Cyber Security and Cloud Outsourcing of Payments*

Ciet Noé, Verdier Marianne

First version: December 2022 - This version: January 2024

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 stores depositors' information in the cloud and offers compatibility services, but is exposed to cyber risk. Without cyber risk, banks outsource excessively to the TPP compared to the first-best because network effects soften competition for deposits. We show that cyber risk and security costs may sometimes reduce banks' incentives to build interoperable payment systems. We discuss several policy options to improve payment system security and interoperability: security standards, the authorization of cloud outsourcing agreements, a common liability regime, a shared-responsibility model, a common public infrastructure.

Keywords: payment systems, banks, cyber risk, cloud outsourcing, compatibility, interoperability.

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

*We thank Marie-Laure Allain, Vincent Bignon, Doh-Shin Jeon, Jerome Mathis, Antonio Russo, Tong Wang, participants to the 14th Digital Economics Paris Conference (March, 2023), BECCLE conference (June, 2023), EARIE conference (August 2023), EEA conference (August 2023), the workhop Monnaie, Banque et Droit (December 2023).

1 Introduction

The recent development of digital innovations and big data in payments has strengthened the role of cloud-based third-party providers in the banking sector.[1] Banks use cloud computing to increase the scale and flexibility of their computing capacity (Financial Stability Board, 2019).[2] Several regulators are concerned that the outsourcing of some critical elements of payment systems to third-party providers could pose risks for the security of retail banking activities and financial stability.[3] Depositors may not internalize cyber risk when they open a bank account, which justifies the need for consumer protection.

In this paper, we analyze banks' decision to outsource their payment services to a cloud-based interoperable platform and their impact on payment system security. We show that without cyber risk, banks outsource excessively their payment systems compared to the first-best because of network effects. However, with cyber risk, banks may sometimes choose not to outsource enough when depositors benefit from interoperability. If cloud outsourcing reduces the expected losses caused by cyber incidents, depositor myopia may reinforce the under-outsourcing. This result provides a rationale for building in some cases a public common infrastructure for retail payment systems, such as the Pix initiative in Brazil.

Our paper contributes to the debate on public intervention in payment systems to reach interoperability. The main question is whether the government should build a common infrastructure, or leave this decision to the private sector.[4] This debate is reminiscent of the discussions on infrastructure sharing in other network industries, though with the different issue of risk contagion (Vogelsang, 2021). We offer a framework to compare several policies in terms of cybersecurity and efficiency: the ex-ante supervision of

[1] See International Data Corporation (2018). In 2020, major partnerships of banks with cloud companies include Deutsche Bank with Google Cloud, Standard Chartered with Microsoft, and Bank of America with IBM. See also Kashyap and Wetherilt (2019).

[2] Cloud services models can be deployed by a private cloud that is only accessible by one firm, or by a public cloud, accessible on the Internet, or by a combination of the two.

[3] See the DORA regulation by the European Commission (2022), which regulates Critical Third-Party Providers, including cloud service providers.

[4] See D'Sliva et al., 2019 for a discussion of this issue. Examples of government operated interoperable payment platforms include Pix in Brazil or UPI in India.

cloud outsourcing agreements, the ex-post allocation of the losses with a common liability system or a shared responsibility regime, and the building of a public infrastructure. We show that an appropriate choice of a strict liability system may implement the first-best levels of security, but this requires subsidizing the cloud service provider.

On the positive side, 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 standardized services without incurring the costs of investing in computing capacity. For example, Volante Technologies offers a cloud-based platform that enables banks to achieve technical interoperability.[5]

On the negative side, several central banks have warned that the outsourcing of banking services to common third-party providers could increase cyber risks in the financial sector (See Bank of Canada, 2019, and the Reserve Bank of New Zealand, 2020, Federal Reserve System, 2021). Their concern seems justified by several recent incidents. For example, in 2021, a five-hour outage of Amazon Web Service (AWS) impacted consumer access to banks' call centers and websites. In addition, the migration of sensitive data outside banks' IT systems increases the risks of data breaches.[6] In response, cloud service providers argue that their technology improves the security of retail payment systems.[7]

To shed light on this debate, we build a model to analyze banks' incentives to join a common payment infrastructure managed by a cloud service provider in the presence of cyber risk. The latter offers 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 their consumers payment services. They incur the same investment costs. If the banks' depositors are equipped with the same payment app, they are able to send payments to one another. Some depositors are naive,

[5]Volante Technologies offers a payments as a service cloud based platform to over a hundred financial institutions. Other examples include Modo in the United States.

[6]In 2019, 106 million credit card applications of Capital One Financial have been stolen from the AWS. Ongoing civil lawsuit suggest that Capital One failed to implement security procedures available on its cloud platform (Covert, 2021).

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

while other are sophisticated and choose their bank according to the level of risk of its payment system. Banks decide whether or not to join the cloud service provider 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 depends on the cloud service provider's investment. Banks lose the benefits of security differentiation, which they obtain if they compete with independent payment solutions. Moreover, they may incur the cost of additional damage.

We start by determining the welfare-maximizing level of security and outsourcing decisions. Cloud outsourcing benefits the society if and only if the marginal social benefits of interoperability are higher than the potential marginal social costs in terms of risk. We show that the welfare-maximizing level of security of the payment system is higher if both banks join the cloud if there are sufficient efficiency gains associated with cloud outsourcing.

Subsequently, we analyze the game in which banks privately decide whether or not to join the cloud after investing in payment system security. We start by considering that investments in security are exogenous. The cloud service provider commits to offer a given level of security and chooses the access and compatibility fees that banks pay if they connect to its infrastructure. The cloud service provider internalizes banks' incentives to remain independent when it chooses the access fee. We show that in equilibrium, both banks outsource their payment services if and only if the benefits of network effects are higher than the variation of the costs of cyber incidents.

We identify the market conditions such that banks under-outsource their payment services with respect to the first-best (resp., over-outsource). Because of network effects, banks tend to choose excessive levels of interoperability to soften price competition for deposits, as in Foros and Hansen (2001). However, we show that cyber risk may sometimes imply that banks sometimes do not outsource enough their payment systems. First, the cloud service provider chooses the access fee without perfectly internalizing banks' costs of security and the variation of risk implied by the outsourcing. Second, it also imperfectly internalizes the variation of the social loss caused by the outsourcing when some depositors are naive. With endogenous investments, there are additional distortions. Banks under-invest in payment system se-

curity to soften security competition for depositors. Moreover, they do not internalize the positive externality that their investments confer on the cloud service provider. In addition, banks bear an inefficiently low share of total payment system security.

We proceed by analyzing the possible remedies. If security audits are not very costly, the regulator may implement the first-best levels of investment with security standards. A combination of security standards and the regulatory power to refuse cloud outsourcing agreements may implement the first-best equilibrium when there is over-outsourcing. However, this solution is not possible for outcomes with under-outsourcing. If security audits are very costly, the regulator may try and design a strict common liability regime for cyber incidents. We show that it is possible to implement the first-best levels of security with such a system. The drawback is that this requires subsidizing the cloud service provider. We compare this solution with a shared responsibility model, which defines contingent transfers, when it is possible to identify the location of the cyber incident. We then analyze the outcomes of the regulation with the building of a public cloud infrastructure. Lastly, we argue that it is essential to complete the regulation with measures to improve the disclosure of cyber incidents and depositor education.

