depart from this literature in three directions. First, we do not analyze the optimal quality of the interconnection service, which is exogenous in our model. We consider instead that firms' investment in cyber security is endogenous. In addition, all firms (upstream and downstream) contribute to the security of the payment system. Therefore, the downstream firms (i.e., the banks) also exert an externality on the upstream firm (i.e., the cloud service provider) when they choose how much to invest in payment system security. Second, the cloud service provider's input is not essential to offer payment services to depositors. This explains our choice to leave aside the issue of a possible vertical integration between banks and the cloud service provider. We only compare two market structures, with and without the upstream provider. Third, we have chosen to simplify the analysis of the compatibility decision, by assuming that banks become either fully compatible or remain incompatible. Firms' decisions to be compatible have been studied extensively in the literature on networks, with the different assumption that firms may become partially compatible (e.g., in Foros and Hansen, 2001 or in Stadler, Trexler and Unsorg, 2022). Our assumption of full compatibility is in line with our understanding of competition in the payments industry: depositors are either equipped with the same payment app or cannot send payments to each other. Our results would remain valid with a sufficiently high degree of interoperability offered by the third-party provider.

Our work is also indirectly related to the literature analyzing co-investment and infrastructure sharing in network industries, in the presence of demand uncertainty (see Inderst and Peitz, 2012, Bourreau et al., 2018). However, this literature studies whether co-investment improves social welfare when an entrant competes with an incumbent, which invests in an upstream infrastructure. Unlike this strand of the literature, we assume that the banks and the cloud service provider incur different costs of security and do not compete for depositors. In addition, we assume that joining a common third-party provider enables the banks to improve the interoperability of their payment systems.

So far, we have assumed that banks cannot become compatible without joining the cloud, which is an assumption that we would like to discuss further in the future of our work, by studying the case in which banks jointly manage the upstream infrastructure.[12] A strand of the literature analyzes how banks jointly manage payment systems by determining the interchange fee, which is paid by the merchant's bank to the consumer's bank each time a consumer pays by card (see Verdier, 2011 and Rochet, 2003 for surveys). However, this literature assumes that payment systems are already interoperable and does not analyze banks' incentives to rely on a common payment infrastructure when outsourcing payment services may generate both benefits and costs.

# 3 Model

We build a model to study banks' incentives to outsource their payment services to a third-party provider when there is cyber risk. There are two banks in our model and a monopolistic third-party provider of a cloud-based infrastructure. When banks rely on cloud services, they may enjoy the benefits of a higher compatibility of their payment solutions. However, the security of their payment system also depends on the cloud service provider's investment. If a cyber incident occurs, depositors, banks and the third-party provider may incur losses.

**Cloud outsourcing:** Two banks $A$ and $B$ are located at the two extremes of a Hotelling line, and compete in prices and security to serve a mass 1 of consumers who open a bank account to make payments. Bank $A$ is located at point 0 and bank $B$ at point 1. The price of an account in bank $i \in \{A, B\}$ is $p_i$ and the level of security of payment transactions in bank $i$ is $s_i$.

In the market, there is a third-party provider of payment services that we call the cloud service provider $C$. The third-party provider does not compete with banks for deposits.[13] Banks may buy two different services from $C$, which invests an amount $s_c \geq 0$ in the security of its infrastructure. First, they may use its cloud-based infrastructure to store information on payment transactions by paying a per-depositor access fee $f^a$ to $C$. Second, if both banks store their payment information in the cloud, they may use additional services offered by the cloud to reach compatibility. If both banks decide to be compatible, we assume that each bank pays to the cloud service provider a fixed compatibility fee $f^c$.[14] The compatibility fee can be interpreted as the price of a payment app that the cloud service provider sells to both banks to help them reach compatibility.[15] The value of a payment app for a given bank increases with

[12] This case differs from the vertical integration hypothesis, because banks compete in the downstream market of deposits. So far, we have not discussed this option, to highlight the fact that the cloud service provider has access to a different technology that reduces the cost of investments in cyber security.

[13] In our setting, the cloud service provider is a firm that has access to a different technology for the management of cyber risk, while being able to offer services that reduce the cost of building interoperable payment solutions.

[14] In the literature on interchange fees, the merchant's bank pays the consumer's bank an interchange each time a merchant pays by card. Our model departs from this literature, because we consider that the payment system is not jointly owned by banks.

[15] In practice, there are different business models of payment system outsourcing (Grabowski, 2021). The cloud service provider may be a Banking-As-a-Service platform,

the number of compatible depositors from the other bank.[16]

With this vertical market structure, the cloud service provider is therefore an upstream provider of payment services, which quality depends on the infrastructure security, whereas banks compete in the downstream market of deposits.[17]

We will refer respectively to the index $n$ for the subgame in which there is no cloud outsourcing, $c$ for the subgame with cloud outsourcing for both banks, and $o$ for the subgame with cloud outsourcing only by bank $i \in \{A, B\}$.

**Security investments and prevention of cyber incidents:** The probability $h_i$ that a cyber incident occurs in the payment system of bank $i$ depends on its investments $s_i \in (0,1)$ in cyber security and the investments $s_c \in (0,1)$ of the cloud service provider, respectively. We assume that that the total level of security of the payment system is a weighted average of the bank's investments and the cloud service provider's investment, in shares $\theta$ and $1-\theta$, respectively. Without cloud outsourcing, the cloud service provider's investments have no impact on the security of the bank's payment system, such that we have $\theta = 1$. With cloud outsourcing, we have $0 \leq \theta < 1$.

The probability $h_i$ is a linear function of security investments, such that $h_i(s_i, s_c, \theta) = h - \sigma(\theta s_i + (1-\theta)s_c)$, where $h \in (0,1)$ represents the (exogenous) vulnerability of the payment system to a cyber incident, and $\sigma > 0$ models the sensitivity of $h_i$ to the security investments.[18] We assume that $s_i$ and $s_c$ belong to $(0, h/\sigma)$. In the rest of the analysis, we will denote by $h_i^n(s_i) \equiv h_i(s_i, s_c, 1)$ the probability that a cyber incident occurs without cloud outsourcing, and by $h_i^c(s_i, s_c) \equiv h_i(s_i, s_c, \theta)$ the probability that a cyber incident occurs if bank $i$ relies on the cloud for its payment system.[19]

We assume that the banks and the cloud service provider incur quadratic costs functions for cyber security investments. Each bank $i = A, B$ incurs a cost $C_b(s_i) = k_b s_i^2/2$ of investing $s_i$ in cyber security, and the cloud service provider incurs a cost $C_c(s_c) = k_c s_c^2/2$, where $k_b > 0$ and $k_c > 0$. Our modeling of a quadratic cost function for security investments implies that each bank's total marginal cost is linear in the level of risk $h_i$ as in Daughety and Reinganum (1995). Without cloud outsourcing, each bank's marginal cost depends only

which does not sell services directly to the consumers. It may sell a payments App directly to banks or connect banks and app providers (see for instance the website of Amazon Web Services for examples of the various add-on services offered by a cloud service providers). Alternatively, the cloud service provider may sell services directly to the depositors.

[16] The storage and the compatibility services are one-way complements because the compatibility service is only available if banks decided to use the storage service.

[17] The cloud service provider cannot price discriminate between banks.

[18] The probability $h$ may depend of macroeconomics factors, ranging from the geopolitical context to the intensity of sector rivalries, as well as the state of the technology regarding the identification of software flaws. The efficiency of cyber protection depends crucially on the proportion of proprietary software, the level of caution of end-users and employees, as well as the identification of known threats by white hats, software firms or local governments.

[19] Typically, the cloud service provider is responsible for the security of the cloud (hardware, software), while banks are responsible for data usage (encryption, resource allocation, outside software), patching, and access to data. The allocation of security resources is negotiated by the bank and the cloud service provider.

on its investments in cyber security.[20] With cloud outsourcing, each bank's marginal cost becomes also dependent on the cloud service provider's investment in security, because $h_i$ is a decreasing function of $s_c$. The higher the security of payment services in the cloud, the lower the bank's marginal cost. Therefore, the cloud exerts a positive externality on the banks when it decides to increase its security investments. This type of externality is common in the literature on vertical relationships (Segal, 1999). In addition the access fee and the compatibility fee impact the cloud service provider's investment incentives, as in the literature on access charges in networks (e.g., Valetti and Cambini, 2004).

**The losses caused by cyber incidents:** When there is a cyber incident, each depositor incurs a loss $l_d > 0$, which corresponds either to a loss of funds or the monetary cost of a leakage of his personal data. Using data on cyber incidents in Canada, Chande and Yanchus (2019) show that the losses incurred by the depositors vary according to the type of the cyber incident.[21] A bank incurs a loss per depositor $l_b > 0$, corresponding to the costs of fixing its security system, its reputation costs, or even higher funding costs. If the bank outsources its payment service to the cloud service provider ($z = 1$), the latter may incur a loss $l_c \geq 0$. Otherwise, without outsourcing ($z = 0$), the cloud service provider does not incur any loss. We assume that cloud outsourcing multiplies the amount of the losses of the bank and the depositors by an amount $\alpha \in (\underline{\alpha}, \overline{\alpha})$, with $\underline{\alpha} \geq 1$.

We normalize $l_c$ to $l_c \equiv 0$ without loss of generality and denote the minimum total loss of the bank and the depositors by $l = l_b + l_d$. The total loss per depositor is $(1 - z + z\alpha)l$. The liability system allocates the total loss per depositor between banks, the cloud service provider and the depositors. We denote by $L_b$, $L_c$, and $L_d$ the net losses incurred by the bank, the cloud service provider and the depositors, including the potential transfers between the players.

**Depositors:** Each depositor located on the Hotelling line derives a utility $u_0 > 0$ for the use of a bank account, expects to obtain an additional utility $\beta > 0$ per payment transaction, and incurs the transportation cost $t > 0$ when he travels to open an account either in bank A or B.

A proportion $\mu \in (0, 1)$ of depositors take into account the level of security of the payment systems when they decide in which bank to open an account, the rest of depositors, in proportion $1 - \mu$, are naive or do not care about secu-

[20] We assume that the security investments of banks generate no spillovers on the overall level of protection of their rivals. Alternatively, if each banks' investment exerts linear spillovers on the overall level of protection of its rival equals $s_i + \sigma s_{-i}$, with spillovers $\sigma \in (0, 1)$ from the security investments of the other bank $-i$, each bank invests only a proportion $1 - \sigma$ of their investments absent spillovers, without altering our results.

[21] However, estimating the losses caused by cyber incidents remains a difficult task. In Canada, of finance and insurance businesses suffering a cyber incident, only 29 per cent reported it to police, 21 per cent reported it to the Canadian Cyber Incident Response Centre, 17 per cent reported the incident to their regulator.

rity.[22] Banks do not observe the depositors' types. We motivate the existence of sophisticated depositors by the empirical evidence offered by Gogolin et al. (2021), who show that successful cyber attacks may decrease deposit growth rates at small banks. In addition, firms are now able to buy cyber ratings from rating agencies.

A depositor makes a payment transaction with all the depositors who can be reached with the payment solution delivered by his bank (i.e., the compatible depositors). The number of depositors who open an account in bank $i = A, B$ is $N_i$ and the expected number of depositors is $N_i^e$.

The number of compatible depositors depends on the bank's decision to outsource its payment services to the third-party provider. In practice, when banks share an infrastructure managed by the same third-party provider, this increases the degree of interoperability of their payment services, compared to the situation without outsourcing. We capture this feature in our model by making the extreme assumption that banks' payment systems are technically perfectly interoperable if banks outsource to the same third-party provider, whereas they remain fragmented otherwise. Formally, we would obtain equivalent results with an additional parameter representing the degree of interoperability of payment solutions, as long as the degree of interoperability is higher with outsourcing. Therefore, if both banks decide to use the compatibility service, each depositor is able to make a transaction with all depositors (the total mass 1 of depositors), whereas, if both banks are not compatible, their depositors expect to make transactions only with the depositors who have an account in the same bank (in share $N_i^e$ for the depositors of bank $i$).

A naive depositor located at point $x$ on the Hotelling line who opens an account in bank $i$ and expects to make transactions with $N_i^e$ depositors obtains the utility

$$u_i(x) = u_0 + \beta(z + (1-z)N_i^e) - tx_i - p_i, \tag{1}$$

where $x_i = x$ if $i = A$, and $x_i = 1 - x$ if $i = B$, $z = 1$ if banks' payment systems are compatible, and $z = 0$ if banks' payment systems are incompatible. A sophisticated depositor located at point $x$ also takes into account the expected losses caused by cyber incidents $L_d(v)$ which occur with probability $h_i(s_i, s_c, \theta)$. Therefore, he obtains a utility

$$u_i(x) - h_i(s_i, s_c, \theta)L_d \tag{2}$$

of opening an account in bank $i$.

**Bank profits:** Bank $i$'s profit is the sum of the profits from deposits, less the costs of security investments and security incidents, and the potential fees paid to the cloud, if any. It is therefore given by

$$\pi_i = (p_i - h_i(s_i, s_c, \theta)L_b - z_i f^a)N_i - z_i z_{-i} f^c - C_b(s_i), \tag{3}$$

[22] We assume that security investments and depositor sophistication are non-verifiable, such that it is not possible to write contingent contracts contingent that depend on these variables.

where $\theta = 1$, $z_i = 0$ if bank $i$ does not outsource its payment services, and $z_i = 1$ otherwise. If both banks' payment services are compatible ($z_i = z_{-i} = 1$), each bank pays the fixed compatibility fee $f^c$.

**Cloud service provider profit:** The cloud service provider's profit is the sum of the revenues from the access fee $f^a$, the compatibility fee $f^c$, if any, less the costs of security investments and security incidents. If the market is covered and banks' payment services are compatible, the cloud service provider makes a profit

$$\pi_C^c = 2f^c + (f^a - h_i^c L_c)N_i + (f^a - h_{-i}^c L_c)N_{-i} - C_c(s_c). \tag{4}$$

If only bank $i$ joins the cloud, the cloud service provider makes a profit

$$\pi_C^o = (f^a - h_i(s_i, s_c, \theta)L_c)N_i - C_c(s_c). \tag{5}$$

Finally, if no bank joins the cloud, the cloud service provider does not make any profit.

**Assumptions** Finally, we formalize four additional assumptions:

- (A1): We have $t - \beta > k_b > 2h(L_d + L_b)/3$. Assumption (A1) implies that banks' profits are concave in security investments and prices and that both banks make positive profits in equilibrium.
- (A2) $h \geq \sigma$. Assumption (A2) implies that if firms invest their maximum possible amount in cyber security ($s_c = s_b^i = 1$), they do not suppress cyber risk completely.
- (A3) $k_c > \max(\theta\underline{\alpha}\sigma l, (1-\theta)\underline{\alpha}\sigma l)$ and $k_b > \sigma l/2$. Assumption (A3) implies that investment costs $k_c$ and $k_b$ are sufficiently high such that there is an interior solution when the regulator chooses the welfare-maximizing levels of investments in security.[23]

**Timing of the game:**

1. The cloud service provider decides on the amount $s_c$ invested in the security of its infrastructure.
2. Each bank $i \in \{A, B\}$ decides non cooperatively on its level of investment $s_i$ in cyber security.
3. The cloud service provider sets an access fee $f^a$ and a compatibility fee $f^c$. Each bank decides on whether or not to outsource its payment services and on whether or not to buy the compatibility service.
4. Banks compete for depositors by choosing their deposit prices $p_i$ for $i \in \{A, B\}$, respectively.