The paper is organized as follows. Section 2 surveys the literature that is related to our work. Section 3 presents the model and the assumptions. Section 4 analyzes the first-best security investment levels and outsourcing choices. Section 5 compares this benchmark to the banks' decisions. Section 6 studies various remedies to the distortions identified in section 5. Section 7 concludes. All proofs are available in the appendix.

2 Related Literature

Our paper is connected to the research on investment in cybersecurity, and more specifically cyber risk in payment systems, the literature studying product liability and product compatibility, respectively, and the literature on the optimal market structure in network industries.

We contribute to the literature on investment in cyber security (see Gordon and Loeb, 2002, August and Tunca, 2006, and Anderson et al., 2009 for a survey). As in this literature, we analyze the relationship between

the liability regime and cyber security (Lam, 2016, De Corniere and Taylor, 2021, Lam and Seifert, 2023). We also assume that some consumers are naive (Lam, 2016, De Corniere and Taylor, 2021, Lam and Seifert, 2023) and that some valuable services for consumers may increase cyber risk (Lam and Seifert, 2023, Jullien et al., 2020). In a close paper, Lam and Seifert (2023) analyze how a firm's decision to share consumer data to a third-party impacts cyber security investments. Unlike our paper, this literature does not consider the relationship between the outsourcing decisions of competing firms and investments in cyber security. Our work is also related to a strand of the literature on the economics of security which studies firms' incentives to outsource their security services to a Managed Security Service Provider (see Ding et al., 2005, 2006, Gupta and Zdanov, 2012, Cezar et al., 2017). As in our paper, Cezar et al. (2017) consider that competitive externalities influence firms' outsourcing decisions. Our paper differs because we analyze how depositor myopia may influence the distortions between the private outsourcing decisions and the social optimum.

A strand of the literature studies firms' incentives to share information on cyber incidents (see Gordon et al., 2003, Gal-Or and Ghose, 2005). Imperfect information sharing on cyber incidents generates horizontal spillovers between competitors. Unlike these papers, we focus on vertical spillovers between competing firms and an upstream supplier. In the extension section, we assume that the cloud service provider may not disclose cyber incidents, as in Choi et al. (2010), and unlike Cezar et al. (2017), who assume that cyber incidents are observable.

Our paper also complements the literature on cyber security in banking and payments. Several 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 the banks' decision to outsource their services to a third-party. A strand of the literature studies how liability for fraud and incidents affects the intermediaries' investment incentives (Kahn et al., 2020, Creti and Verdier, 2014). We contribute to this literature by considering that the banks may share their losses with a common third-party provider. Anand, Duley and Gai (2022) incorporate cyber attacks in the model of Rochet and Vives (2004) of bank runs. We differentiate from this paper by studying the cloud service provider's investment incentives and by endogenizing banks' outsourc-

ing decisions. In contrast, we do not assume that cyber risk may cause bank failures. A nascent empirical literature analyzes how cyber security impacts financial stability (Duffie and Younger, 2019, Eisenbach et al., 2022).

Our work is related to the law and economics literature on product liability (see Daughety and Reinganum, 2013, for a survey). As Jacob and Lovat (2016), we analyze the optimal liability regime in a vertical structure, but with network effects and downstream competition.

We also contribute to a literature which analyzes firms' incentives to become interoperable, surveyed by Bianci et al. (2023).[8] We analyze whether banks have incentives to become interoperable when this decision implies variations in cyber security.[9] Our framework of Hotelling competition with symmetric firms is similar to Doganoglu and Wright (2006), except that we do not allow consumers to multi-home. As Malueg and Schwartz (2006), who consider quantity competition and asymmetric firms, we find that banks prefer to outsource when the degree of network effects is sufficiently high.

Our paper is connected to several families of papers analyzing the optimal market structure in vertical networks (see Dogan, 2009), the role of network sharing agreements (see Foros, Hansen and Vergé, 2023), and the impact of co-investment in networks on social welfare (see Inderst and Peitz, 2012, Bourreau et al., 2018).[10] Unlike these papers, our model is applied more specifically to the banking industry. First, we do not analyze the optimal quality of the interconnection service, and consider instead payment system security as a public good. Second, the cloud service provider's input is not essential to offer payment services to depositors. Third, we do not allow for partial compatibility, which is rare in the payments industry (e.g., in Foros and Hansen, 2001 or in Stadler, Trexler and Unsorg, 2022). Unlike in the literature on competition in networks (Armstrong, 1998, Laffont, Rey and Tirole, 1998, Cambini and Valetti, 2005), banks share their network through a third-party provider, which also invests in security. This implies that they may trade-off the benefits of efficiency gains and interoperability against the costs of risk contagion.

[8] A strand of the literature studies banks' decisions to make their ATMs compatible (Matutes and Padilla, 1994, Massoud and Bernhardt, 2002), or the choice of the optimal interchange fee (see Verdier, 2011, and Rochet, 2003, for surveys).

[9] We consider interoperability at the platform level, that is, the extent to which the users of one payment system can make transactions with the users of another service provider.

[10] There is also a link between our paper and the literature analyzing the role of mergers on firms' innovation incentives and efficiency gains (see Bourreau et al., 2018, for a survey).

3 Model

We build a tractable model to study banks' incentives to outsource their payment services to a third-party provider when there is cyber risk.

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 depositors who 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.

In the market, there is a third-party provider C of a cloud-based infrastructure, which does not compete with banks for deposits. Banks may buy two different services from C. First, they may use its infrastructure to store information on payment transactions. Second, if both banks store information in the cloud, they may buy additional services from C such that their payment systems become compatible (interoperable).[11] The storage and the compatibility services are one-way complements because both banks must buy the storage service to become compatible.

The cloud service provider offers banks a contract that involves the payment of a per-depositor access fee f^a to store information and a fixed compatibility fee f^c if both banks decide to buy compatibility services, such as a payment app.[12] The cloud service provider does not price discriminate between banks.[13] We discuss in section 6 the case in which the contract includes penalties for security incidents such as Service-Level Agreements (SLAs).[14]

If banks do not join the cloud, we assume that their payment systems remain incompatible (fragmented). We motivate this assumption by the superior quality of the cloud service provider's services to reach payment system interoperability. In practice, banks often use cloud based platforms

[11]For example, in the United States, Volante Technologies offers banks cloud based services to connect to Fed Now, or to adopt a technological standard for text messaging.

[12]If the cloud service provider bundles the two services, the mechanism of the model remains identical, but the mathematical expressions become more complex. Offering a fixed compatibility fee rather than a variable fee enables the cloud service provider to extract more surplus from banks when they become compatible.

[13]There are different business models: the cloud service provider may either be a Banking-As-a-Service platform, which does not sell services directly to the consumers, it may directly sell a payments App to banks or connect banks and app providers (see the website of AWS and Grabowski, 2021, for examples).

[14]See Cezar et al. (2017) for SLA agreements for security outsourcing.

and hyperscalers to offer additional payment services.[15]

In the rest of the paper, we focus on determining an equilibrium in which banks make symmetric outsourcing decisions. For the sake of simplicity, we represent by the parameter $z = 1$ the subgame c in which both banks join the cloud and become compatible, and by the parameter $z = 0$ the subgame n in which banks remain independent, respectively. The conditions such that both banks do not prefer to deviate to the subgame o in which only one bank joins the cloud are given in the appendix. We consider equilibria in which the total demand for banking services is the same with and without cloud outsourcing because the market for deposits is covered.[16]

Payment system security: A bank's payment system security $s_i(z)$ is a function of its outsourcing decision $z \in \{0, 1\}$. If bank $i \in \{A, B\}$ does not join the cloud, the security of its payment system is $s_i(0) = s_i$. If bank i joins the cloud, the security of its payment system is a public good with an aggregate additive effort function $s_i(1) = \theta s_i + (1 - \theta)s_c$, where s_c denotes the cloud service provider's investment and $\theta \in [0, 1]$ is a technology parameter (as in Varian, 2004).[17] The parameters θ and $(1 - \theta)$ represent the bank's and the cloud service provider's respective shares of the security of the common infrastructure. For example, if banks retain a higher share of their depositors' payment information when they outsource, the parameter θ is closer to 1.[18] If both banks join the cloud, the security of their payment

[15]In a supplementary material, we fully develop the model in which banks may become interoperable with a lower-quality technology without the cloud service provider. If there is sufficient differentiation in quality, this does not impact our results.

[16]See Cremer, Rey and Tirole (2000) for a model in which compatibility increases total consumer demand and Gal-Or and Ghose (2005) for a model in which total quantities depend on security investments.

[17]Incentives for providing security are sensitive to the technology for precaution against cyber incidents. With this technology, the marginal benefits of security investments are constant, which simplifies the analysis (as Acemoglu et al., 2013). Other possibilities would be the best-shot and the weakest-link functions.

[18]Blessing and Anderson (2023) offer a comprehensive overview of all the technical possibilities to reach interoperability. In a hybrid cloud business model, banks rely on a mix of on-premises private cloud and third-party infrastructure. 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. We discuss in section 6 how the endogenous choice of a business model for cloud computing (i.e, θ) impacts our results. The parameter θ has also some similarities with the parameter used by Gordon et al. (2003) to model horizontal spillovers in security

systems jointly depends on the cloud service provider's investment, where a lower θ captures a smaller correlation of risks.

The probability h that a cyber incident occurs in bank i's payment system is a linear function of its security, that is, we have

$$h(s_i(z)) = v - \sigma s_i(z),$$

where $v \in (0,1)$ represents the exogenous maximum vulnerability of the payment system to a cyber incident, and $\sigma \in (0,v)$ is a parameter that captures the sensitivity of h to security investments. We assume that $s_i(z) \in (0, v/\sigma)$. We denote by $h_i^n \equiv h(s_i(0))$ and by $h_i^c \equiv h(s_i(1))$. If both banks invest the same amount of security, we have $h_A^n = h_B^n = h^n$ if they do not join the cloud, and $h_A^c = h_B^c = h^c$ if they both join the cloud.

The banks and the cloud service provider incur quadratic costs functions for security investments, which are denoted by $C_b(s_i) = k_b s_i^2/2$ for $i \in \{A, B\}$ and $C_c(s_c) = k_c s_c^2/2$, respectively, with $k_b > 0$ and $k_c > 0$.[19] Cloud outsourcing amounts to sharing a network infrastructure, which saves a costly duplication of security investments. We therefore measure efficiency gains by

$$\kappa \equiv \frac{k_c}{2k_b}.$$

If $\kappa < 1$, cloud outsourcing implies some efficiency gains, because the marginal cost of security investments is reduced for the common payment system.

The losses caused by cyber incidents: Cyber incidents may cause losses which depend on banks' outsourcing decisions.[20] The probabilities that a cyber incident occurs and the losses are common knowledge, except

information sharing organizations.

[19]With quadratic investment costs, our framework is equivalent to the Gordon and Loeb (2002) model of security investments with decreasing marginal returns of security investments. Our specification is more convenient to include the effects of security breaches on the product (deposit) market as in Gal-Or and Ghose (2005).

[20]If the risks of a direct attack on a bank and the cloud service provider's infrastructure are mutually exclusive (as Acemoglu et al., 2013), our model can also be seen as having two points of entry for attacks, one being located in bank i, and the other in the cloud service provider, with a perfect contagion because all players incur losses when an incident occurs. The parameter θ could also depend on the hackers' incentives to target the most vulnerable point of entry. The additive technology differs from Riordan (2014), who models the total security of the network as multiplicative in safety from a direct and an indirect attack.

for naive depositors. In the baseline model, we assume that all players can observe whether a cyber incident has occurred, and discuss in section 6.7 the case in which the disclosure of cyber incidents is imperfect. We denote by $L_b(z)$, $L_c(z)$, and $L_d(z)$ the net losses per depositor incurred by the bank, the cloud service provider and the depositor, respectively, including the potential transfers between the players if there is a liability system. The total loss per depositor is $L(z) = L_b(z) + L_c(z) + L_d(z)$.

Without outsourcing, when there is a cyber incident, each depositor incurs a loss $L_d(0) = l_d > 0$, which corresponds either to a loss of funds or the monetary cost of a data leakage (see Chande and Yandus, 2019).[21] A bank incurs a loss per depositor $L_b(0) = l_b > 0$, corresponding to the costs of fixing its security system, its reputation costs, or even higher funding costs.[22] Without outsourcing, the cloud service provider does not incur any loss. The total loss caused by cyber incidents is therefore $L(0) = l_b + l_d = l$.

If both banks outsource their payment services, the cloud service provider incurs a loss $L_c(1)$, which we normalize to zero if there are no transfers without loss of generality. Cloud outsourcing multiplies the losses of the bank and the depositors by a factor α. Therefore, we have $L_b(1) = \alpha l_b$ and $L_d(1) = \alpha l_d$, respectively, and the total loss is then $L(1) = \alpha l$.[23]

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.

Depositors are divided into two types. A proportion $\mu \in (0, 1)$ is sophisticated and the rest of depositors, in proportion $1 - \mu$, is naive. A given depositor's type will determine whether or not they will care about the level of security of the bank's payment system when they decide to open a bank

[21] Estimating the losses caused by cyber incidents is empirically challenging because 17 percent of finance and businesses report it to the regulator (Chande and Yanchus, 2019).

[22] Banks incur an annual average loss from cyber attacks representing 9 percent of their net income globally (Bouveret, 2018).

[23] Higher losses could be caused by the behavior of hackers who obtain higher rewards of targeting a common infrastructure. For example, if the latter incur a fixed entry cost before security investments, the perspective of doubling the gains of a successful attack by targeting the cloud's infrastructure (when the two banks join the cloud) would also double the probability that the depositors of a given bank incur losses. For the sake of simplicity, we capture the increased probability of losses with the exogenous parameter α.

account. Banks do not observe the depositors' types.[24]

A depositor makes a payment transaction with all the depositors who can be reached with the payment solution offered 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 expected number of compatible depositors depends on bank i's outsourcing decision. In practice, when banks share an infrastructure managed by the same third-party provider, this increases the degree of interoperability of their payment services. We assume that banks' payment systems are technically perfectly interoperable if banks outsource to the same third-party provider, whereas they remain fragmented otherwise.[25] Therefore, if both banks are compatible, each depositor is able to make a transaction with all 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.