[23] The inequality $k_b > \sigma l/2$ is implied by (A1) and (A2).

5. A cyber incident occurs with probability $h_i(s_i, s_c, \theta)$ in the payment system of bank $i \in \{A, B\}$. The depositors, the banks and the cloud service provider incur losses.

# 4 The welfare effects of cloud outsourcing

In this section, we analyze a benchmark in which a social planer chooses the welfare-maximizing levels of investment in security and the optimal level of disclosure of cyber incidents. We examine the impact of cloud outsourcing on social welfare.

## 4.1 Welfare-maximizing security investments

Social welfare is the sum of the depositors' surplus and the firms' profits less the transportation costs incurred by the depositors. We assume in this section that the losses are multiplied by the minimum factor $\underline{\alpha}$ when there is outsourcing.[24]

In Proposition 1, we give the welfare-maximizing levels of investment in security and compare payment system security with or without cloud outsourcing.

**Proposition 1** *If banks do not outsource their payment services to the cloud, the welfare-maximizing level of payment system security for banks is*

$$s_w^n = \frac{\sigma l}{2k_b}.$$

*If banks outsource their payment services to the cloud, the welfare-maximizing level of investment in payment security is*

$$(s_w^c)^c = \frac{2k_b}{k_c}(1-\theta)\underline{\alpha} s_w^n,$$

*for the cloud service provider and $(s_w^c)^b = \theta \underline{\alpha} s_w^n$ for each bank, respectively.*

*The welfare-maximizing level of security is higher if both banks outsource their payment services to the cloud if either $\Delta s^b \equiv s_w^n - \theta(s_w^c)^b \leq 0$ or $\Delta s^b > 0$ and*

$$k_c < k_s \equiv 2k_b \frac{(1-\theta)^2 \underline{\alpha}}{1-\theta^2 \underline{\alpha}}.$$

**Proof.** See Appendix 1. ■

The welfare-maximizing contributions of banks to payment system security differ with and without cloud outsourcing. The social planer chooses security investments such that the marginal benefits of a higher security are equal to the marginal costs. Cloud outsourcing multiplies the marginal benefits of banks' investments in security by a factor $\theta \underline{\alpha}$. First, banks' investments in security

[24] The minimum losses occurring with cloud outsourcing could result from endogenous choices of the social planer if there is moral hazard.

have a lower marginal impact on the probability that a cyber incident occurs, because banks only take on a marginal share $\theta$ of the security effort. Second, with cloud outsourcing, the minimum total loss equals $\underline{\alpha} l$. Therefore, banks' welfare-maximizing level of security increases if and only if $\theta\underline{\alpha} > 1$. Since banks take on a share $\theta$ of security investments, the welfare-maximizing contribution of banks to payment system security is higher with cloud outsourcing if and only if $\theta^2\underline{\alpha} > 1$.

The presence of the cloud service provider is beneficial for the society if the marginal benefits of security investments implied by cloud outsourcing exceed the marginal costs. If banks' welfare-maximizing contributions to payment system security increase with cloud outsourcing, social welfare is always higher when both banks join the cloud. If banks' welfare-maximizing contributions to payment system security are reduced, the welfare-maximizing level of security is higher with cloud outsourcing if and only if the cloud service provider's contribution compensates for the banks' lower investment.

The cloud service provider contributes marginally to payment system security in share $(1-\theta)$ and it invests a share $(2k_b/k_c)(1-\theta)\underline{\alpha}$ of the welfare-maximizing security without cloud outsourcing. Therefore, the presence of the cloud service provider implies a marginal benefit for the society that is equal to $(2k_b/k_c)(1-\theta)^2\underline{\alpha}$, and a marginal cost $(1-\theta^2\underline{\alpha})$, which are expressed in share of the initial security without outsourcing, respectively. If the inequality of Proposition 1 holds, the marginal benefits implied by cloud outsourcing exceed the marginal costs.

In the special case in which banks neither contribute to the security of the payment system (i.e., $\theta = 0$), nor do they incur additional losses with cloud outsourcing (i.e., $\underline{\alpha} = 1$), the welfare-maximizing level of security is higher with cloud outsourcing if and only if $k_c < 2k_b$. Cloud outsourcing enables the social planer to avoid an inefficient duplication of security investments, because the cloud service provider's investments benefit both banks. Thus, without cloud outsourcing, reaching the same level of security in each bank requires spending twice the same amount, which is a source of inefficiency.

## 4.2 Welfare-maximizing outsourcing decisions

An important issue is whether cloud-based interoperability is socially efficient. We denote by

$$\Delta L_w = (\underline{\alpha} h_c((s_w^c)^b, (s_w^c)^c) - h_n(s_w^n))l$$

the difference in the total expected loss with and without cloud outsourcing, respectively, and by

$$\Delta C_w = k_b((s_w^c)^b)^2 - (s_w^n)^2) + \frac{k_c((s_w^c)^c)^2}{2}$$

the difference in the costs of payment system security with and without cloud outsourcing, respectively.

In Proposition 2, we give the conditions under which the social planer should choose to build a common cloud-based payment infrastructure when it controls payment system security.

**Proposition 2** *Cloud outsourcing increases social welfare if and only if:*

$$\beta > max(0, \beta_w),$$

*with $\beta_w \equiv 2(\Delta L_w + \Delta C_w)$. If the costs of security investments incurred by the cloud service provider are sufficiently low, cloud outsourcing is beneficial for the society for any level $\beta > 0$ of network effects. Such a situation happens if and only if:*

$$k_c < k_w \equiv k_s \frac{(1-\theta^2\underline{\alpha})C_b^n}{(1-\theta^2\underline{\alpha}^2)C_b^n + (\underline{\alpha}-1)hl} < k_s,$$

*with $C_b^n = (\sigma l)^2/(4k_b)$ representing banks' cost of security if the social planer chooses a market structure without cloud outsourcing.*

**Proof.** See Appendix 1. ■

Cloud outsourcing reduces the cost of fragmentation of payment systems (see the BIS annual report, June 2022).[25] First, cloud outsourcing increases the welfare benefits of network effects by $\beta/2$, because banks' payment systems become compatible. With interoperable payment systems, a depositor is able to make a payment transaction with all other depositors (in share 1, which generates a benefit $\beta$ for the society), whereas, he makes a transaction with only half of the depositors if banks' payment systems are fragmented (with a welfare benefit of $\beta/2$). Second, as explained in Proposition 1, cloud outsourcing avoids an inefficient duplication of security investments, which benefits the society if the cloud service provider's marginal cost of security is less than twice the banks' marginal cost of security.

At the same time, with welfare-maximizing investments, cloud outsourcing may not improve payment system security and also implies additional potential losses for banks and depositors. Even if the cloud service provider discloses perfectly cyber incidents, cloud outsourcing raises the additional maximal potential loss in case of a cyber incident by $(\underline{\alpha}-1)hl$.[26] We have shown in Proposition 1 that with the welfare-maximizing levels of security investments, payment system security may be either higher or lower with cloud outsourcing than with independent banks. Therefore, cloud outsourcing may either improve or weaken payment system security. Even a higher level of payment system security may not be sufficient to compensate for the additional losses incurred by the banks and the depositors. In addition, the society benefits from a more secure payment system, only if the welfare gains from a reduction of the expected loss compensate for the costs of security investments. Thus, payment system security may

[25] The BIS report of 2022 mentions the cost of fragmented payment systems for the economy and the welfare gains associated with interoperability. The report does not mention whether the infrastructure that manages the joint payment system is public or private (see e.g. on p.91).

[26] The potential loss is maximal if security investments are equal to zero.

become also more costly with cloud outsourcing. Therefore, cloud outsourcing improves social welfare only if the benefits of interoperability are sufficiently high with respect to the marginal net costs implied by cloud outsourcing. If cloud outsourcing lowers the total cost of cyber incidents, including security investments and expected losses, social welfare is always higher when both banks join the cloud, whatever the level of network effects. This happens if the cloud service provider's marginal cost is sufficiently low (i.e., lower than $k_w$).[27]

# 5 Cyber security and bank competition

In this section, we analyze banks' decisions to outsource their payment services to a private third-party provider when they choose their investments in security non-cooperatively.

## 5.1 Stage 4: competition for deposits

We determine how banks price deposit services if they take symmetric outsourcing decisions (that is, in subgames $n$ without cloud outsourcing and $c$ with cloud outsourcing, respectively).

### 5.1.1 The deposit prices and bank profits:

We start by analyzing consumer demand for deposits. We omit in this subsection the fact that depositor losses and payment system security depend on banks' outsourcing decisions to economize on the notations.

From Eqs.(1) and (2), a naive depositor obtains a utility $u_i(x)$ of opening an account in bank $i$, while a sophisticated depositor only obtains $u_i(x) - h_i L_d$ because he expects to face the loss $L_d$ with probability $h_i$. Given that only a proportion $\mu$ of depositors are sophisticated, the average expected utility of a depositor equals $u_i(x) - \mu h_i L_d$.

We denote by $\Delta h \equiv h_i - h_{-i}$ the degree of security differentiation between banks. At the equilibrium of stage 4, depositors' expectations of banks' market shares are fulfilled, and each bank $i \in \{A, B\}$ obtains a market share given by:

$$N_i = \frac{1}{2} + \frac{p_{-i} - p_i - \mu \Delta h L_d}{2(t - (1-z)\beta)}, \tag{6}$$

where $z = 1$ if both banks join the cloud and pay the compatibility fee and $z = 0$ otherwise.[28]

[27] If banks were free to choose to join the cloud, while being constrained to choose the welfare-maximizing levels of investment in security (e.g., by a security standard), they would make inefficient decisions, as they would not take into account the impact of their outsourcing choice on the cloud service provider's investment incentives, nor on its expected loss.

[28] No bank corners the market if $N_i \in (0,1)$, which is equivalent to $p_i - p_{-i} + \mu \Delta h L_d \in (-t + (1-z)\beta, t - (1-z)\beta)$.

The market share of bank $i$ depends on the marginal cost asymmetries implied by security differentiation, which are internalized by sophisticated depositors (in proportion $\mu$). Indeed, the latter incur different expected costs of cyber incidents according to their bank choice. In addition, the price sensitivity of consumer demand for deposits is increasing with network effects if payment systems are fragmented. Indeed, consumers anticipate that when a bank undercuts the price of its rival, the value of its payment services increases because of network effects. This effect does not exist if payment systems are interoperable. Therefore, interoperability softens competition for deposits.

At the competition stage, each bank $i$ chooses $p_i$ to maximize its profit $\pi_k$ given in Eq.(3). Solving for the first-order conditions of bank profit-maximization, at the equilibrium of stage 4, if banks take symmetric outsourcing decisions, the prices of deposits are given by

$$p_i^* = t + h_i L_b + z f^a - (1-z)\beta - \frac{\Delta h}{3}\rho, \tag{7}$$

where banks' marginal cost of cyber incidents, including the internalization of the sophisticated depositors' losses, is given by :

$$\rho = L_b + \mu L_d.$$

The deposit prices chosen by banks at the equilibrium of stage 4 correspond to those of a standard Hotelling model with asymmetric marginal costs. A bank's marginal cost is the sum of the expected losses caused by cyber incidents $h_i L_b$, the access fee paid to the cloud service provider $z f^a$ (if any when $z = 1$), net of the marginal benefit of network effects $(1-z)\beta$. The last term captures the differentiation of banks' marginal costs if they choose different levels of security for their payment systems. The higher the magnitude of network effects, the higher the banks' incentives to decrease their prices if their payment systems are fragmented. Banks take into account the marginal benefits of attracting an additional depositor when they choose their prices, because they anticipate that this depositor will have a positive impact on the overall demand for deposits

Since the losses depend on banks' outsourcing decisions, we denote by $\rho^c$ and $\rho^n$ banks' marginal cost (including internalization) in the subgame $c$ and $n$, respectively. The degree of differentiation between payment systems is $\Delta h = \Delta h^c$ in the subgame $c$ and $\Delta h = \Delta h^n$ in the subgame $n$, respectively. Replacing for $p_i^*$ given by Eq.(7) in Eq.(3), the profit of bank $i$ at the equilibrium of stage 4 is given by:

$$\pi_i = \frac{(t - \beta(1-z) - (\Delta h)(z\rho^c + (1-z)\rho^n)/3)^2}{2(t-(1-z)\beta)} - z f^c - C_b(s_i). \tag{8}$$

There is full pass-through of banks' expected marginal costs to their depositors. Therefore, if banks take symmetric outsourcing decisions, the access fee has no impact on their profits.

## 5.2 Stage 3: the compatibility and the access fees

At stage 3, the cloud service provider chooses the access fee $f^a$ for its storage service and the compatibility fee $f^c$. In the rest of the analysis of stage 3, we assume, without loss of generality, that bank $A$ has a higher level of security than bank $B$ following stages 1 and 2, that is, we have $s_A \geq s_B$.

### 5.2.1 The optimal fees according to the number of outsourcing banks:

Banks' willingness-to-pay for cloud services depend on their respective levels of investment in security, and their incentives to deviate to an asymmetric equilibrium in which they offer different levels of security to their depositors.

If the cloud service provider obtains a positive demand for its storage services, it trades off between setting fees such that both banks join the cloud and become compatible or such that only one bank joins the cloud. If neither of the two banks joins the cloud, the cloud service provider makes zero profit.

Suppose that the cloud service provider serves both bank. As an upstream monopolist, it chooses the profit-maximizing compatibility fee $f^{c*}$ so as to extract banks' additional profit of compatibility. Therefore, the banks will obtain the same profit of using only the storage service (without compatibility), and becoming compatible. In Appendix 2, we show that the equalization of banks' profits in both cases gives

$$f^{c*} \equiv \frac{\beta}{2}(1 - \frac{((\Delta h^c)\rho^c/3)^2}{t(t-\beta)}). \tag{9}$$

In addition, the cloud service provider sets the maximum access fee such that each bank does not have the incentives to deviate and becoming independent. Since banks' levels of security may differ after stage 2, one bank may have higher incentives to deviate than the other, and therefore, a lower willingness-to-pay for cloud services. If it serves both banks, the cloud service provider chooses the access fee such that the bank having the lowest willingness-to-pay for the storage service joins the cloud. For this bank, the access fee equalizes the expected marginal cost of cyber incidents if it outsources and if it remains independent. Banks' expected marginal cost of cyber incidents when they join the cloud is $h_i^c \rho^c$, whereas the independent bank has an expected marginal cost given by $h_i^n \rho^n$. Therefore, in order to join the cloud, the bank that has the lowest willingness-to-pay for cloud services should pay a maximum access fee implicitly defined by

$$h_i^c \rho^c + f_i^{a*} \equiv h_i^n \rho^n. \tag{10}$$

If $f_A^{a*} \geq f_B^{a*}$ or else if $\theta\rho^c \leq \rho^n$, the riskiest bank B has the highest willingness-to-pay for cloud services, because its marginal cost (including the limit access fee) $f_B^{a*} + h_i^c \rho^c$ is lower than that of bank A. The reverse is true otherwise.