A naive depositor located at point x on the Hotelling line who opens an account at bank i located at $x_i \in \{0, 1\}$ and expects to make transactions with N_i^e depositors derives utility

$$u_i(x) = u_0 + \beta(z + (1 - z)N_i^e) - t|x - x_i| - p_i. \tag{1}$$

Since sophisticated depositors expect to lose $h(s_i(z))L_d(z)$ when a cyber incident occurs in bank i, the depositor's average utility of opening an account at bank i is given by

$$u_i(x) - \mu h(s_i(z))L_d(z). \tag{2}$$

Bank profits: Bank i makes profit from deposits and incurs the costs of security investments and security incidents, plus the potential outsourcing fees. In the symmetric outsourcing subgames, its profit is therefore given by

$$\pi_i = (p_i - zf^a - h(s_i(z))L_b(z))N_i - zf^c - C_b(s_i). \tag{3}$$

Each bank's total marginal cost is linear in the level of risk $h(s_i(z))$ as in Daughety and Reinganum (1995). Without cloud outsourcing, each bank's

[24] Gogolin et al. (2021) offer empirical evidence of depositor sophistication by showing that successful cyber-attacks may decrease deposit growth rates at small banks. In addition, some depositors may discover the cyber ratings offered by dedicated agencies.

[25] Formally, we would obtain equivalent results with partial interoperability if the degree of interoperability is higher in the cloud.

marginal cost only depends on its investments in security.[26] With cloud outsourcing, since $h(s_i(z))$ is decreasing with s_c, the cloud service provider exerts a positive externality on a bank when it increases its investment in security by lowering its marginal cost. Therefore, if both banks join the cloud, the levels of security of their payment systems are correlated.[27]

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 cyber incidents. If banks' payment services are compatible, the cloud service provider makes a profit

$$\pi_C^c = 2f^c + (f^a - h(s_i(1))L_c(1))N_i + (f^a - h(s_{-i}(1))L_c(1))N_{-i} - C_c(s_c). \quad (4)$$

If only bank i joins the cloud, the cloud service provider makes a profit[28]

$$\pi_C^o = (f^a - h(s_i(1))L_c(1))N_i - C_c(s_c). \quad (5)$$

Banks exert a positive externality on the cloud service provider when they increase their security investments because they reduce its marginal cost.

Assumptions Finally, we formalize two additional assumptions:

- (A1): For $z \in \{0, 1\}$, we assume that $t - \beta > k_b > 2v(L_d(z) + L_b(z))/3$. Assumption (A1) implies that banks' profits are concave in security investments and prices, and that both banks make positive profits in equilibrium. Assumption (A1) and $\sigma \leq v$ imply that $k_b > \sigma l/2$.
- (A2) $k_c > \max(\theta\alpha\sigma l, (1-\theta)\alpha\sigma l)$. Assumption (A2) implies that there is an interior solution when the regulator chooses the first-best levels of investment in security.

Timing of the game:

The cloud service provider and the banks decide how much to invest in payment system security before banks make their outsourcing decisions. We

[26] Linear horizontal spillovers would not change our results.

[27] This externality differs from a direct link between banks' investment, which happens for instance with a weakest-link type technology (Hirshleifer, 1983, Anand et al., 2022).

[28] The probability that a cyber incident occurs in bank i is the same whether one bank or two banks join the cloud service provider.

consider long-term investments (i.e, R&D of encryption technologies, firewalls, authentication methods...), which are essential for payment system interoperability.[29] The timing of the game is as follows:

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. Each bank $i \in \{A, B\}$ chooses the price of deposit accounts p_i and then depositors choose in which bank to open an account.

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

4 The social planner's decisions

In this section, we analyze a benchmark in which a social planner chooses security investments and whether to build an interoperable payment system.[30]

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 denote by $s_b^w(z)$ and s_c^w the welfare-maximizing investments in security of the banks and the cloud service provider, respectively.

Proposition 1 compares welfare-maximizing levels of payment system security with or without cloud outsourcing.

[29] In practice, all players make continuous investment decisions, and may also invest after a cyber incident (e.g, patches to repair software bugs). We do not consider this type of investment (see Cavusoglu et al., 2008, August and Tunca, 2006 and 2008, and Lam, 2016 for an analysis of software patching).

[30] The first-best and the second-best are equivalent in our setting, because deposit prices are simply transferred from the bank to the depositors and do not impact social welfare.

Proposition 1 *The welfare-maximizing level of security is higher if both banks outsource their payment services if either* $\theta^2\alpha \geq 1$ *or* $\theta^2\alpha < 1$ *and*

$$\kappa < \kappa_s \equiv \frac{(1-\theta)^2\alpha}{1-\theta^2\alpha}.$$

Proof. See Appendix A.1. ■

The welfare-maximizing security investments are such that the marginal social benefits of a higher security are equal to the marginal social costs. If banks' welfare-maximizing contributions to payment system security increase with cloud outsourcing, the welfare-maximizing level of security is always higher when both banks join the cloud. Cloud outsourcing multiplies the marginal benefits of banks' investments in security by a factor $\theta\alpha$. First, banks' investments in security have a lower marginal impact on the probability that a cyber incident occurs, because banks only take on a marginal share θ of the security effort. Second, with cloud outsourcing, the minimum total loss equals αl. Therefore, banks' welfare-maximizing level of security increases if and only if $\theta\alpha > 1$. Since banks take on a share θ of security investments, the welfare-maximizing contribution of banks to payment system security is higher with cloud outsourcing if and only if $\theta^2\alpha \geq 1$.

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. This happens if and only if there are sufficient efficiency gains. The cloud service provider contributes marginally to a share $(1-\theta)$ of payment system security and invests a share $(1-\theta)(\alpha/\kappa)$ 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 $(1-\theta)^2(\alpha/\kappa)$, and a marginal cost $(1-\theta^2\alpha)$, which are expressed in share of the initial security without outsourcing, respectively. If the inequality of Proposition 1 holds (i.e, $\kappa < \kappa_s$), 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 (i.e., $\alpha = 1$), the welfare-maximizing level of security is higher with cloud outsourcing if and only if there are efficiency gains (i.e., $\kappa < 1$).

4.2 Welfare-maximizing outsourcing decisions

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

$$\Delta L_w = (\alpha h(\theta s_b^w(1) + (1-\theta)s_c^w) - h(s_b^w(0))l$$

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

$$\Delta C_w = 2\Delta C_b + C_c(s_c^w),$$

the difference in the costs of payment system security with and without cloud outsourcing, respectively, where $\Delta C_b = C_b(s_b^w(1)) - C_b(s_b^w(0))$.

Proposition 2 gives the conditions under which cloud outsourcing increases social welfare with the socially optimal levels of investments.

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

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

with $\beta_w \equiv 2(\Delta L_w + \Delta C_w)$.

Proof. See Appendix A.2. ■

Cloud outsourcing reduces the cost of fragmentation of payment systems (see BIS, 2022).[31] First, this decision increases the welfare benefits of network effects by $\beta/2$, because it enables each bank's depositors to make transactions with the consumers of its competitor. Second, 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. The additional maximal potential loss in case of a cyber incident increases by $(\alpha - 1)vl$. As shown in Proposition 1, cloud outsourcing may either improve or weaken payment system security, and increases sometimes security costs. 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 there are sufficient efficiency gains, social welfare is always higher with cloud outsourcing.

[31] The BIS annual report of 2022 mentions the cost of fragmented payment systems for the economy and the welfare gains associated with interoperability (see e.g. on p.91).

If there are no additional losses (i.e., $\alpha = 1$), cloud outsourcing benefits the society for any level of network effects β when the level of security is higher if both banks join the cloud (i.e., if $\kappa < \kappa_s$, as shown in Appendix A.2).

5 Cyber security and bank competition

In this section, we analyze the market equilibrium, when banks compete in prices and security.

5.1 Stage 4: competition for deposits

We determine how banks price deposit services if they take symmetric outsourcing decisions.