Suppose now that the cloud service provider serves only one bank. It chooses the access fee that equalizes the bank's marginal cost of joining the cloud and remaining independent. As shown in Appendix 2, if cloud outsourcing increases both banks' marginal costs, the cloud service provider never makes positive profits if only bank A outsources its payment services. This situation happens if the riskiest bank B has the lowest willingness-to-pay for cloud services. The intuition is that the cloud service provider is not able to extract enough rents from bank A, which enjoys high benefits of security differentiation if it remains independent. Therefore, in that case, the cloud service provider serves either both banks, or does not enter the market. The cloud service provider is also ready to subsidize access to extract rents from the compatibility service. Otherwise, if the riskiest bank B has the highest willingness-to-pay for cloud services, the cloud service provider may serve either one or two banks, or decide not to enter the market.

We determine in Lemma 1 the profit-maximizing fees chosen by the cloud service provider according to the number of outsourcing banks.

**Lemma 1** *If both banks outsource their payment services, the cloud service provider sets a compatibility fee equal to $f^{c*}$, and it sets an access fee equal to the lowest willingness-to-pay for cloud services, that is*

$$min\{f_A^{a*}, f_B^{a*}\} = \begin{cases} f_A^{a*} & \textit{if } \theta\rho^c \leq \rho^n \\ f_B^{a*} & \textit{otherwise.} \end{cases}$$

*If only the riskiest bank B outsources its payment services, the cloud service provider sets an access fee equal to $f_B^{a*}$.*

**Proof.** Appendix 2. ■

It is interesting to note that the cloud service provider subsidizes access when both banks' marginal cost of cyber incidents increases if they join the cloud, which happens if and only if the riskiest bank has the lowest willingness-to-pay for cloud services.

### 5.2.2 The cloud service provider's optimal strategy:

We determine the conditions such that the cloud service provider prefers to serve both banks, only the riskiest bank, or remain inactive. At this stage of the game, banks are differentiated in security. However, to simplify the exposure of the results, we focus on the case in which banks take symmetric investment decisions at stage 2, which will happen at the equilibrium of the game with endogenous security investments. We denote by $\overline{\rho}^c \equiv \rho^c + L_c$ the total marginal cost of cyber incidents internalized by the cloud service provider.

We derive in Proposition 3 the conditions such that the cloud service provider enters the market and serves both banks.[29]

**Proposition 3** *If banks choose symmetric investments in security, banks outsource their payment services and become compatible if and only if the cloud service provider makes a positive profit, that is, if and only if* $\beta \geq \max\{0, \widehat{\beta}\}$, *with*

$$\widehat{\beta} \equiv h^c \overline{\rho}^c - h^n \rho^n + C_c(s_c). \tag{11}$$

*Otherwise, the cloud service provider does not enter the market and banks remain independent.*

**Proof.** Appendix 2. ■

Banks join the common private infrastructure managed by the cloud service provider and become interoperable if and only if the magnitude of network effects is sufficiently high. For the cloud service provider, the private benefit of entering the market and serving both banks is equal to the sum of the value of network effects and the access fee (that is, $\beta + f^{a*}$). The private cost is equal to its expected cost of damage and its cost of security investment (or else, $h^c(s_c, s_b^c)L_c + C_c(s_c)$). The cloud service provider enters the market when its private benefit exceeds its private cost.[30]

As shown in the next section, an asymmetric equilibrium does not exist in our setting. However, the possibility that banks take asymmetric outsourcing decisions to enjoy the benefits of security differentiation impacts the characterization of the symmetric equilibrium where both banks join the cloud. Indeed, the cloud service provider internalizes banks' incentives to deviate to an asymmetric outsourcing market structure when it chooses the access fee.

**The distortions with respect to the first-best:**

In Proposition 4, we compare banks' outsourcing decisions with cyber risk to the first-best with exogenous investments.

**Proposition 4** *With cyber risk and different investment levels with and without cloud outsourcing, there may be either excessive outsourcing or under-outsourcing to the cloud compared to the first-best. If* $\beta^w > \widehat{\beta}$, *banks outsource excessively their payment services when* $\beta \in (\widehat{\beta}, \beta^w)$. *If* $\beta^w < \widehat{\beta}$, *banks under-outsource their payment services when* $\beta \in (\beta^w, \widehat{\beta})$.

**Proof.** The difference between banks' private incentives to outsource their payment services and the social optimum depends on $\beta^w - \widehat{\beta}$. We show in Appendix 4 that we may either have $\beta^w - \widehat{\beta} > 0$ or the reverse. ■

[29] All the details with asymmetric investment decisions are given in Appendix 2.

[30] The final expression of Proposition 3 is obtained by replacing for $\overline{\rho}^c = \rho^c + L_c$ and $f^{a*} = h_i^n \rho^n - h_i^c \rho^c$.

Because of cyber risk, there may be either over-outsourcing or under-sourcing of payment services to a third-party. To understand why, we start by considering that there is no cyber risk and that banks do not incur any investment costs. If banks' investments in security are exogenous and constant, if there is no cyber risk ($h^n = h^c = 0$), cloud outsourcing is socially desirable if and only if $\beta/2 \geq C_c(s_c)$.[31] However, banks take the private decision to outsource their payment system the cloud if and only if $\beta \geq C_c(s_c)$.[32] Therefore, banks join the cloud for an inefficiently low level of network effects. Indeed, the marginal social benefit of interoperability equals $\beta/2$, as all depositors value marginally at $\beta$ the benefit of making transactions with the depositors of the other bank (in proportion 1/2). However, banks value excessively the benefits of compatibility with respect to the social optimum. Indeed, *each bank* values its benefit from the compatibility service at $\beta/2$, as it does not internalize the benefits of compatibility of its competitor. The cloud service provider extracts the rents that both banks obtain from compatibility through the access fee (i.e., $2 * \beta/2$). Therefore, the private benefits of outsourcing are twice as high as the marginal social benefit of outsourcing. This implies that cloud outsourcing occurs for an inefficiently low level of network effects, compared to the social optimum. This result is standard in the literature on network industries (e.g., in Foros and Hansen, 2001).

The cloud service provider does not internalize banks' costs of security, which adds another distortion with respect to the first-best. For exogenous levels of investment, the regulator prefers that both banks join the cloud if and only if $\beta/2 \geq \Delta C_w$, with $\Delta C_w = 2(C_b((s_w^c)^b) - C_b(s_w^n)) + C_c(s_c)$. If banks' costs of security increase with cloud outsourcing when the market regulated (i.e, $C_b((s_w^c)^b) - C_b(s_w^n)) > 0$), the bias towards excessive outsourcing is reinforced compared to the first-best (resp., reduces the bias if $C_b((s_w^c)^b) - C_b(s_w^n)) < 0$). Indeed, the cloud service provider does not internalize banks' investment costs and enters the market when $\beta \geq C_c(s_c)$.

Cyber risk adds another inefficiency compared to the first-best. Suppose that the minimal social damage is identical with and without cloud outsourcing ($\underline{\alpha} = 1$). From Proposition 2, we see that cloud outsourcing is socially desirable if and only if $\beta/2 \geq \Delta L_w + \Delta C_w$. The marginal social cost of outsourcing now includes the variation of the total social loss given by:

$$\Delta L_w = (h^c - h^n)l.$$

With private outsourcing decisions, the cloud service provider internalizes imperfectly the variation of the losses caused by outsourcing. We denote by $L_d^n$ the depositors' losses without outsourcing and by $L_d^c$ the depositors' losses with outsourcing. The marginal additional loss internalized by the cloud service provider is lower that the variation of the social loss caused by outsourcing if and only if

$$(1 - \mu)(h^n L_d^n - h^c L_d^c) > 0.$$

[31] This results stems from Proposition 2, with $\Delta L_w = 0$ and $\Delta C_w = C_c(s_c)$.

[32] This results stems from Proposition 3 without cyber risk, and thus, no expected damage and no access fee.

If the private investment levels are exactly identical to the welfare-maximizing levels of investment, there is a distortion if some depositors are naive ($\mu < 1$). Banks internalize a lower share of the variation of the depositors' losses caused by the decision to outsource than in the first-best scenario. If cloud outsourcing increases cyber risk (i.e., $h^c > h^n$), banks incur a marginal cost of outsourcing which is too low with respect to the marginal social cost (resp., too high if cloud outsourcing decreases cyber risk). This effect implies that there is either under-outsourcing or over-outsourcing.

**The impact of cloud outsourcing on bank profits and depositor surplus:**

In Proposition 5, we detail the effect of cloud outsourcing on the profits of banks and depositor surplus, respectively.

**Proposition 5** *Suppose that banks have invested symmetric levels of security at stage 2. Cloud outsourcing increases banks' profits if and only if it reduces their security investments (i.e., if $s_b^c \leq s_b^n$). Depositor surplus is higher with cloud outsourcing if and only if*

$$\sigma\rho(0)(s_b^c - s_b^n) \geq \frac{\beta}{2}.$$

**Proof.** See Appendix 3. ■

Banks' profits on the deposit market are independent from cyber risk if they choose symmetric levels of investment in security. Therefore, banks benefit from joining the cloud if this decision reduces their expected marginal cost of cyber incidents.

If payment system security is lower in the cloud, depositor surplus is always reduced by cloud outsourcing. The reason is that interoperability softens competition for deposits, which increases depositor prices. If payment system security is higher in the cloud, depositor surplus may increase with cloud outsourcing for low values of network effects. In that case, the positive effect of cloud outsourcing on payment system security compensates for the rise in deposit prices.

## 5.3 Stage 2: banks' investment in security

In the next subsections, we endogenize investments in cyber security. At stage 2, each bank $i \in \{A, B\}$ chooses the level of security that maximizes its profit. We give in Lemma 2 the profit-maximizing levels of investment chosen by banks at the equilibrium of stage 2.

**Lemma 2** *The subgame in which banks choose their investment in security admits a unique symmetric Nash equilibrium. If both banks remain independent, they invest an amount of security given by*

$$s_b^{n*} = \sigma\frac{\rho(0)}{3k_b}, \tag{12}$$

*and if both banks join the cloud, they invest an amount of security given by*

$$s_b^{c*} = \sigma\theta\frac{\rho(v^*)}{3k_b}. \tag{13}$$

**Proof.** See Appendix 4. ■

Banks choose their investments in security such that their marginal benefit equals their marginal cost. Depending on their outsourcing decision, bank's marginal cost of security investment is either $k_b s_b^c$ or $k_b s_b^n$. The marginal benefit of security investment is equal to $\sigma\theta\rho^c/3$ when banks join the cloud, because banks only contribute to a share $\theta$ of payment system security. When banks do not join the cloud, their marginal benefit is $\sigma\rho^n/3$. Therefore, banks' investments in cyber security decrease when they join the cloud (compared to the no outsourcing case) if their marginal benefit of security investment increases. Compared to the social optimum, banks reduce their investments in security to soften competition for depositors.

## 5.4 Stage 1: The equilibrium of the game

At stage 1, the cloud service provider chooses the level of investment in security $s_c^*$ that maximizes its profit $\pi_C^c$ given in Proposition 4. Solving for the first-order condition gives

$$s_c^* \equiv \sigma(1-\theta)\frac{\overline{\rho}^c}{k_c}. \tag{14}$$

The cloud service provider's investment in security is maximal when the total marginal cost internalized by the cloud service provider is maximal.

At the equilibrium of the game, from Proposition 3, both banks outsource their payment services if and only if the cloud service provider makes a positive profit. Therefore, the cloud service provider makes a positive profit if and only if the magnitude of network effects is sufficiently high, that is, if and only if $\beta > \max\{0, \widehat{\beta}\}$, with

$$\widehat{\beta} \equiv h^c(s_c^*, s_b^{c*})\overline{\rho}^c - h^n(s_b^{c*})\rho^n + C_c(s_c^*). \tag{15}$$

If $\widehat{\beta} \leq 0$, both banks always join the cloud. This happens if the expected damage incurred by the firms decreases more than the security costs of the cloud service provider, or else, if and only if $k_c < \widehat{k}_c$, where $\widehat{k}_c$ is given in Appendix 4.

### The distortions with endogenous investments:

With endogenous investments in security, there are additional distortions with respect to the first-best. Banks do not take into account the effect of their investments on the damage incurred by the cloud service provider when they choose how much to invest in security, which reduces their investment incentives. Also, both banks and the cloud service provider choose their levels of investment without internalizing the effect of the outsourcing on the expected damage of myopic depositors if they are not liable for the damage. The under-investment of the cloud service provider always leads to over-outsourcing, because the cloud service provider has higher incentives to enter the market when its profit increases. However, the under-investment of banks may either increase or decrease the incentives of the cloud service provider to enter the market with respect to the first-best, through their impact on the access fee.

# 6 The liability regime and moral hazard

In this section, we use our baseline model to analyze the role of the liability regime for cyber incidents when the cloud service provider may not disclose all the information on cyber incidents.

## 6.1 Extension of our model setup with moral hazard

One difficulty with the liability regime for cyber incidents is caused by the lack of incentives both for the banks and the cloud service provider to report cyber incidents to the depositors, which may prevent them to claim compensation.[33] This specific characteristic of cyber risk is a source of concern for the financial supervisors and regulatory bodies (see for instance the reports by the European Banking Authority, 2019, and the UK House of Commons, 2019).

Banks' incentives to report cyber incidents to their depositors are arguably higher than that of a cloud service provider, because of reputation incentives created by long-term relationships, cross-selling of financial services and regular audits performed by the financial supervisor.[34]

**Information disclosure on cyber incidents:** We denote the amount of information concealed by a bank and the cloud service provider from the other players by $v_b$ and $v_c$, respectively. The total amount of information $v$ concealed on the cyber incident depends on the sharing of security investments, that is, we have $v = \theta v_b + (1-\theta)v_c$.

We assume that the cloud service provider does not have the incentives to disclose perfectly the information on cyber incidents to the other players, while banks are perfectly transparent. The amount of information hidden by the cloud service provider $v_c \in (\underline{v_c}, \overline{v_c})$ depends on its cost $K(v_c) = \kappa(v_c^2 - \underline{v_c^2})/2$ of concealing information, with $K(\underline{v_c}) = 0$, $K'(v_c) > 0$ and $K''(v_c) > 0$.[35] Both banks conceal the same exogenous amount of information $v_b$, which we normalize to $v_b \equiv 0$. This implies that $v = (1-\theta)v_c$.

[33] On a sample of 276 incidents between 2010 and 2015 occurring in various sectors, Amir et al. (2018) estimated that, on average, firms hid cyber-attacks if their investors perceive the probability of the attack to be below 40%.

[34] See the reports by Horvath et al. (2014) and Robinson et al. (2011) for justifications of the cloud service provider's lack of incentives to report cyber incidents. The financial supervisor may not have the mandate to supervise the cloud service provider, which is sometimes not located in the same country.

[35] This simplification remains valid as long as the cost of disclosing cyber incidents is much higher for the cloud service provider than for the banks.

If the cloud service provider does not disclose perfectly all the information on cyber incidents to the other players, the depositors and the banks may not claim compensation or find convincing evidence that a cyber incident occured (as in Daughety and Reinganum, 2005). Therefore, we assume that they are able to claim compensation with some positive probability $q(v) \in (0,1)$, which is a decreasing convex function of $v$ such that $q(0) = 1$, $q(1) \in (0,1)$, $q'(v) \leq 0$ and $q''(v) \geq 0$ for all $v \in ((1-\theta)\underline{v_c}, (1-\theta)\overline{v_c})$.

If the information is not disclosed perfectly by the cloud service provider, the amount of the losses incurred by the banks and the depositors, respectively, is multiplied by a factor $\alpha(v)$ and increases with the amount of hidden information. If all information is disclosed, we have $v = 0$ and $\alpha(0) = 1$. We further assume that $\alpha((1-\theta)\underline{v_c}) = \underline{\alpha}$ and $\alpha((1-\theta)\overline{v_c}) = \overline{\alpha}$. The cloud service provider chooses how much information to hide on cyber incidents at stage 5 of the game.

**The liability regime for cyber incidents:** We consider a regime with strict liability and discuss in the extension section other possible regulatory instruments.[36] Without cloud outsourcing, the liability system defines the amount of compensation $\eta_d \in (0, l_d)$ given by the bank to a depositor when a cyber incident occurs.[37] Therefore, the bank incurs a loss $l_d + \eta_d$ and each depositor incurs a loss $l_d - \eta_d$. In addition, with cloud outsourcing, the liability system defines the transfers $\gamma_d$ and $\gamma_b$ from the cloud service provider to the depositor and the bank, respectively. Such transfers are common in payment systems (e.g., Visa and MasterCard).[38]

**The losses:** Following a cyber incident, if a bank joins the cloud, each depositor claims compensation with probability $q$ and incurs a loss

$$L_d(v) = \alpha(v)l_d - q(v)(\eta_d + \gamma_d),$$

the bank incurs a loss

$$L_b(v) = \alpha(v)l_b + q(v)(\eta_d - \gamma_b),$$

[36] We do not include in our discussion a comparison with the negligence rules, which would involve changing our model to include the role of regulatory audits. The sharing of the losses for cyber incidents may vary across jurisdictions and depends on the liability regime. If banks do not outsource their services to the cloud, there is evidence that banks may be held liable for the cyber incidents that affect their depositors (e.g., in the United-States, Ocean Bank versus Patco Construction Company, the case of Comerica Inc. versus Mich. Experi-Metal). In the US, litigation follows almost all publicly disclosed breaches (Southwell et al., 2017). If banks outsource their services to the cloud, several jurisdictions make a distinction between the user of the service, the data owner (the bank) and the data holder (a cloud service provider providing hosting services). In the United-States (except HIPAA which places direct liability on a data holder), the data owner is liable for the losses resulting from a data breach, even if the security failures result from insufficient investment from the data holder (cloud provider).

[37] In a landmark cyber security case, the UK Financial Conduct Authority (FCA) has fined Tesco Personal Finance plc (Tesco Bank) £16,400,000 after a cyber attack exposed weaknesses in the design of its debit card business and affected 8,261 personal current accounts.

[38] The payment system Heartland had to compensate several banks after a security breach and it paid 60 million dollars of financial damages.

and the cloud service provider incurs a loss

$$L_c(v) = q(v)(\gamma_d + \gamma_b) + K(v), \tag{16}$$

We include into $L_c$ the additional cost $K$ of not disclosing cyber incidents to the other players.[39] The total loss caused by a cyber incident is

$$L(v) = \alpha(v)l + zK(v).$$

**Additional assumption:** Finally, we make one additional assumption.

(A4): For all $v_c \in (\underline{v_c}, \overline{v_c})$, we have $L_c''(v_c) \geq 0$, with $L_c'(\underline{v_c}) < 0 < L_c'(\overline{v_c})$. Assumption (A4) is a necessary condition for the cloud service provider not to disclose either the minimum or the maximum level of information on cyber incidents to the other players.

## 6.2 Moral hazard and outsourcing decisions

In this subsection, we solve the extended version of our model with moral hazard.

### 6.2.1 Stage 5: information disclosure on cyber incidents:

At the last stage of the game, if bank $i$ joined the cloud, the cloud service provider observes whether a cyber incident has occurred with the depositors of bank $i$, and it chooses how much information to hide on the cyber incident. The cloud service provider maximizes its profit by minimizing its expected loss in case of incident $L_c(v)$, given in Eq.(16). If $\gamma_d + \gamma_b > 0$ and $\theta < 1$, the loss-minimizing level of information $v_c^*$ equalizes the marginal benefit of avoiding to be liable for the cyber incident and the marginal cost of hidden information, that is we have

$$-(1-\theta)(\gamma_d + \gamma_b)q'(v^*) = \kappa v_c^*, \tag{17}$$

where $v^* = (1-\theta)v_c^*$. When the liability regime allocates a higher share of the losses to the cloud service provider, its incentives to disclose cyber incidents are reduced, because the latter prefers to avoid becoming liable. If the cloud service provider is not liable (i.e., if $\gamma_d + \gamma_b = 0$), it hides the minimum amount of information from the bank and depositors, that is, we have $v^* = (1-\theta)\underline{v_c}$.

If bank $i$ does not join the cloud, this bank and its depositors are perfectly informed on cyber incidents. Therefore, the amount of information hidden to bank $i$ and its depositors equals $zv^*$, where $z = 0$ for the bank that does not join the cloud, and $z = 1$ for its competitor if the latter joins the cloud.

[39] The expressions of $L_d$ and $L_b$ encompass the case in which banks do not join the cloud, when $\gamma_b = \gamma_d = 0$, $z = 0$, $\theta = 1$ (full contribution of banks to security), $v = 0$ (perfect disclosure), $\alpha(0) = 1$ (no additional damage) and $q(0) = 1$ (perfect ability to claim compensation).

### 6.2.2 The impact of the liability regime on the internalized marginal costs:

The liability regime impacts banks' marginal costs of cyber incidents. Without cloud outsourcing ($z = 0$), a bank's marginal cost of cyber incidents, including internalization effects, is given by:

$$\rho^n = l + (1 - \mu)(\eta_d - l_d).$$

and with cloud outsourcing ($z = 1$), it is given by:

$$\rho^c = \alpha(v^*)l + (1 - \mu)(q(v^*)\eta_d - \alpha(v^*)l_d) - q(v^*)(\mu\gamma_d + \gamma_b). \tag{18}$$

We proceed by analyzing how the liability regime impacts the banks' marginal costs: the transfer of banks to depositors $\eta_d$ and the transfers of the cloud service provider to the depositors and to the bank, $\gamma_d$ and $\gamma_b$, respectively. We explain below that the effects of the liability regime depends on depositor sophistication and moral hazard.

The transfer $\eta_d$ impacts banks' marginal cost only if some depositors are naive ($\mu < 1$). If all depositors are sophisticated ($\mu = 1$), banks internalize perfectly the depositors' losses. Without cloud outsourcing, their marginal cost of cyber incidents is equal to the total loss $l = l_b + l_d$. With cloud outsourcing, their marginal cost is equal to the total loss, less the total transfers received from the cloud service provider when a cyber incident is disclosed (i.e, $\alpha(v^*)l - q(v^*)(\gamma_d + \gamma_b)$). In both cases, the transfer $\eta_d$ is neutral, because the banks pass on their marginal cost to the depositors through higher deposit prices. If some depositors are naive, the banks internalize imperfectly the depositors' losses. Therefore, a higher transfer $\eta_d$ increases their marginal cost.

The impact of the transfers from the cloud service provider on banks' marginal costs depends on moral hazard. With an exogenous amount of hidden information, the transfers from the cloud service provider reduce banks' marginal costs. However, because of moral hazard, the cloud service provider hides more information when its liability is extended, which has an ambiguous impact on banks' marginal costs. Taking the derivative of $\rho$ with respect to the amount of hidden information $v$ gives:

$$(\rho^c)'(v) = \alpha'(v)(l_b + \mu l_d) + q'(v)(\eta_d(1 - \mu) - \mu\gamma_d - \gamma_b). \tag{19}$$

On the one hand, if the cloud service provider hides more information, banks' expected damage increases, which raises their marginal cost. On the other hand, this reduces the probability that banks have to compensate their depositors for cyber incidents when the latter are unable to claim compensation. This second effect lowers their marginal cost.

To explain the role of moral hazard and depositor sophistication, we consider examples:

- **High proportion of sophistication of depositors:**
  If the proportion of sophisticated depositors is high ($\mu$ close to 1), such

that $\eta_d(1-\mu) - \gamma_b - \mu\gamma_d < 0$, the bank's marginal cost of cyber incidents is increasing with the amount of hidden information by the cloud service provider. Then, increasing the liability of the cloud service provider raises the bank's marginal cost, because the cloud service provider hides more information when its liability is extended.

- **Low impact of disclosure on additional damage:** Suppose that the additional damage is not sensitive to the amount of information hidden by the cloud service provider ($\alpha'(v) = 0$). If the transfers received from the cloud service provider are low (i.e., $\gamma_d$ and $\gamma_b$ close to zero), the bank's marginal cost of cyber incident is decreasing with the amount of hidden information by the cloud service provider because $\eta_d(1-\mu) \geq 0$. In that case, higher transfers from the cloud service provider unambiguously decrease the bank's marginal cost.

- **Low impact of disclosure on the ability to claim compensation:** If the bank and the depositors' ability to claim compensation is not sensitive to the disclosure of information on cyber incidents ($q'(v) = 0$), the bank's marginal cost of cyber incidents is increasing with the amount of hidden information, and therefore, with the transfers from the cloud service provider.

#### 6.2.3 The impact of the liability regime on investments in payment system security:

The transfers received from the cloud service provider impact banks' marginal cost $\rho^c$, and therefore, their investment incentives. The maximum contribution of banks to payment system security is obtained when their marginal cost of cyber incident is maximal. If the cloud service provider is not liable, and if there is a positive proportion of naive consumers (such that $1 - \mu > 0$), this is achieved by increasing banks' liability towards their depositors. If the cloud service provider is liable, the transfers that maximize banks' marginal cost depend on the intensity of moral hazard. If the amount of hidden information is exogenous, the transfers should be set to zero to maximize banks' investment incentives. However, with moral hazard, positive transfers may improve banks' investment in security. Indeed, banks may decide to invest more to protect themselves from the additional damage that is caused by the under-reporting of cyber incidents. On the other hand, banks may face lower marginal costs when the cloud service provider hides cyber incidents.

The liability regime for cyber incidents impacts the cloud service provider's investment incentives through two main channels: depositor sophistication and moral hazard.

Suppose first that the amount of hidden information is exogenous. Then, the transfer from the cloud service provider to the banks ($\gamma_b$) has no impact on its marginal cost of cyber incident, because it can be extracted through the access fee. The cloud service provider's investment is maximal if the transfer to depositors ($\gamma_d$) is maximal, if there is at least a small proportion of naive depositors. In this case, banks do not internalize perfectly the cloud service provider's transfer to the depositors. Therefore, the transfer from the cloud service provider to the depositors is not neutral and increases the cloud service provider's marginal cost.

With moral hazard, the impact of the liability regime changes. A higher transfer to the banks ($\gamma_b$) is likely to increase the cloud service provider's investment incentives, because it internalizes the additional damage incurred by banks when there is hidden information. If all depositors are sophisticated (i.e, $\mu = 1$), increasing the cloud service provider's transfers to the banks and the depositors, respectively, is the best way to increase its investment incentives. The cloud service provider hides more information, but all firms (including the cloud service provider) invest more to protect themselves from the additional potential damage. However, if there is a positive proportion of naive depositors, the case for increasing the cloud service provider's transfers is less clear. Moral hazard may decrease banks' marginal costs, in which case the cloud service provider benefits from the internalization of banks' cost savings when a cyber incident is hidden.

We conclude this analysis by comparing in Proposition 6 the cloud service provider's investment in security when it is liable and without liability.

**Proposition 6** *If the minimum amount of hidden information is $\underline{v_c} = 0$, the cloud service provider has higher investment incentives when it is liable than without liability if and only if:*

$$(1-\mu)(1-q(v^*))\eta_d \leq (\alpha(v^*)-1)(l_b+\mu l_d) + (1-\mu)q(v^*)\gamma_d + K(v^*). \quad (20)$$

**Proof.** The cloud service provider has higher investment incentives when it is liable than when it is not if and only if its total marginal cost when it is liable (including internalization effects) is higher than its marginal cost with zero liability (with $\gamma_b = \gamma_d = v^* = 0$). ■

A liability regime that includes transfers from the cloud service provider may increase the cloud service provider's investment in specific circumstances. The transfers to the bank and to the depositors, respectively, do not have the same effect on the cloud service provider's investment incentives (See Eq.(20)). On the one hand, if there is no moral hazard, higher transfers to the depositors increase the cloud service provider's investment incentives if there is a positive proportion of naive depositors. The transfers to the bank are neutral, because the cloud service provider is able to extract them perfectly through the choice of a higher access fee. On the other hand, with moral hazard, there is an additional indirect effect. Higher transfers (either to the banks or to the depositors) affect the cloud service provider's incentives to disclose information when a cyber incident occurs, with ambiguous consequences on the banks' marginal cost (which is extracted through the access fee), as discussed in section 5.2.2. Therefore, because of the internalization effects, the transfers to the bank and to the depositors are not equivalent instruments to increase the cloud service provider's investment incentives. Allowing the cloud service provider to compensate the depositors directly is more efficient to improve the security of payment systems than imposing transfers to the banks if there is no moral hazard. With moral hazard, extending the cloud service provider's liability (either towards the banks or the depositors) may sometimes decrease the cloud service provider's investment in security, because banks avoid being liable towards their depositors when the cloud service provider hides a cyber incident.[40]

In practice, financial regulators often expect that their supervised institutions should retain full responsibility for outsourced services (e.g, the FDIC). Proposition 6 shows that this regulatory option may sometimes reduce the cloud service provider's investment in security. Other regulators (like the Australian APRA) have a more balanced position, which emphasizes the role of the shared responsibility model. In such a framework, each party is accountable for different aspects of security investment and monitoring.