5.1.1 Deposit prices and bank profits

We start by analyzing consumer demand for deposits. At the equilibrium of stage 4, depositors' expectations of banks' market shares are fulfilled, and from Eq.(2), each bank $i \in \{A, B\}$ obtains a market share given by:

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

where $\tau(z,\beta) \equiv t - (1-z)\beta$ and $\Delta h(z) \equiv h(s_i(z)) - h(s_{-i}(z))$ represents the degree of security differentiation.[32] Banks' market shares depend on the marginal cost asymmetries implied by security differentiation, which are internalized by sophisticated depositors. If payment systems are fragmented, depositor demand response to prices is increasing with network effects. Therefore, interoperability softens price competition for deposits.[33]

At the competition stage, each bank i chooses p_i to maximize its profit π_k given in Eq.(3). If banks take symmetric outsourcing decisions, at the equilibrium of stage 4, banks choose deposit prices given by

$$p_i^*(z) = \tau(z,\beta) + h(s_i(z))L_b(z) + zf^a - \frac{\Delta h(z)}{3}\rho_b(z), \tag{7}$$

[32] No bank corners the market if and only if $p_i - p_{-i} + \mu\Delta h(z)L_d(z) \in (-\tau(z,\beta), \tau(z,\beta))$.

[33] If the total size of the market is not fixed (e.g, as in Katz and Shapiro, 1985), there is an additional countervailing effect of compatibility on prices: it increases the total quantities and may sometimes lower firms' common equilibrium price.

where banks' marginal cost of cyber incidents, including the internalization of the sophisticated depositors' losses (in proportion μ), is given by

$$\rho_b(z) = L_b(z) + \mu L_d(z).$$

The equilibrium deposit prices correspond to those of a Hotelling model with asymmetric marginal costs. A bank's marginal cost is the sum of the expected losses caused by cyber incidents $h(s_i(z))L_b(z)$, the access fee paid to the cloud service provider zf^a, net of the marginal benefit of network effects $(1-z)\beta$ (included in $\tau(z,\beta)$). The last term captures banks' differentiation in security.

Replacing for $p_i^*(z)$ given by Eq.(7) in Eq.(3) gives the profit of bank i at the equilibrium of stage 4:

$$\pi_i = \frac{(\tau(z,\beta) - \Delta h(z)\rho_b(z)/3)^2}{2\tau(z,\beta)} - zf^c - C_b(s_i). \tag{8}$$

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 and the compatibility fee. In this subsection, we assume without loss of generality, that bank A has a higher level of security than bank B following stages 1 and 2.

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 their depositors different levels of security. 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 compatibility fee f^{c*} so as to extract banks' additional profit of compatibility. Therefore, banks obtain the same profit of using only the storage service without compatibility, and becoming compatible. In Appendix C, we show that the equalization of banks' profits in both cases gives

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

In addition, the cloud service provider sets the maximum access fee such that each bank does not have the incentives to become independent. Since banks' levels of security may differ after stage 2, one bank (the strongest bank) may have higher deviation incentives 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 strongest bank 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. Therefore, the strongest bank is willing to pay a maximum access fee implicitly defined by

$$h(s_i(1))\rho_b(1) + f_i^{a*} \equiv h(s_i(0))\rho_b(0). \tag{10}$$

If $f_A^{a*} \geq f_B^{a*}$ or else if $\theta\rho_b(1) \leq \rho_b(0)$, the riskiest bank B has the highest willingness-to-pay for cloud services, because its marginal cost (including the limit access fee) is lower than that of bank A. The reverse is true otherwise.

Suppose now that the cloud service provider serves a single bank. It chooses the access fee that equalizes the bank's marginal cost of joining the cloud and remaining independent. As shown in Appendix C, 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 is the strongest bank. 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 either serves 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.

Lemma 1 gives 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*

$$min\{f_A^{a*}, f_B^{a*}\} = \begin{cases} f_A^{a*} & \text{if } \theta\rho_b(1) \leq \rho_b(0) \\ f_B^{a*} & \text{otherwise.} \end{cases}$$

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 C. ■

It is noteworthy 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

Proposition 3 gives the conditions such that the cloud service provider enters the market and serves both banks.[34]

Proposition 3 *If banks choose symmetric investments in security, the cloud service provider enters the market and serves both banks, which become compatible, if and only if $\beta \geq \max\{0, \widehat{\beta}\}$, with*

$$\widehat{\beta} \equiv h(s_i(1))\rho_c(1) - h(s_i(0))\rho_b(0) + C_c(s_c), \tag{11}$$

where $\rho_c(1) \equiv \rho_b(1) + L_c(1)$ represents the marginal cost of cyber incidents internalized by the cloud service provider. The cloud service provider makes profit $\pi_C^c = \max\{0, \beta - \widehat{\beta}\}$. Otherwise, both banks remain independent.

Proof. Appendix D. ■

The cloud service provider enters the market when its entry benefit exceeds the costs of cyber risk. The benefit of serving both banks is equal to the sum of the value of network effects (β) and the access fee ($h(s_i(0))\rho_b(0) -$

[34] All the details with asymmetric investment decisions are given in Appendix C.

$h(s_i(1))\rho_b(1))$, which represents the variation of banks' expected loss when they join the cloud. The cloud service provider's cost of cyber risk is equal to its expected cost of damage and its cost of security investment (or else, $h(s_i(1))L_c(1) + C_c(s_c)$).

The distortions with respect to the first-best

Proposition 4 compares banks' outsourcing decisions with cyber risk to the first-best when security investments are exogenous.

Proposition 4 *With cyber risk, there may be either over-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 the sign of $\beta^w - \widehat{\beta}$. We show in Appendix E that we may either have $\beta^w - \widehat{\beta} > 0$ or the reverse. ■

Because of cyber risk, there may be either over or under-outsourcing of payment services. The first distortion is caused by competition and network effects. Suppose that there is no cyber risk and that banks do not incur any investment costs. Then, the private benefits of outsourcing are twice as high as the marginal social benefit of outsourcing.[35] This result arises because banks take their outsourcing decision without internalizing its effect on the profit of their competitor. As in Foros and Hansen (2001), this mechanism implies that they over-outsource their payment services with respect to the social optimum, that is, we have $\beta^w - \widehat{\beta} = \beta^w/2 > 0$.[36]

The second distortion is caused by the effect of the outsourcing on banks' investment costs, which is imperfectly internalized by the cloud service provider. If the welfare-maximizing levels of bank security are higher with cloud out-

[35]From Proposition 3 without cyber risk, banks join the cloud if and only if $\beta \geq C_c(s_c)$, whereas, from Proposition 2, if there is no cyber risk ($h = 0$, $\Delta L_w = 0$ and $\Delta C_w = C_c(s_c)$), cloud outsourcing is socially desirable if and only if $\beta/2 \geq C_c(s_c)$.

[36]Each bank values its benefit from the compatibility service at $\beta/2$. In the literature on production management, firms outsource when there are scale economies because it dampens price competition (see Mc Guire and Staelin, 1983, Van Mieghem, 1999).

sourcing, higher investment costs reinforce the over-outsourcing[37] because

$$\beta^w - \widehat{\beta} = \beta^w/2 + 2\Delta C_b > 0.$$

With cyber-risk, the third distortion is due to the imperfect internalization of the variation of the social loss. If welfare-maximizing levels of security are higher with cloud outsourcing, higher security levels reduce the over-outsourcing because

$$\beta^w - \widehat{\beta} = \beta^w/2 + 2\Delta C_b + (h(s_b^w(1)) - h(s_b^w(0)))l,$$

with $(h(s_b^w(1)) - h(s_b^w(0)))l < 0$. Otherwise, if welfare-maximizing levels of security are lower, this reinforces the over-outsourcing.