In addition, the transfer of the cloud service provider to the depositors is not neutral when some depositors are naive. The cloud service provider's total marginal cost increases when it has to give a higher amount of compensation to the depositors. The transfer limits the inefficiency caused by over-outsourcing when cyber risk increases in the cloud but it amplifies the inefficiency caused by under-outsourcing otherwise.

### 6.2.4 Moral hazard and the distortions of outsourcing decisions:

The presence of moral hazard impacts the variation of the total loss caused by outsourcing with exogenous levels of investment. We have seen that moral hazard impacts the total damage internalized by the bank, and therefore, by the cloud service provider (see Eqs. (15) and (25)). If the cloud service provider internalizes a higher share of the damage because of moral hazard, this reduces the bias towards excessive outsourcing (see Eq. (28)). This is the case for instance if the depositors' ability to claim compensation is not sensitive to the disclosure of information on cyber incidents. However, if the cloud service provider internalizes a lower share of the damage, the bias towards excessive outsourcing is reinforced. This happens if the additional damage is not sensitive to moral hazard, if the cloud is not liable, and if the ability to claim compensation is very sensitive to moral hazard.

In addition, moral hazard changes banks' investments incentives. If banks' invest more to protect themselves from the additional damage caused by moral hazard, the cloud service provider has a higher marginal cost of outsourcing, because it extracts lower rents. Therefore, this effect reduces the bias towards excessive outsourcing compared to the first-best.

#### The role of liability regime

The liability regime for cyber incidents may not suppress the distortion caused by the presence of naive depositors. However, it may impact the distortions

[40] See Appendix 6 for the full details of the impact of the liability regime on security investments.

caused by moral hazard and affect the players' investment incentives. One interesting question is whether increasing the cloud service provider's liability may provide banks with higher incentives to become interoperable. The answer to this question is not clear. On the one hand, raising the cloud service provider's marginal cost may reduce the cloud service provider's expected loss, which may lower the threshold value of network externalities such that banks become interoperable. On the other hand, the cloud service provider has incentives to increase its investment in security, which may raise its investment cost. This effect may reduce the cloud service provider's incentives to enter the market. Therefore, a liability regime with transfers from the cloud service providers to the banks and the depositors may not necessarily provide banks with higher incentives to become interoperable. This might not be a concern if banks tend to outsource excessively to the cloud in a given market, but could be problematic if banks do not rely on a joint payment infrastructure when this would be socially desirable.

## 6.3 Alternative remedies

In this section, we discuss the potential remedies to the inefficiencies that arise when banks make private outsourcing decisions.

### i) Regulatory control of cloud outsourcing agreements:

The financial regulator can intervene in the market by refusing to authorize cloud outsourcing when there is excessive outsourcing. This could happen in several countries (e.g., England, Australia), where banks need to show their outsourcing agreements to the financial supervisor before joining a cloud-based infrastructure. This regulatory option may correct the bias towards excessive outsourcing. However, this instrument is inefficient to correct for the bias towards under-outsourcing that may arise with cyber risk.[41]

So far, in the welfare analysis, we have studied the case in which the regulator controls firms' decisions to outsource their payment services and their levels of security investments. Another possibility is that the regulator only controls outsourcing decisions at stage 3 after the cloud has chosen its prices and firms have invested in security (see Appendix 7). Since there is an imperfect disclosure of cyber incidents with cloud outsourcing, the regulator authorizes banks to outsource their payment service for a higher degree of network externalities than in the first-best.

The effect of banks' investment in security on the regulator's incentives to authorize outsourcing is twofold. First, with and without cloud outsourcing, banks reduce their investment in security to soften competition for deposits compared to the first-best. If this effect has more consequences on social welfare when banks outsource (i.e., if $\theta\alpha(v^*) > 1$), the regulator prefers that banks remain independent. Second, the compensation offered by the cloud service

[41] In addition, one potential difficulty with this type of regulatory tool consists in establishing precise criteria for authorizing cloud outsourcing agreements.

provider and moral hazard imply that banks internalize less damage when they outsource, which increases the regulator's incentives not to authorize outsourcing, compared to the first-best.

Unlike banks, the cloud service provider may either over-invest or under-invest in security with respect to the first-best. If its reputation cost is high enough (i.e., if $K(v^*) > \alpha(v^*)(1-\mu)L_d(v^*)$), the cloud service provider may increase its security investment, which offsets partially the fact that banks internalize less damage. However, this is not sufficient to increase the overall level of security. It follows that the regulator has lower incentives to authorize outsourcing than in the first-best.[42]

To conclude, if banks keep a high share of investment in payment system security (i.e., if $\theta$ is high enough) or if the cloud service provider is likely to under-report cyber incidents, the inability of the supervisor to implement first-best security decisions restricts its incentives to promote outsourcing. However, if banks delegate a high share of their investment in security to the cloud service provider, and if the latter is disciplined by a private reputation cost in case of a cyber incident, the regulator may prefer to delegate the management of the payment system infrastructure to the third-party provider rather than to the banks.

### ii) The shared responsibility model:

Another option for the financial regulator consists in by assessing ex ante the perimeter of responsibility of the cloud service provider and the banks, in terms of investment and maintenance of the security of the joint payment system. The Australian regulator (APRA) calls this regulatory option "the shared responsibility model".

In that case, we assume that a cyber incident occurs in a bank with probability $h^b = \theta(h - \sigma s_b)$, and in the cloud with probability $h^c = (1-\theta)(h - \sigma s_c)$, respectively. Compared to our setting, the probability that the system is attacked and firms' contribution to security investment remain unchanged. The only difference with respect to our setting is that a firm only compensates the other parties (the depositors for the banks, and the depositors and the banks for the cloud) when the cyber incident occurs in its perimeter of responsibility.

We denote by $s_b^{sr*}$ and $s_c^{sr*}$ the respective security investment of the outsourcing banks and of the cloud service provider under the shared responsibility model. Replacing for $\rho(v^*)$ in the equilibrium security investments $s_b^{c*}$ and $s_c^*$ given in Eq.(13) and Eq.(14) gives the banks' security investment:

$$s_b^{sr*} = s_b^{c*} + \sigma\theta \frac{\gamma_b + \mu\gamma_d}{3k_b},$$

[42] If the cloud service provider over-invests in security, this does not compensate for the fact that banks under-invest when they join the cloud, because the probability of attack is linear in each player's investment.

and the cloud service provider's investment:

$$s_c^{sr*} = s_c^* - \sigma(1-\theta)\frac{(1-\mu)\eta_d}{k_c}.$$

With the shared responsibility model, if a cyber incident hits a bank, its internalized damage increases by $\gamma_b + \mu\gamma_d$, compared to our setting. The cloud service provider no longer compensates the banks nor their depositors in that case, which increase banks' liability. This makes the depositors more sensitive to banks' security investments. Therefore, the access fee decreases, and banks invest more in security than in our benchmark setting. If a cyber incident hits the cloud service provider, the damage internalized by the bank decreases by $(1-\mu)\eta_d$, because the bank does not compensate its depositors. Since banks' expected marginal cost of cyber incidents decreases, they pay a higher access fee. Therefore, the sensitivity of depositor demand to the investment of the cloud service provider decreases.

The shared responsibility model has two effects on banks' investment incentives compared to our setting. On the one hand, since the sensitivity of sophisticated depositors to banks' investments increases if the cyber incident occurs in the bank, banks invest more in security. On the other hand, when the cyber incident occurs in the cloud, banks do not compensate their depositors. Therefore, their marginal cost decreases, because they do not take into account the damage of myopic depositors. This reduces their investment incentives compared to our setting. The first effect dominates the second effect if the proportion of myopic depositors is sufficiently low. Therefore, banks invest more in security than in our setting with the shared responsibility model if the proportion of sophisticated depositors is sufficiently high.

### iii) Mandatory levels of investment in security:

Another option for the regulator consists in setting up security standards that are equal to the first-best levels of security investments for each player. If firms always comply with the standard, this affects banks' incentives to join the cloud.[43] However, this second-best policy instrument may not correct for the distortions that arise because of the vertical structure, and in particular, the fact that the cloud service provider internalizes imperfectly the damage.

### iv) Public management of a common infrastructure in the cloud:

One last policy option consists in building a public cloud when this is socially desirable. In that case, the regulator is able to decide how much to invest in cloud security for the shared infrastructure, and the banks may choose ex post their levels of investment for their part of the system, before competing in the market for deposits. This option has been chosen by several emerging countries

[43] This may not be the case that firms comply with the standard. In that case, the regulator may incur the costs of auditing firms regularly.

for the development of a joint payment infrastructure (see Pix in Brazil or UPAI in India).

Suppose that the regulator wishes to foster interoperability because this option is socially efficient. Then, it chooses the access and the compatibility fee that maximize social welfare, and the maximum level of disclosure for cyber incidents. Since the access fee and the compatibility fee are neutral, the fees chosen by the regulator are indeterminate, provided that banks do not deviate from the equilibrium in which they both join the cloud and become compatible.

The possibility that the regulator chooses the service fees does not change social welfare with respect to the situation of (iii) with mandatory investments (see Appendix 8). Indeed, he needs to choose the access and the compatibility fee, respectively, such that banks join the common infrastructure when it is socially optimal. As in our setting, the service fees have no effect on banks' investment in security when they both join the cloud. Also, if only one bank joins the cloud, the regulator either sets the maximum or a minimum access fee such that only one bank outsources. Anticipating this choice, banks choose symmetric levels of investment in security, and the regulation of fees does not increase banks' investment in security.

In some cases, the regulator may choose the prices of the cloud services at the same time as banks' investments in security. Thus, he sets the maximum compatibility fee such that one bank (say, bank $A$) is indifferent between using the compatibility service and using only the storage service. This subgame admits a Nash Equilibrium, but it implies both positive and negative effects on social welfare that we detail in Appendix 8. On the one hand, this reinforces the incentives of the rival bank $B$ to invest in security. Indeed, this compatibility fee setting suppresses the incentives of bank $A$ to react to investment changes of its competitor, such that the indirect effect disappear in the investment decision of bank $B$. We show that the optimal security investment of bank $B$ doubles with respect to the situation where the regulator sets its compatibility fee after banks' investment. On the other hand, bank $A$ has indeterminate incentives to invest, because the fee exactly compensates for its benefit from compatibility, including its effect on its investment decision. Thus, compatibility may either correct the under-investment problem of bank $A$, or may reinforce it. Consequently, the regulator faces a trade-off between setting a high compatibility fee, which maximizes the incentives of one bank to invest, and setting a low compatibility fee, which preserves both banks' incentives to invest.

# 7 Conclusion

In this paper, we discussed the impact of the liability regime for cyber incidents on banks' decisions to outsource their payment system, and on the expected level of security. We identified the market conditions such that defining a liability regime for the cloud service provider may improve its investment incentives and interoperability. We explained how moral hazard may impact the distortions with respect to the first-best. While moral hazard cannot be completely eliminated, limiting its effect on the players' investment incentives may clarify the role of the liability regime for cyber incidents in banking retail markets. Currently, in most countries, banks may not outsource their responsibilities. However, other policy options may be considered in the future. In this respect, the point of view of the Australian financial regulator (APRA) which is encouraging shared responsibility models before authorizing cloud outsourcing by banks is interesting.

# Appendix

### Appendix 1 - Welfare-maximizing investments in security and outsourcing decisions

**The welfare-maximizing security investments:**

We denote the social welfare by $W^n$ when banks do no outsource, and by $W^c$ when banks outsource and they are compatible. Without cloud outsourcing, since banks have identical costs, the social planner chooses symmetric levels of security investments for both banks, such that their profit at the equilibrium of stage 4 does not depend on the level of security.[44] The social planner maximizes

$$W^n = \beta/2 - t/4 - h_i^n(s_i)l - k_b s_i^2. \tag{21}$$

The social planer chooses a level of security for each firm (bank and cloud service provider) such that the marginal benefits of a higher security for the society are equal to the marginal costs. Thus, the welfare-maximizing level of investment in cyber security $s_w^n$ equals

$$s_w^n = \frac{\sigma l}{2k_b}. \tag{22}$$

Banks' total cost of security investments is equal to $C_b^n = k_b(s_w^n)^2$.

If both banks outsource their payment services to the cloud, the social planner maximizes

$$W^c = \beta - t/4 - h_i^c(s_i, s_c)L(v) - k_b s_i^2 - k_c s_c^2/2. \tag{23}$$

Since the total loss $L$ is increasing with $v$, the social planner prefers that the cloud service provider discloses the maximum amount of information on cyber incidents, that is, $v_c = \underline{v_c}$. Therefore, the welfare-maximizing level of banks' investment in cyber security equals

$$(s_w^c)^b = \theta\underline{\alpha} s_w^n,$$

and the welfare-maximizing level of cloud service provider's investment in cyber security equals

$$(s_w^c)^c = \frac{2k_b}{k_c}(1-\theta)\underline{\alpha} s_w^n.$$

Since a bank and the cloud service provider contribute respectively in share $\theta$ and $1-\theta$ to payment system security, with cloud outsourcing, the total security of the payment system is given by:

$$s_w^c = (\theta^2 + \frac{2k_b}{k_c}(1-\theta)^2)\underline{\alpha} s_w^n. \tag{24}$$

[44] If the social planner chooses symmetric levels of investment in security for both banks, because increasing the level of security for bank $i$ does not increase marginally bank k's profit.

**Comparison of welfare-maximizing security investments:** Using the calculations of $s_w^c$ and $s_w^n$ given in Eq.(24) and Eq.(22), respectively, we have that $s_w^c \geq s_w^n$ if and only if $1 - \theta^2\underline{\alpha} \leq 0$ or $1 - \theta^2\underline{\alpha} > 0$ and

$$k_c \leq k_s \equiv 2k_b \frac{(1-\theta)^2\underline{\alpha}}{1-\theta^2\underline{\alpha}},$$

where $k_s \geq 0$. The condition $1 - \theta^2\underline{\alpha} \leq 0$ is equivalent to $\Delta s_b \leq 0$.