Depositor myopia to cyber risk adds a fourth distortion. If some depositors are naive, we have

$$\beta^w - \widehat{\beta} = \beta^w/2 + \Delta C_b + (h(s_b^w(1)) - h(s_b^w(0)))l + (1-\mu)\Delta\mathbb{E}(L_d),$$

where $\Delta\mathbb{E}(L_d) \equiv h_w^c L_d(1) - h^n(s_b^w(1))L_d(0)$ represents the difference in the depositors' expected loss, which banks do not internalize when depositors are myopic. If cloud outsourcing increases the depositors' expected loss, depositor myopia gives banks incentives to over-outsource (resp., under-outsource if it reduces their expected loss).

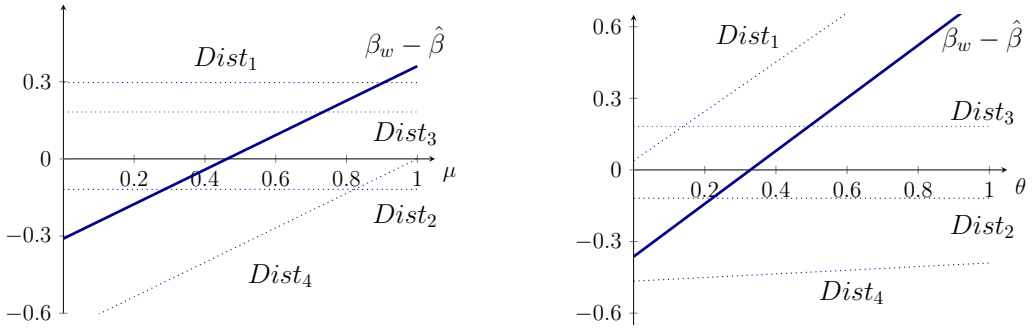

Fig. 1 and 2 - Outsourcing decision with exogenous investments[38]

[37] See Proposition 1 for the conditions.

[38] Figures are plotted using first-best investments, $l_d = 2$, $l_b = 1$, $\alpha = 6/5$, $\eta_d = \eta_c = \gamma_b = 1$, $\gamma_d = 2$, $h = \sigma = 1$, $k_c = 2k_b = 6$, with $\theta = 1/3$ (Figure 1) and $\mu = 1/3$ (Figure 2).

Figure 1 and 2 above illustrate the difference between the private outsourcing decisions and the social optimum with an inefficient cloud service provider, each distortion from 1 to 4 being represented by *Dist* with dashed lines. If there is over-outsourcing, a lower degree of correlation of security (i.e, a higher θ) or a higher share μ of sophisticated depositors reinforce banks' incentives to over-outsource.[39]

The impact of outsourcing on bank profits and depositor surplus

Proposition 5 details the effect of cloud outsourcing on the banks' profits and depositor surplus, respectively.

Proposition 5 *Suppose that banks invest symmetric levels of security $s_b(z)$ at stage 2, where $z \in \{0,1\}$. Cloud outsourcing increases banks' profits if and only if it reduces their security investments (i.e., if $s_b(1) \leq s_b(0)$). Depositor surplus is higher with cloud outsourcing if and only if*

$$\sigma\rho(0)(s_b(0) - s_b(1)) \geq \frac{\beta}{2}.$$

Proof. See Appendix F. ■

Banks' profits on the deposit market are independent from cyber risk if their security levels are identical. 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, cloud outsourcing always reduces depositor surplus. The reason is that interoperability softens price 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 this case, the improvement of payment system security compensates for higher deposit prices.

5.3 Stage 2: banks' investment in security

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

[39] With the parameters of Figure 1 and 2, there is over-outsourcing if $\mu > 0.47$ (Figure 1) and $\theta > 1/3$ (Figure 2).

Lemma 2 *If both banks make the outsourcing decision $z \in \{0,1\}$, the subgame in which banks choose their investment in security admits a unique symmetric Nash equilibrium, where each bank invests an amount*

$$s_b^*(z) = (1 - z(1-\theta))\frac{\sigma\rho_b(z)}{3k_b}. \tag{12}$$

Proof. See Appendix G. ■

Banks choose their investments in security such that their marginal benefit equals their marginal cost $k_b s_i(z)$. When both banks join the cloud, their marginal benefit of security investment is equal to $\theta\sigma\rho_b(1)/3$. When banks remain independent, their marginal benefit is $\sigma\rho_b(0)/3$. Therefore, banks' investments in cyber security increase when they join the cloud if their marginal benefit of security investment increases. Compared to the social optimum, banks reduce their investments in security to soften security 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 $s_c^*(1)$ that maximizes π_C^c given in Proposition 4, that is,

$$s_c^*(1) \equiv \sigma(1-\theta)\frac{\rho_c(1)}{k_c}. \tag{13}$$

At the equilibrium of the game, both banks outsource their payment services if and only if the cloud service provider makes a positive profit, which happens, as in Proposition 3, if and only if $\beta > \max\{0, \widehat{\beta}\}$, with

$$\widehat{\beta} \equiv h(\theta s_b^*(1) + (1-\theta)s_c^*(1))\rho_c(1) - h(s_b^*(1))\rho_b(0) + C_c(s_c^*(1)). \tag{14}$$

The distortions with endogenous investments

With endogenous investments in security, there are additional distortions with respect to the first-best, because firms under-invest in security. First, banks do not take into account the effect of their investments on the damage incurred by the cloud service provider. Second, banks under-invest in security to soften security competition for depositors. Third, banks and the cloud service provider choose how much to invest in security without internalizing the expected damage of myopic depositors. The under-investment of the

cloud service provider always leads to over-outsourcing, because it increases its incentives to enter the market. However, banks' under-investment may sometimes enable the cloud service provider to charge a higher access fee, which increases its incentives to enter the market. In addition, investments are inefficiently shared between the cloud service provider and the banks. If $\rho_b(1)+3L_c(1) > 0$, the cloud service provider bears an inefficiently high share of security investments compared to the first-best, because we have

$$\frac{s_b^*(1)}{s_c^*(1)} = \frac{2\rho_b(1)}{3\rho_c(1)} \frac{s_b^w(1)}{s_c^w(1)} < \frac{s_b^w(1)}{s_c^w(1)}.$$

Comparative statics with endogenous investments:

We examine how the main parameters of the model (i.e, μ and θ) impact the comparison of the private outsourcing decisions with the first-best.

If security levels are exogenous and outsourcing increases the expected loss, a higher proportion of sophisticated depositors increases banks' incentives to join the cloud. This effect amplifies the distortion between the private outsourcing decisions and the social optimum if there is over-outsourcing.[40] Our conclusion resembles the result of Lam and Seifert (2023), in a different setting. These authors show that a higher proportion of sophisticated consumers reinforces the over-sharing of consumer data by a data controller to a third-party. We also reach the opposite conclusion when outsourcing reduces the expected loss: a higher proportion of sophisticated depositors reduces banks' incentives to join the cloud when the latter is efficient enough.[41]

In addition, depositor sophistication has an indirect effect on the cloud service provider's incentives to enter the market because banks invest in security. If there is a higher proportion of sophisticated depositors, banks invest more in security. However, this has an ambiguous impact on the cloud service provider's entry decision. On the one hand, the latter benefits from a higher level of payment system security, but on the other hand, it extracts lower revenues from access because banks' profit decreases. The cloud service provider has lower incentives to enter the market when the proportion of sophisticated depositors increases if $\rho_b(0) - \theta\rho_c(1) > 0$. This happens for

[40] See Appendix H.1.

[41] Unlike Lam and Seifert (2023), we consider downstream competition and endogenous access prices.

instance if cloud outsourcing generates low efficiency gains.[42]

The impact of θ on the comparison between the private outsourcing decisions and the social optimum depends on the efficiency of cloud outsourcing.[43] If there are very high efficiency gains associated with cloud outsourcing, the difference between β^w and $\widehat{\beta}$ is first increasing and then decreasing with θ, the banks' share of the common payment system. Therefore, if there is over-outsourcing, there exists a value of θ which maximizes the distortion of outsourcing decisions.

6 The role of public intervention

In this section, we discuss the impact of several regulations on payment system security and outsourcing decisions. In practice, the financial regulator's optimal policy-mix depends on the costs of security audits, the perimeter of regulation and the enforcement power given by the legislation. Recently, several jurisdictions have decided to extend the financial regulator's power to reach cloud service providers, access their data or inspect their facilities (e.g, DORA regulation in Europe, FCA in the United-Kingdom). This evolution can be justified by the costs of exerting market discipline for small depositors.[44]

6.1 Security Standards

If security audits are not very costly, setting-up security standards is the best solution to implement the first-best levels of investments in security, provided that firms pay high penalties if they are not compliant. For this solution to be effective, the financial regulator should have the power to audit the cloud service provider and to impose fines. However, security standards may not be sufficient to reach the socially optimal outsourcing decision. First, standards for cloud security reduce the third-party provider's incentives to enter the market by increasing its investment costs. Second, standards for

[42]This effect does not arise in Lam and Seifert (2023) because they neither model the third-party provider's investment incentives, nor do they consider access fees.

[43]See Appendix H.2.

[44]Defining the optimal policy-mix between regulation and tort law is not obvious (see Hiriart et al., 2008). In payment systems security, there is a mix of ex-ante regulation (sometimes with the zero-liability rule for depositors) and ex-post tort law.

bank security may sometimes reduce the cloud service provider's revenues from access more than its expected damage (i.e., if $\theta\rho_c(1) \geq \rho_b(0)$). In this case, security standards make outsourcing less profitable for all firms than the social optimum.[45] In addition, this solution does not fully cover the depositors, who have to incur the losses of cyber incidents which occur even if firms are compliant.

6.2 Authorization of cloud outsourcing agreements

Security standards could be combined with a mandatory review of cloud outsourcing contracts by the regulator. In several countries (e.g., England, Australia), the regulator may correct the bias towards excessive outsourcing by refusing to allow outsourcing contracts. Then, a combination of security standards and the power to refuse outsourcing agreements enables the regulator to implement the first-best allocation. In particular, we have seen in section 5.2.2 that if the marginal increase in the losses is higher than the marginal reduction of the investment costs, banks' incentives to over-outsource are reinforced. In that case, the regulatory power to refuse outsourcing agreements improves welfare. However, this instrument cannot correct outcomes with under-outsourcing.

6.3 Common liability regime

If full security audits are very costly, the regulator may try and design ex ante a strict liability system to implement the first-best security investments.[46] We assume as a benchmark that the financial regulator may always find convincing evidence that a cyber incident occurred without performing any security audit. The regulator may prefer that firms jointly bear the responsibility for cyber incidents. We call this solution the common liability regime, in which the upstream firm and the downstream firms are both liable with respect to end-users when a cyber incident occurs.

[45] Security standards decrease outsourcing if there are sufficient efficiency gains. See Appendix K for the exact threshold.

[46] The sharing of the losses for cyber incidents may vary across jurisdictions. Banks may often 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). 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 (the cloud service provider).

Without cloud outsourcing, the bank pays a depositor $\eta_d \in (0, l_d)$ when a cyber incident occurs.[47] Therefore, the bank incurs a loss $l_b + \eta_d$ and each depositor incurs a loss $l_d - \eta_d$. In addition, with cloud outsourcing, the liability system defines the transfers $\gamma_d \geq 0$ and $\gamma_b \geq 0$ from the cloud service provider to the depositor and the banks, respectively. Banks may also compensate the cloud service provider with a transfer $\eta_c \geq 0$.

If the penalties for cyber incidents were privately chosen by the cloud service provider (e.g, with SLAs), the cloud service provider would not choose the socially optimal investment in security, because it does not perfectly internalize all the social losses.[48] Lemma 3 shows that a regulator may use a common strict liability regime to implement the first-best if some depositors are naive.

Lemma 3 *If all depositors are sophisticated, a common liability regime is ineffective. If some depositors are naive ($\mu < 1$), a common liability regime may be used to increase firm's investment incentives.*

Proof. See Appendix I.1. ■

If all depositors are sophisticated, banks perfectly internalize the depositors' losses and pass on the costs of compensating depositors into higher retail prices, which renders the liability rules ineffective. The cloud service provider passes on the costs of compensating the banks and the depositors into higher access prices. However, if some depositors are naive, firms' internalization of the depositors' losses is imperfect, which implies that a common liability regime may be used to implement the first-best.

In Proposition 6, we analyze the properties of the common liability regime that enables the social planer to implement the first-best.

Proposition 6 *To implement firms' first-best security investments, the social planner needs to subsidize the cloud service provider. Such a common liability system fully covers the depositors' losses, subsidizes the cloud service provider, and offers banks partial damage coverage.*

Proof. See Appendix I.2. ■

To implement banks' first-best investments in cyber security, the social planner needs to raise their marginal cost of cyber incidents. Since the cloud

[47] In a landmark cyber security case, the UK Financial Conduct Authority (FCA) has fined 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.

[48] If the cloud service provider's profit is increasing with banks' investment in security, the transfer γ_b should be minimal, so as to provide banks' with investment incentives.

service provider internalizes the banks' marginal cost of security incidents, its marginal cost is then necessarily too high to reach its first-best level investment in security. The cloud service provider's investment incentives can be reduced thanks to a reward, which reduces its expected loss. If subsidizing the cloud service provider with transfers is impossible, the social planner cannot simultaneously implement the first-best levels of investments in security for all players. Hylton and Lin (2014) obtain a similar result that the optimal punishment is sometimes a reward when firms may invest with external benefits.[49]

If it is possible to award punitive damages, the social planer may implement the first-best total level of payment security without subsidizing the cloud service provider.[50] As a benchmark, it is also interesting to note that the social planner is never able to implement the first-best total level of payment system security without punitive damages when the cloud service provider is not liable.[51]

6.4 Shared responsibility model

If full security audits are very costly, one compromise is to perform a light security audit, which enables the regulator to determine whether the cyber incident occurred in the bank's perimeter (with probability $\theta(h - \sigma s_b)$) or in the cloud service provider's perimeter (with probability $(1-\theta)(h - \sigma s_c)$). Then, the liability regime may be designed such that the transfers become contingent on the location of the cyber incident. The Australian regulator (APRA) calls this regulatory framework "the shared responsibility model".

Proposition 7 compares firms' investment and payment system security with a shared responsibility model and the common liability regime.

Proposition 7 *In the shared responsibility model, banks' investment in cyber security is higher than in the common liability regime, whereas the cloud service provider's investment is lower. Total payment system security in-*

[49] Hylton and Lin (2014) show that the recommendation that the optimal penalty should internalize the marginal social harm is no longer valid.