**Comparison of social welfare with and without cloud outsourcing:** Replacing for $s_w^c$ given in Eq.(24) into $W_c$ given in Eq.(23), and for $s_w^n$ given in Eq.(22) into $W_n$ given in Eq.(21), outsourcing increases social welfare if and only if $W_c > W_n$, which happens if and only if $\beta > \max\{0, \beta_w\}$, with

$$\beta_w = 2h(\underline{\alpha} - 1)l - \sigma^2(\frac{(\underline{\alpha}l(1-\theta))^2}{k_c} + \frac{(\theta\underline{\alpha}l)^2 - l^2}{2k_b}). \tag{25}$$

Solving for $k_c$ in Eq.(25), we find that $\beta_w < 0$ if and only if $k_c < k_w$, where

$$k_w \equiv \frac{2k_b\sigma^2(1-\theta)^2\underline{\alpha}^2 l}{4hk_b(\underline{\alpha}-1) - \sigma^2 l(\underline{\alpha}^2\theta^2 - 1)},$$

and $4hk_b(\underline{\alpha} - 1) > \sigma^2 l(\underline{\alpha}^2\theta^2 - 1)$ from Assumptions (A1) and (A2), such that $k_w > 0$. Denoting $C_b^n = (\sigma l)^2/(4k_b)$ and rearranging, we find that

$$k_w = \frac{2k_b(1-\theta)^2\underline{\alpha}^2 C_b^n}{(1-\underline{\alpha}^2\theta^2)C_b^n + (\underline{\alpha}-1)hl}.$$

Factorizing by $k_s = 2k_b(1-\theta)^2\underline{\alpha}/(1-\theta^2\underline{\alpha})$ and assuming that $\theta^2\underline{\alpha} \neq 1$, we obtain the expression of $k_w$ given in Proposition 2, that is,

$$k_w = k_s \frac{(1-\theta^2\underline{\alpha})C_b^n}{(1-\theta^2\underline{\alpha}^2)C_b^n + (\underline{\alpha}-1)hl}.$$

## Appendix 2

**Competition stage when only one bank outsources:** As in the main text, we assume, without loss of generality, that bank $A$ is safer than bank $B$ after stage 2, that is, we have $s_A \geq s_B$.

In the following, we consider the competition stage if only one bank outsources. If bank $i \in \{A, B\}$ does not outsource, no depositor benefits from the compatibility service. As a consequence, the outsourcing bank $-i$ does not pay any compatibility fee $f^c$. At the equilibrium, depositors' expectations are fulfilled, such that the independent bank $i$ faces a total demand $N_i^o$ equal to

$$N_i^o = \frac{1}{2} + \frac{p_{-i}^o - p_i^o - \mu h_i^n L_d(0) + \mu h_{-i}^c L_d(v^*)}{2(t-\beta)},$$

and the cloud bank $-i$ faces a total demand $N^o_{-i}$ equal to

$$N^o_{-i} = \frac{1}{2} + \frac{p^o_i - p^o_{-i} - \mu h^c_{-i} L_d(v^*) + \mu h^n_i L_d(0)}{2(t-\beta)}. \tag{26}$$

At the competition stage, the independent bank $i$ chooses $p^o_i$ to maximize

$$\pi^o_i = (p^o_i - h^n_i L_b(0)) N^o_i - C_b(s_i) \tag{27}$$

while the cloud bank $-i$ chooses $p_{-i}$ to maximize

$$\pi^o_{-i} = (p^o_{-i} - f^a - h^c_{-i} L_b(v^*)) N^o_{-i} - C_b(s_{-i})\ . \tag{28}$$

Solving for the first-order conditions in Eqs.(27) and (28), the prices of deposits of banks $i$ and $-i$ are equal to

$$p^o_i = t - \beta + h^n_i L_b(0) + \frac{f^a}{3} - \frac{h^n_i \rho(0) - h^c_{-i}\rho(v^*)}{3}, \tag{29}$$

and

$$p^o_{-i} = t - \beta + h^c_{-i} L_b(v^*) - \frac{2f^a}{3} - \frac{h^c_{-i}\rho(v^*) - h^n_i \rho(0)}{3},$$

respectively. The profit of the independent bank $i$ at the competition stage equals

$$\pi^o_i(s_i, s_{-i}, s_c, f^a) = \frac{(t - \beta + (f^a + h^c_{-i}\rho(v^*) - h^n_i\rho(0))/3)^2}{2(t-\beta)} - C_b(s_i), \tag{30}$$

and the profit of the cloud bank $-i$ equals

$$\pi^o_{-i}(s_i, s_{-i}, s_c, f^a) = \frac{(t - \beta - (f^a + h^c_{-i}\rho(v^*) - h^n_i\rho(0))/3)^2}{2(t-\beta)} - C_b(s_i). \tag{31}$$

**Fee setting by the CSP:** The cloud service provider sets the fees $f^a$ and $f^c$ to maximize its profit, which equals $\pi^c_C$ given in Eq.(4) if both banks outsource, and $\pi^o_C$ in Eq.(5) if only bank $-i$ outsources. We distinguish these two situations below, before comparing the profit of the cloud service provider in each case.

**Case A: Both banks outsource:** If both banks $A$ and $B$ store their payment services in the cloud, the cloud service provider always prefers to offer the compatibility service because it can be offered at no additional cost. In that case, the cloud service provider sets the fees $f^a$ and $f^c$ to maximize its profit $\pi^c_C$ given in Eq.(4), under the constraint that no bank deviates from the situation where they both use the compatibility service. Because banks pay the same fee to the cloud service provider, and since the deposit market is always covered,

$\pi_C^c$ is linear in $f^c$ and $f^a$. Therefore, the maximization problem of the cloud service provider is equivalent to:

$$\begin{aligned} \max_{f^c,\, f^a} \quad & 2f^c + f^a & & \\ \text{s.t.} \quad & \pi_i^c(f^c, f^a) \geq \pi_i^{st} & \text{for i=\{A,B\}} & \quad \text{(C1a)} \\ & \pi_i^c(f^c, f^a) \geq \pi_i^o(f^a) & \text{for i=\{A,B\}} & \quad \text{(C2a)} \\ & \pi_C^c \geq 0. & & \quad \text{(C3a)} \end{aligned}$$

In the constraints above, $\pi_i^c$ represents the profit of bank $i$ when both banks use the compatibility service, and it is obtained by setting $v = v^*$ and $z = 1$ in $\pi_i$ given in Eq.( 8). The profit $\pi_i^{st}$ is the profit of bank $i$ when both banks only use the storage service and it is obtained by setting $v = v^*$ and $z = 0$ in $\pi_i$ given in Eq.( 8). The profit $\pi_i^o$ given in Eq.(30) is the profit of bank $i$ when it remains independent, while its rival uses the storage service.

The interpretation of this maximization problem is as follows. Given that the compatibility and the storage services are one-way complements, there are two possible deviations from the situation in which both banks use the two services. First, each bank should not deviate by remaining independent, if its rival outsources (constraints C1a). Second, banks should not deviate by not using the compatibility service, if their rival uses it and both banks outsource (constraints C2a). Finally, condition (C3a) states that the cloud service provider makes a positive profit.

Replacing for $\pi_i^c$ and $\pi_i^s$ defined above into (C1a) for both banks $A$ and $B$, we find that the constraints (C1a) are equivalent to $f^c \leq f^{c*}$, where $f^{c*}$ is given in Eq.(9). Since the profit of the cloud service provider $\pi_C^c$ is increasing with $f^c$, the cloud service provider chooses the compatibility fee $f^{c*}$ when both banks outsource.

Replacing for $f^c = f^{c*}$, $\pi_i^c$ and $\pi_i^{st}$ defined above into (C2a), the constraint (C2a) for bank $i$ is equivalent to $(f_i^{a*} - f^a)(f^a + \tau_1) \geq 0$, with $f_i^{a*} = h_i^n\rho(0) - h_i^c\rho(v^*)$ and $\tau_1 \equiv 6(t-\beta) - h_i^c\rho(v^*) + 2h_{-i}^c\rho(v^*) + h_i^n\rho(0)$. From Assumption (A1), we have that $\tau_1 \geq 0$ and $\tau_1 \geq f_i^{a*}$. Therefore, the constraint (C2a) is satisfied for bank $i$ if and only if $f^a \in (-\tau_1, f_i^{a*})$. Since the profit of the cloud service provider is increasing with $f^a$, the latter chooses the maximum access fee such that the constraint (C2a) is satisfied for both banks $A$ and $B$. Therefore, it sets an access fee equal to $min\{f_A^{a*}, f_B^{a*}\}$.

Replacing for $h_i^n = h - \sigma s_i$ and $h_i^c = h - \sigma(\theta s_i + (1-\theta)s_c)$ in $f_A^{a*}$ and $f_B^{a*}$, we find that $f_B^{a*} \geq f_A^{a*}$ is equivalent to

$$\theta\rho(v^*) \geq \rho(0). \tag{33}$$

To conclude for Case A, the cloud service provider chooses an access fee equal to $f_A^{a*}$ if $\rho(v^*) \geq \theta\rho(0)$ and $\pi_C^c(\ f^{c*},\ f_A^{a*}) \geq 0$. It chooses an access fee equal to $f_B^{a*}$ if $\rho(v^*) < \theta\rho(0)$ and $\pi_C^c(\ f^{c*},\ f_B^{a*}) \geq 0$, and it prefers not outsource to both banks otherwise.

**Case B: Bank $i \in \{A, B\}$ does not outsource:** In this case, the cloud service provider does not provide a compatibility service, and it only chooses the access fee $f^a$ to maximize its profit $\pi_C^o$ in Eq.(5), under the constraint that no bank has incentives to deviate from the situation in which only one bank (here, bank $-i$) uses the storage service. The maximization problem of the cloud service provider is equivalent to

$$\begin{aligned} \max_{f^a} \quad & \pi_C^o \\ \text{s.t.} \quad & \pi_{-i}^o(f^a) \geq \pi_{-i}^n && \text{(C1b)} \\ & \pi_i^o(f^a) \geq \pi_i^s && \text{(C2b)} \\ & \pi_C^o \geq 0 && \text{(C3b)} \end{aligned}$$

In the constraints above, $\pi_i^o$ and $\pi_{-i}^o$ represent the profit of banks $i$ and $-i$ when only bank $-i$ uses the storage service of the cloud service provider, and they are given in Eqs.(30)-(31), respectively. The profit $\pi_{-i}^n$ represents the profit of bank $-i$ when no bank outsources, and it is obtained by setting $v = 0$ and $z = 0$ in $\pi_i$ given in Eq.(8). Finally, the profit $\pi_{-i}^s$ represents the profit of bank $-i$ when both banks only use the storage service, and it is obtained by setting $v = v^*$ and $z = 0$ in $\pi_i$ given in Eq.(8).

The interpretation of the constraints is as follows. If bank $i$ does not outsource, bank $-i$ can deviate by refusing to outsource as well, such that both banks are independent (constraint C1b). Second, bank $i$ can deviate by using the storage service too (constraints C2b). Third, the cloud service provider must make a positive profit (constraint C3b).

Following the analysis of the constraint (C2a) in Case A above, where $\pi_i^c(f^c) = \pi_i^s$ from the constraint (C1a), the constraint (C2b) is equivalent to $f^a \leq f_{-i}^{a*}$, with $f_{-i}^{a*} = h_{-i}^n \rho(0) - h_{-i}^c \rho(v^*)$. In addition, the constraint (C1b) is equivalent to $f^a \geq f_i^{a*}$.

We now determine the maximum of $\pi_C^o$ with respect to $f^a$ and show that the constraint (C1a) is binding. Differentiating $\pi_C^o$ wth respect to $f^a$, we find that $\partial \pi_C^o / \partial f^a = (f_m^a - f^a)/(3(t-\beta))$, with

$$f_m^a \equiv \frac{3(t-\beta) + h_{-i}^c(L_c(v^*) - \rho(v^*)) + h_i^n \rho(0)}{2}.$$

Since $\pi_C^o$ is concave in $f^a$, this profit function reaches a maximum at $f^a = f_m^a$. From Assumption (A1), we have $f_m^a - f_{-i}^{a*} \geq 3(t-\beta)/2 - h_{-i}^n \rho(0) \geq 0$. Therefore, the condition (C1b) constrains the maximum fee that may be chosen by the cloud service provider. The constraints (C1b) and (C2b) imply that the cloud service provider sets an access fee equal to $f^{a*} = f_{-i}^{a*}$ if $f_{-i}^{a*} \geq f_i^{a*}$ and if constraint (C3b) holds. Otherwise, it does not outsource only to bank $-i$.

We show that a necessary condition for condition (C3b) to hold is that $f^{a*} = f_i^{a*} > 0$. Since $f_i^{a*}$ is decreasing with $h_i^c$ for bank $i \in \{A, B\}$ and $h_i^c$ is decreasing with the investment of the cloud service provider $s_c$, $f_i^{a*}$ is increasing with $s_c$. Given that $s_c \leq h/\sigma$, we have $f_i^{a*} \leq f_i^{a*}|_{s_c = h/\sigma}$, with $f_i^{a*}|_{s_c = h/\sigma} = (h - \sigma s_i)(\rho(0) - \theta \rho(v^*))$. If $\rho(0) < \theta \rho(v^*)$, the fee $f_i^{a*}|_{s_c = h/\sigma}$ is negative, which implies that $f_i^{a*}$ is negative. Therefore, if $\rho(0) < \theta\rho(v^*)$, the cloud service provider cannot make a positive profit when it serves only bank $-i$.

To conclude, from Eq.(33), if $\rho(0) > \theta\rho(v^*)$ and the constraint (C3b) is satisfied, the cloud service provider sets an access fee equal to $f_B^{a*}$ such that only bank $B$ outsources. Otherwise, it does not provide a storage service to one bank only.

**Comparison of CSP profits of serving either one or two banks:** We are now able to determine the number of banks that the cloud service provider prefers to serve at the equilibrium of stage 3. Assume that $\rho(0) \geq \theta\rho(v^*)$, such that the cloud service provider faces a non-trivial trade-off between serving both banks or bank $B$ only. In that case, the cloud service provider charges an access fee equal to $f_A^{a*}$ when it serves both banks and $f_B^{a*}$ when it serves only bank B.

Suppose that the cloud service provider serves only bank B. We start by determining the demand of bank B at the profit-maximizing fees chosen by the cloud service provider, before determining the cloud service provider's profit. Replacing $p_i$ and $p_{-i}$ given in Eq.(29) into $N_B^o$ gives

$$N_B^o = \frac{(t - \beta - (f_B^{a*} + h_B^c\rho(v^*) - h_A^n\rho(0))/3)}{2(t-\beta)}.$$

Since $f_B^{a*} = h_B^n\rho(0) - h_B^c\rho(v^*)$, we have that $N_B^o = N_B^n$. Therefore, the profit of the cloud service provider if only bank $B$ joins the cloud equals

$$\pi_C^o = \Phi^o N_B^n - C_c(s_c),$$

where $N_B^n = N_B^o$ represents the demand of bank $B$ when both banks are independent, and $\Phi^o = f_B^{a*} - h_B^c L_c(v^*)$ is the margin of the cloud service provider.

Suppose that the cloud service provider serves both banks. Replacing $p_i$ given by Eq.(7) with $z = 1$ and $v = v^*$ into $\pi_C^c$ given in Eq.(4), if banks become compatible, the cloud service provider makes a profit equal to

$$\pi_C^c = 2f^{c*} + (f_A^{a*} - h_B^c L_c(v))N_B^c + (f_A^{a*} - h_A^c L_c(v))N_A^c - C_c(s_c).$$

Since the market is covered, we have $N_B^c = 1 - N_A^c$. This implies that:

$$\pi_C^c = 2f^{c*} + f_A^{a*} - h_B^c L_c(v) + (h_B^c - h_A^c)L_c(v)N_A^c - C_c(s_c),$$

with $f_A^{a*} = h_A^n\rho(0) - h_A^c\rho(v^*)$. Replacing for $\Phi^o = f_B^{a*} - h_B^c L_c(v^*)$ gives:

$$\pi_C^c = 2f^{c*} + f_A^{a*} - f_B^{a*} + \Phi^o + (h_B^c - h_A^c)L_c(v)N_A^c - C_c(s_c).$$

Since $h_B^c - h_A^c = \theta(h_B^n - h_A^n)$, we find that:

$$\pi_C^c = \Phi^c + \Phi^o - C_c(s_c),$$

where

$$\Phi^c \equiv 2f^{c*} + f_A^{a*} - f_B^{a*} + \theta(h_B^n - h_A^n)N_A^c L_c(v^*). \tag{35}$$

Therefore, the profit of the cloud service provider is positive only if $\Phi^o \geq -\Phi^c$. Finally, we define the difference of the cloud service provider's profit if it serves both banks and only bank B as:

$$\Delta\pi_C = \Phi^c + \Phi^o(1 - N_B^n).$$

Since $N_A^n = 1 - N_B^n$, we have $\Delta\pi_C \geq 0$ if and only if $N_A^n\Phi^o \geq -\Phi^c$.

Since $\theta\rho(v^*) \leq \rho(0)$, the sign of $\Phi^c$ is ambiguous. We remark that $\partial\Phi^c/\partial\beta = \partial f_c^*/\partial\beta$, because $\Phi^c$ only depends on $\beta$ through $f_c^*$, and $\partial f_c^*/\partial\beta > 0$ from Assumption (A1). Therefore, $\Phi^c$ is increasing with $\beta$. Since $\Phi^c|_{\beta=0} = \theta N_A^c L_c(v^*) - \rho(0) + \theta\rho(v^*)$, we have that $\Phi^c|_{\beta=0} < 0$ if and only if $\theta < \theta_1$ with $\theta_1 \equiv \rho(0)/(N_A^c L_c(v^*) + \rho(v^*))$. Therefore, $\Phi^c$ given in Eq.(35) is negative if and only if $\theta\rho(v^*) < \rho(0)$, $\beta \leq \beta_1$ and $\theta < \theta_1$, with $\beta_1$ the solution of $\Phi^c(\beta) = 0$ and $\theta_1$ the solution of $\Phi^c|_{\beta=0} = 0$. Otherwise, it is positive.

To conclude, the cloud service provider chooses to outsource only to bank $B$ if $\Phi^c < -N_A^n\Phi^o$, when $\Phi^o > 0$, and it outsources to both banks either if $\Phi^c > -N_A^n\Phi^o$ when $\Phi^o > 0$, or if $\Phi^o + \Phi^c > 0$ when $\Phi^o \leq 0$. Finally, the cloud service provider remains inactive if $\Phi^o < \min\{0, -\Phi^c\}$.

Suppose that banks choose the same level of security at stage 2. Therefore, $\Phi^c$ given in Eq.(35) equals $2f^{c*}$ , such that $\Phi^c > 0$. This contradicts the first condition (i.e., $\Phi^c < -N_A^n\Phi^o$). Therefore, no bank joins the cloud alone when banks invest the same amount of security at stage 2.

**Appendix 3: Effect of cloud outsourcing on depositor surplus:**

We assume that banks choose symmetric prices (see Appendix 4 for the proof). Therefore, banks share the deposit market equally, and the outsourcing has no effect on depositors' transportation costs. Also, this implies that the access fee $f_i^{a*}$ given in Eq.(10) is equal to $f_{-i}^{a*}$.

Given that only a proportion $\mu$ of depositors are sophisticated, the average expected utility of a depositor $E(U_i(z))$ equals $u_i(x) - \mu h_i L_d(zv^*)$, with $u_i(x)$ given in Eq.(1), and $z = 1$ (resp., $z = 0$) if banks outsource (do not outsource). Replacing for $p_i^*$ given in Eq.(7), the average expected utility of a depositor (net of transportation costs) equals

$$E(U_i(0)) = -t + \frac{3\beta}{2} - h_i^n(s_b^n)\rho(0)$$

if both banks do not outsource their payment services, and

$$E(U_i(1)) = -t + \beta - h_i^c(s_b^c)\rho(v^*) - f_i^{a*}$$

if both banks outsource their payment services, with $f_i^{a*} = h_i^n(s_b^c)\rho(0) - h_i^c(s_b^c)\rho(v^*)$ given in Eq.(10). Therefore, the effect of outsourcing on depositor surplus equals

$$E(U_i(1)) - E(U_i(0)) = \frac{-\beta}{2} + \rho(0)(h_i^n(s_b^n) - h_i^n(s_b^c)).$$

Replacing for $h_i^n(s_b) = h - \sigma s_b$, depositor surplus is higher when banks outsource (i.e., if $z = 1$) if and only if $\beta/2 \leq \sigma\rho(0)(s_b^c - s_b^n)$, and it is lower otherwise.

## Appendix 4 - The equilibrium at stage 2

**The first-order conditions:** For $i \in \{A, B\}$, we denote by $\tilde{p}_i^*$ and by $\tilde{\pi}_i^*(s_i, s_{-i})$ banks' prices and profits, at the equilibrium of stage 3, respectively. From the envelop theorem, solving for the first-order condition of each bank's profit maximization gives

$$\frac{\partial \tilde{\pi}_i^*}{\partial s_i} = \frac{\partial \pi_i}{\partial s_i} + \frac{\partial \pi_i}{\partial p_{-i}}\frac{\partial \tilde{p}_{-i}^*}{\partial s_i} + \frac{\partial \pi_i}{\partial f_a}\frac{\partial f^{a*}}{\partial s_i} + \frac{\partial \pi_i}{\partial f_c}\frac{\partial f^{c*}}{\partial s_i} = 0. \tag{36}$$

In the equation above, if both banks do not join the cloud, the fees chosen by the cloud service provider have no impact on the bank's profit.

Replacing for each term in Eq.(36), we find that

$$\frac{d\tilde{\pi}_i^*}{ds_i} = \sigma\theta((1 - \frac{\Delta h}{3(t-(1-z)\beta)})\frac{\rho(zv^*)}{3} + z\frac{\beta \Delta h^c}{t(t-\beta)}) - k_b s_i, \tag{37}$$

where $z = 1$ and $\Delta h = \Delta h^c$ if bank $i$ joins the cloud, and $z = 0$, $\theta = 1$, $\Delta h = \Delta h^n$, otherwise. The first-order condition gives the profit-maximizing investments in security.

We show that the subgame in which banks choose their security investments admits a unique Nash equilibrium which is symmetric. For this purpose, we analyze the best response of bank $i$ given in Eq.(37), to $s_{-i}$ the security investment chosen by bank $-i$.

**Case A. Interior solution for bank $-i$ ($s_{-i} \in (0, h/\sigma)$).** If there exists a Nash equilibrium such that both banks choose interior solutions for security investments, banks' best responses are given by the first-order conditions in Eq.(37). Since banks' costs functions are identical, banks' best responses are symmetric and given by

$$\left.\frac{d\pi_i}{ds_i}\right|_{s_i = s_i^*} = 0.$$

This solution $s_i^*$ is interior if and only if $h_i(s_i^*) \in (0, h)$. Since $s_c \leq h/\sigma$, this is equivalent to $s_i^* \in (0, h/\sigma)$.

If banks expect to outsource (i.e., $z = 1$), we have $s_i^* = s_i^{c*}$, with $s_i^{c*} = \sigma\theta\rho(v^*)/3k_b$ from Eq.(13). We have $s_i^* > 0$. Also, given that $\theta \in (0, 1)$ and $h > \sigma$ from Assumption (A2), we have $(\sigma/h)s_i^* < (\sigma/h)h\rho(v^*)/3k_b$, which is always lower than 1 from Assumptions (A1) and (A2). Therefore, we conclude that $s_i^* < h/\sigma$.

If banks expect to remain independent (i.e., $z = 0$), we can prove similarly that $s_i^{n*} \in (0, h/\sigma)$, with $s_i^{n*}$ given in Eq.(12). Therefore, the symmetric solution given in Eqs.(12)-(13) constitutes a Nash equilibrium.

**Case B. Minimum investment of bank $-i$.** Suppose that bank $-i$ chooses not to invest in cyber-security (i.e., it chooses $s_{-i} = 0$). Replacing for $h_i(s_i, s_c) = h_i^c(s_i, s_c)$ and $h_{-i}(s_{-i}, s_c) = h_{-i}^c(0, s_c)$ in Eq.(37) if banks expect to outsource (or for $h_i(s_i, s_c) = h_i^n(s_i)$ and $h_{-i}(s_{-i}, s_c) = h_{-i}^n(0)$ if banks expect to be independent), the optimal investment of bank $i$, denoted by $s_i^m$ in this case, is given by

$$s_i^m = \frac{\sigma\theta\rho(zv^*)(3t - 3(1-z)\beta)}{9k(t-(1-z)\beta) - (\sigma\theta\rho(zv^*))^2},$$

with $z = 1$ if banks expect to outsource, and $z = 0$ and $\theta = 1$ if banks expect to be independent. From Assumptions (A1) and (A2), we have $s_i^m \in (0, h/\sigma)$. Therefore, from Case A, the best response of bank $-i$ consists in choosing an interior solution for its security investment. Since $d\pi_{-i}/ds_{-i}|_{(s_i=s_i^m, s_{-i}=0)} > 0$, bank $-i$ has an incentive to deviate from the strategy $s_{-i} = 0$, and the pair of strategies $(s_i = s_i^m, s_{-i} = 0)$ does not constitute a Nash equilibrium. By symmetry, the pair of strategies $(s_i = 0, s_{-i} = s_i^m)$ does not constitute a Nash equilibrium neither.

**Case C. Maximum investment of bank $-i$.** Suppose that bank $-i$ chooses a maximum level of investment in cyber-security (i.e., $s_{-i} = h/\sigma$). Replacing for $h_i(s_i, s_c) = h_i^c(s_i, s_c)$ and $h_{-i}(s_{-i}, s_c) = h_{-i}^c(h/\sigma, s_c)$ in Eq.(37) if banks expect to outsource (or for $h_i(s_i, s_c) = h_i^n(s_i)$ and $h_{-i}(s_{-i}, s_c) = h_{-i}^n(h/\sigma)$ if banks except to be independent), the optimal investment of bank $i$, denoted $s_i^M$ in this case, is given by

$$s_i^M = \frac{\sigma\theta\rho(zv^*)(3t - 3(1-z)\beta - \theta h\rho(zv^*))}{9k(t-(1-z)\beta) - (\sigma\theta\rho(zv^*))^2} \ ,$$

with $z = 1$ if banks expect to outsource, and $z = 0$ and $\theta = 1$ if banks expect to be independent. From Assumptions (A1) and (A2), we have $s_i^M \in (0, h/\sigma)$. Therefore, from Case A, the best response of bank $-i$ consists in choosing an interior solution for its security investment. Since $d\pi_{-i}/ds_{-i}|_{(s_i=s_i^M, s_{-i}=h/\sigma)} < 0$, bank $-i$ has an incentive to deviate from the strategy $s_{-i} = h/\sigma$, and the pair of strategies $(s_i = s_i^M, s_{-i} = h/\sigma)$ does not constitute a Nash equilibrium. By symmetry, the pair of strategies $(s_i = h/\sigma, s_{-i} = s_i^M)$ does not constitute a Nash equilibrium neither.

To conclude, the only Nash equilibrium at stage 2 is that banks choose symmetric levels of security investments, which are defined by $s_i^{c*}$ in Eq.(12) if they join the cloud, and $s_i^{n*}$ given in Eq.(12) if they remain independent.

### Appendix 5 - Comparison of the private and the public outsourcing decisions:

**Condition such that $\widehat{\beta} \leq 0$ banks always join the cloud:** Replacing for $s_i$ in $\widehat{\beta}$ given in Eq.(15), solving for $\widehat{k}_c$ the solution of $\widehat{\beta}(k_c) = 0$ gives:

$$\frac{\widehat{k}_c}{k_w} \equiv \frac{\overline{\rho}(v^*)^2}{(\underline{\alpha} l)^2} \frac{(\underline{\alpha} - 1)l}{\overline{\rho}(v^*) - \rho(0)} \frac{hk_b - \sigma^2 l \widehat{r}_{k1}/4}{hk_b - \sigma^2\theta\rho(v^*)\widehat{r}_{k2}/3}, \tag{38}$$

where $k_w$ is given in Proposition 2 assumed different from 0, $\widehat{r}_{k1} = ((\theta\underline{\alpha}l)^2 - 1)/(\underline{\alpha} - 1)$ and $\widehat{r}_{k2} = (\theta\overline{\rho}(v^*) - \rho(0))/(\overline{\rho}(v^*) - \rho(0))$.

From Eq.(38), private outsourcing occurs for inefficiently high security costs, with respect to first-best level $k_w$, if and only if $\widehat{k}_c > k_w$, which happens if and only if the product of the three ratios in the right-hand side of Eq.(38) are higher than 1. Below, we explain why each ratio may be higher than one.

- i) The first ratio is higher than one if the cloud service provider internalizes more damage than in the first-best because of moral hazard. Indeed, if this is the case, the benefit of security investment by the cloud service provider is more sensitive to its security cost, and $\frac{\widehat{k}_c}{k_w}$ increases.

- ii) The second ratio is higher than one if the change in the damage internalized by firms is lower than in the first-best. In this case, the cloud service provider earns a positive profit for higher levels of security costs than in the first-best.

- iii) The third ratio is higher than one because for a given level of damage, the cloud service provider faces different objectives with respect to the first-best. As we detail in the main text, the remaining differences stem from the vertical relationships, as the banks fail to internalize the effect of their security decisions on other players (the rival bank, the cloud service provider, and myopic depositors), and the cloud service provider do not internalize the effect of its decision to provide its services on the equilibrium security investment of banks.

  If the cloud service provider contributes to all security investments when banks outsource ($\theta = 0$), then the third ratio is equal to $1 + \sigma^2 l/(4hk_b(\underline{\alpha} - 1))$, which is higher than 1, because the cloud service provider underestimates the ability of independent banks to invest in protection at the equilibrium.

**Comparison of first-best and second-best outsourcing decision:** Recall that the total social damage is given by $L(v) = \alpha(v)l + zK(v)$, with $K(\underline{v_c}) = 0$. Replacing for $s_c^*$ given in Eq.(14) and for $s_b^{c*}$ given in Eq.(13) into Eq.(15), we find that

$$\widehat{\beta} = h(\overline{\rho}(v^*) - \rho(0)) - \sigma^2(\frac{(1-\theta)^2\overline{\rho}(v^*)^2}{2k_c} + \theta\rho(v^*)\frac{\theta\overline{\rho}(v^*) - \rho(0)}{3k_b}).$$

Therefore, replacing for $\beta^w$ given in Eq.(25), we find that

$$\begin{aligned}\beta^w - \widehat{\beta} &= h(2(\underline{\alpha} - 1)l - \overline{\rho}(v^*) + \rho(0)) - \sigma^2\frac{(1-\theta)^2}{2k_c}(2(\underline{\alpha}l)^2 - \overline{\rho}(v^*)^2) \\ &\quad -\frac{\sigma^2}{k_b}(\frac{\theta^2(\underline{\alpha}l)^2 - l^2}{2} - \frac{\theta\rho(v^*)(\theta\overline{\rho}(v^*) - \rho(0))}{3}).\end{aligned}$$

## Appendix 6 - Effect of the liability of the cloud service provider on investments in cyber security:

**Effect on banks' investments:** For $\gamma \in \{\gamma_b, \gamma_d\}$, the derivative of $s_b^{c*}$ in Eq.(13) with respect to $\gamma$ is given by

$$\frac{ds_b^{c*}}{d\gamma} = \frac{\sigma\theta}{3k_b}(\frac{\partial\rho(v^*)}{\partial\gamma} + \frac{\partial\rho(v)}{\partial v}\frac{\partial v^*}{\partial\gamma}\bigg|_{v=v^*}).$$

Replacing for $\epsilon_\rho^v(v^*) = (\partial\rho(v)/\rho(v))/(\partial v/v)|_{v=v^*}$ the elasticity of $\rho(v)$ with respect to $v$ evaluated at $v = v^*$, this expression is equivalent to

$$\frac{ds_b^{c*}}{d\gamma} = \frac{\sigma\theta}{3k_b}(\frac{\partial\rho(v^*)}{\partial\gamma} + \epsilon_\rho^v(v^*)\frac{\partial v^*}{\partial\gamma}\frac{\rho(v^*)}{v^*}).$$

From Eq.(18), $\partial\rho(v^*)/\partial\gamma_b = -q(v^*)$, and $\partial\rho(v^*)/\partial\gamma_d = -\mu q(v^*)$. Also, applying the implicit function theorem on Eq.(17), we have $\partial v^*/\partial\gamma > 0$ from Assumption (A2).

To conclude, we have $ds_b^{c*}/d\gamma_b < 0$ if $q(v^*) > \epsilon_\rho^v(v^*)(\partial v^*/\partial\gamma)\rho(v^*)/v^*$, and $ds_b^{c*}/d\gamma_b \geq 0$ otherwise. Similarly, $ds_b^{c*}/d\gamma_d < 0$ if $\mu q(v^*) > \epsilon_\rho^v(v^*)(\partial v^*/\partial\gamma)\rho(v^*)/v^*$, and $ds_b^{c*}/d\gamma_d \geq 0$ otherwise.

**Effect on the cloud service provider' investments:** For this purpose, using $l = l_b + l_d$, we rearrange $\rho(v^*) = \alpha(v^*)l - (1-\mu)L_d(v^*) - L_c(v^*)$ in Eq.(14), such that

$$s_c^*(v^*) = \sigma(1-\theta)\frac{\alpha(v^*)l - (1-\mu)L_d(v^*) + K(v^*)}{k_c}, \tag{39}$$

where $\alpha(v^*)l$ represents the total damage in the economy when banks join the cloud.

For $\gamma \in \{\gamma_b, \gamma_d\}$, the derivative of $s_c^*$ in Eq.(39) with respect to $\gamma$ is such that

$$\frac{ds_c^*}{d\gamma} = \frac{\sigma(1-\theta)}{k_c}(\frac{\partial\rho(v^*)}{\partial\gamma} + \frac{\partial L_c(v^*)}{\partial\gamma} + \frac{\partial\rho(v)}{\partial v}\frac{\partial v^*}{\partial\gamma}\bigg|_{v=v^*} + \frac{\partial L_c(v)}{\partial v}\frac{\partial v^*}{\partial\gamma}\bigg|_{v=v^*}).$$

We have $\partial\rho(v^*)/\partial\gamma_b = -q(v^*)$, and $\partial\rho(v^*)/\partial\gamma_d = -\mu q(v^*)$. Also, from Eq.(16), $\partial L_c(v)/\partial\gamma_b = q(v^*)$ and $\partial L_c(v)/\partial\gamma_d = q(v^*)$. From Eq.(17), at $v = v^*$, we have $\partial L_c(v)/\partial v = 0$. Finally, applying the implicit function theorem on Eq.(17), we have $\partial v^*/\partial\gamma > 0$ from Assumption (A2).

Using the definition of $\epsilon_\rho^v(v^*)$ given above, we have $ds_c^*/d\gamma_b > 0$ if $\epsilon_\rho^v(v^*) > 0$, and $ds_c^*/d\gamma_b \leq 0$ otherwise. Similarly, $ds_c^*/d\gamma_d > 0$ if $(1-\mu)q(v^*) > \epsilon_\rho^v(v^*)(\partial v^*/\partial\gamma)\rho(v^*)/v^*$, and $ds_c^*/d\gamma_d \leq 0$ otherwise.

## Appendix 7 - Comparison of outsourcing decision when the government does not decide on security investments :

Replacing for $s_c^*$ given in Eq.(14) and for $s_b^{c*}$ given in Eq.(13) into $W_c$ given in Eq.(23), and for $s_b^{n*}$ given in Eq.(12) into $W_n$ given in Eq.(21), the cloud service provider makes a positive profit when both banks join the cloud if and only if $\beta > \max\{0, \overline{\beta}_w\}$, with

$$\overline{\beta}_w \equiv 2h(\alpha(v^*) - 1)l - \sigma^2 \frac{(1-\theta)^2 \overline{\rho}(v^*)}{k_c}(2\alpha(v^*)l - \overline{\rho}(v^*))$$
$$-2\sigma^2(\frac{\theta^2\alpha(v^*)\rho(v^*) - \rho(0)}{3k_b}l + \frac{(\rho(0))^2 - (\theta\rho(v^*))^2}{3k_b}).$$

Replacing for $\widehat{\beta}$ given in Eq.(15) gives:

$$\begin{aligned}\overline{\beta}_w - \widehat{\beta} \quad = \quad & h(2(\underline{\alpha} - 1)l - \overline{\rho}(v^*) + \rho(0)) - \sigma^2 \frac{(1-\theta)^2 \overline{\rho}(v^*)}{2k_c}(4\underline{\alpha}l - 3\overline{\rho}(v^*)) \\ & -\sigma^2(\frac{\theta^2\rho(v^*)(6\alpha(v^*)l - 2\rho(v^*) - 3\overline{\rho}(v^*))}{9k_b} - \frac{\rho(0)(6l - 3\theta\rho(v^*) - 2\rho(0))}{9k_b}).\end{aligned}$$

## Appendix 8 - Public cloud infrastructure

**With the same timing as in our setting:** In this Appendix, we denote by $\underline{v} = (1-\theta)\underline{v_c}$ the amount of information hidden by the public cloud service provider. We first show that in our setting, if the regulator is able to set access and compatibility fees, banks' investments do not change. At stage 3, if both banks outsource and they are compatible, social welfare is independent from the access fee. In addition, the setting of the compatibility fee by the regulator is also indeterminate. Therefore, the regulator may set any compatibility fee $f^c \in (0, f^{c*})$, with $f^{c*}$ in Eq.(9) the maximum compatibility fee set by the private cloud service provider, and any access fee $f^a \in (0, \min\{f_A^{a*}, f_B^{a*}\})$, with $f_A^{a*} = h_A^n\rho(0) - h_A^c\rho(v^*)$.

Following Appendix 2 - Case B, assume now that only bank $-i$ outsources. The regulator discloses all information in case of incident, such that the damage in case of attack on bank $-i$ equals $\underline{\alpha}l$. Thus, the regulator maximizes

$$W^o = \beta(N_i^o)^2 + \beta(N_{-i}^o)^2 - \int_0^{N_i^o} tx \; dx - \int_{N_{-i}^o}^1 t(1-x) \; dx - h_i^n N_i^o l - h_{-i}^c N_{-i}^o \underline{\alpha} l \; ,$$

with $N_i^o$ and $N_{-i}^o$ given in Eq.(26) the respective demands of bank $i$ and bank $-i$ when only bank $-i$ outsources.

Differentiating $W^o$ with respect to $f^a$, we find that $W^o$ is increasing with $f^a$ if and only if $f^a < f_1^a$, with

$$f_1^a \equiv h_i^n\rho(0) - h_{-i}^c\rho(\underline{v}) - 3(t-\beta)\frac{t + l(h_i^n - h_{-i}^c\underline{\alpha})}{t - 2\beta}$$

if $t \neq 2\beta$, and $\delta(W^o)/\delta f = -(1/3 - l(h_{-i}^c\underline{\alpha} - h_i^n)/6\beta$ otherwise.

Following Appendix 2 - Case B, the regulator is not constrained by banks' incentives if and only if $f_1^a \in (f_i^a, f_{-i}^a)$, with $f_i^{a*} = h_i^n\rho(0) - h_i^c\rho(v^*)$. Denoting $H = -\,3(t + l(t-\beta)(h_i^n - h_{-i}^c\underline{\alpha})/(t-2\beta)$, we have $f_i^a - f_1^a = -\,H + \rho(\underline{v})(h_i^c - h_{-i}^c)$ and $f_i^a - f_1^a = -\,H + \rho(0)(h_i^n - h_{-i}^n)$. Given that $h_i^c - h_{-i}^c$ and $h_i^n - h_{-i}^n$ are of the same sign, the regulator is always constrained by the necessity to provide one bank with the incentive to outsource.

Therefore, if $f_{-i}^{a*} \geq f_i^{a*}$ and $\partial W^o/\partial f^a > 0$, the regulator is constrained by condition (C1b) in Appendix 2, and it sets an access fee equal to $f_{-i}^{a*}$. If $f_{-i}^{a*} \geq f_i^{a*}$ and $\partial W^o/\partial f^a < 0$, the regulator is constrained by condition (C2b) in Appendix 2, and it sets an access fee equal to $f_i^{a*}$. Finally, if $f_{-i}^{a*} < f_i^{a*}$, the regulator cannot outsource to bank $-i$ only. In both cases where the regulator can outsource to bank $-i$ only, banks' profit are symmetric (see conditions (C1b)-(C2b)). From Appendix 3, banks set symmetric security investment in these cases, such that $f_{-i}^{a*} = f_i^{a*}$ at the equilibrium of the game, and the regulator never outsources to one bank only.

**With a different timing (Fees and banks' investments in security chosen at stage 2):** We assume in this section that the regulator only provides a public infrastructure if it delivers a compatibility service. We first detail banks' investments at Stage 2, before considering the regulator's choice of fees.

At Stage 2, the security investment of banks remain equal to our main setting if banks do not outsource, i.e., it equals $s_b^{n*} = \sigma\rho(0)/3k_b$ given in Eq.(12). Also, if banks outsource, but do not use the compatibility service, the profit of bank $i$ equals $\pi_{-i}^{st}$, which is obtained by setting $v = \underline{v}$ and $z = 0$ in $\pi_i$ given in Eq.(8), such that it is independent from any access fee, and it equals $s_b^{st*} = \sigma\theta\rho(\underline{v})/3k_b$, which is $s_b^{c*}$ in Eq.(13), with $v^* = \underline{v}$.

The security investment of banks may depend on the fees set by the regulator in two cases. Let $s_i^{sc*}$ and $s_{-i}^{sc*}$ the investment decided by banks $i$ and $-i$, respectively, when both banks outsource and they use the compatibility service, with $s_{-i}^{sc*} \leq s_i^{sc*}$. Also, let $s_i^{o*}$ and $s_{-i}^{o*}$ banks' investments when only one bank $-i$ uses the storage service.

At stage 2, the regulator sets the compatibility and access fees, with banks' security investments given above. Replacing for symmetric $s_i = s_b^{st*}$ and $s_{-i} = s_b^{st*}$ in $\pi_{-i}^{st}$ and solving the constraint (C1a) in Appendix 2 with respect to $f^c$, we find that the maximum compatibility fee such that bank $i$ uses the compatibility service is such that $\pi_i^c(f_i^c, s_i^{sc*}, s_{-i}^{sc*}) = \pi_i^{st}(s_b^{st*})$, and it equals

$$f_i^c = \frac{\beta}{2} + \frac{((\Delta h^{sc})\rho(\underline{v}))^2}{18t}) - \frac{(\Delta h^{sc})\rho(\underline{v})}{3} + C_b(s_b^{st*}) - C_b(s_i^{sc*}),$$

with $\Delta h^{sc} = h^c(s_i^{sc*}, s_c) - h^c(s_{-i}^{sc*}, s_c)$. We have $f_i^c \leq f_{-i}^c$ if and only if

$$(s_i^{sc*} - s_{-i}^{sc*})(3k_b(s_i^{sc*} + s_{-i}^{sc*}) - 4\sigma\theta\rho(\underline{v})) \geq 0,$$

and $f_i^c > f_{-i}^c$ otherwise.

Replacing for $f^c = f_i^c$ in $\pi_i^c(f_i^c, s_i^{sc*}, s_{-i}^{sc*})$, and using $\pi_i^o(s_i^{o*}, s_{-i}^{o*})$ defined in Appendix 2 with $s_i = s_i^{o*}$ and $s_{-i} = s_{-i}^{o*}$, the constraint (C2a) for bank $i$ is equivalent to $f_i^a \in (\underline{f_i^a}, \overline{f_i^a})$, with

$$\underline{f_i^a} = h_i^o\rho(0) - h_{-i}^o\rho(\underline{v}) - 3(t-\beta)(1 - \sqrt{1 + k(s_i^{o*} - s_b^{st*})(s_i^{o*} + s_b^{st*})/(t-\beta)}).$$

If both banks outsource and use the compatibility service, at the Nash equilibrium, bank $i$ maximizes $\pi_i^c(f_i^c, s_i^{sc*}, s_{-i}^{sc*})$ with respect to $s_i^{sc*}$. By definition of $f_i^c$, $\pi_i^c = \pi_i^{st}(s_b^{st*})$ such that the security investment of bank $i$ is indeterminate. Replacing for $f^c = f_i^c$ in $\pi_{-i}^c(f_i^c, s_i^{sc*}, s_{-i}^{sc*})$, the profit of bank $-i$ equals

$$\pi_{-i}^c = \frac{t-\beta}{2} + \frac{2\Delta h^{sc}}{3}\rho(\underline{v}) + C_b(s_b^{st*}) - C_b(s_i^{sc*}) - C_b(s_{-i}^{sc}),$$

such that

$$s_{-i}^{sc*} = \sigma\theta\frac{2\rho(\underline{v})}{3k_b}.$$

Replacing for $s_{-i}^{sc*}$ given above, the equilibrium condition such that the regulator indeed sets $f_i^c$ (i.e., $f_i^c \leq f_{-i}^c$) can be rewritten as $(3k_b s_i^{sc*} - 2\sigma\theta\rho(\underline{v}))^2 \geq 0$, which is true for all $s_i^{sc*}$. Therefore, the situation where both banks outsource and use the compatibility service constitutes a subgame Nash equilibrium.