[50] See Appendix I.3.

[51] If firms can escape liability without being detected, punitive damages may improve social welfare. We refer the reader to Polinsky and Shavell (2000) for a discussion of the drawbacks of this solution. In our framework, punitive damages may improve social welfare because of investment incentives even if firms disclose perfectly cyber incidents.

creases if there is a high proportion of sophisticated depositors, if banks' liabilities are low and if the cloud service provider's liability is high.

Proof. See Appendix J. ■

If a cyber incident occurs in a bank's perimeter, the bank internalizes a higher share of damage in the shared responsibility model because the cloud service provider does not pay compensations in that case. This increases depositor demand response to security investments, which implies that banks invest more in security, but pay a lower access fee. If a cyber incident occurs in the cloud service provider's perimeter, banks internalize a lower amount of damage because they do not pay compensations. Since banks' expected marginal cost of cyber incidents decreases, they pay a higher access fee. This reduces depositor demand response to the cloud service provider's investment, and thus, decreases the cloud service provider's investment incentives. Since the shared responsibility model increases banks' investment and reduces the cloud service provider's investment, it improves payment system security if an only if banks have a sufficiently high share of payment system security, and if the latter are relatively more efficient than the cloud service provider.

Figure 3 below illustrates security investments as a function of depositor sophistication. The solid blue line and the red line represent payment system security with a common responsibility regime and a shared responsibility model, respectively. To facilitate the analysis, we express payment system security as a percentage of the welfare-maximizing level of payment system security (see the vertical axis s/s^w). The dashed lines illustrate firms' investments as a percentage of their welfare-maximizing investments. We see that under the shared responsibility regime, each firm's investment is more sensitive to the proportion of sophisticated depositors. Therefore, payment system security increases with depositor sophistication.

Figure 4 below illustrates the probability that the system is attacked as a function of the bank's share of payment system security θ. As shown in Proposition 7, payment system security is higher with the shared responsibility model when banks have a high share of the common system.[52]

Implementing the first-best levels of security with the shared responsibil-

[52]Using the parameters of the figures below, the shared responsibility regime increases the security if $\kappa < 3/5$.

[53]Figures are plotted using $L_d = 4$, $L_b = 2$, $\eta_d = \eta_c = \gamma_b = 1$, $\gamma_d = 2$, $\overline{h} = 1$, $\sigma = 5/6$, $k_c = 2k_b = 12$, with $\theta = 1/2$ (Figure 3) and $\mu = 1/3$ (Figure 4). These parameters satisfy our assumptions (A1), (A2), and $\overline{h} > \sigma$.

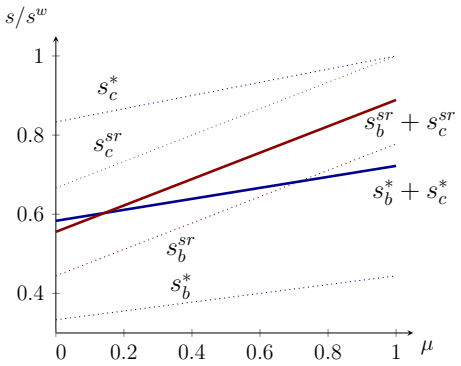

Fig. 3 - Investments[53]

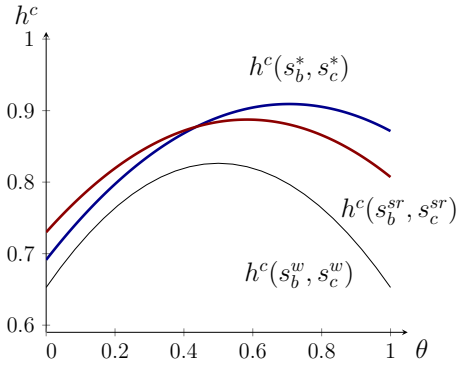

Fig. 4 - Probability of attack[53]

ity model requires imposing higher liabilities on the cloud service provider and lower liabilities on banks than under a common responsibility regime.[54] First, when a cyber incident occurs in the cloud service provider's perimeter, the latter does not share with banks the compensation of depositors. Second, when a cyber incident occurs in a bank's perimeter, banks internalizes a higher share of the damage, which implies that they should pay smaller compensations. Also, implementing the first-best levels of security no longer requires that depositors are fully covered when an incident occurs in a bank's perimeter. Indeed, a full coverage of depositors' losses has no effect on the cloud service provider's investment when a cyber incident occurs in the bank's perimeter, and banks' under-investments can also be corrected thanks to firms' transfers.

6.5 Common public infrastructure

The financial regulator may lack the proper instruments to correct market outcomes with low degrees of interoperability. In this case, it might be socially desirable to build a public interoperable payment infrastructure (see Pix in Brazil or UPAI in India). Then, the regulator has the power to choose the prices of access and compatibility, and how much to invest in the security of the common infrastructure.[55] Banks remain free to choose how much to invest in security and to compete for deposits.

As before, the regulator cannot implement the first-best level of security

[54] See Appendix J.
[55] See Appendix L.

without subsidizing the infrastructure. However, the latter may influence the banks' outsourcing decisions by choosing the compatibility fee, which reduces the distortions with respect to the first-best. Nevertheless, the regulator is unable to influence the banks' profit when they renounce to join the common infrastructure. Since banks under-invest with respect to the first-best in that case, their outsourcing decisions may still be inefficient.

If the level of interoperability is inefficiently low, joining the common public infrastructure may become mandatory. In Brazil, the Central Bank has made it mandatory for large institutions to join the payment system Pix. In addition, it is noteworthy that it decided in September 2023 to apply penalties to banks if they do not report cyber incidents.[56]

6.6 The third-party provider's perimeter

So far, we have assumed that banks' shares of the common system (i.e, the parameter θ) were exogenous. In this subsection, we discuss the optimal design of the hybrid cloud. The social optimum is reached if banks store the maximum amount of data in the cloud when there are efficiency gains associated with cloud outsourcing (i.e, $\theta = 1$ if $\kappa < 1$), and retain the maximum amount of data otherwise. This solution does not maximize the surplus of depositors because the latter would prefer that banks always keep the maximum of data in their private clouds.[57]

If the cloud service provider is able to add a data sharing dimension to the outsourcing contract by choosing a technology that impacts θ, it sometimes excessively chooses to keep the maximum of data compared to the social optimum. The cloud service provider chooses $\theta = 1$ for a degree of efficiency gains $\kappa < \kappa_p$ with sometimes $\kappa_p > 1$.[58] However, the cloud service provider may sometimes prefer that banks manage themselves a maximum share of payment system security, which maximizes depositor surplus.[59] This result is interesting in light of the recent discussions about the possibility to allow users to choose where to store their data.[60]

[56]See the BCB resolution N°342 of September 2023.

[57]See Appendix M.

[58]See Appendix M.

[59]As in the previous sections, the cloud service provider does not internalize the effect of the choice of θ on banks' costs of security and on their investment incentives.

[60]The project of a Data Act in the European Union is to implement data portability, which is defined as the ability of a customer to move data between their own system and

6.7 Information disclosure

One difficulty with the liability regime for cyber incidents is caused by firms' lack of incentives to report cyber incidents to the depositors.[61] This specific characteristic of cyber risk is a source of concern for the financial supervisors (see EBA, 2019, and the UK House of Commons, 2019). Banks' incentives to disclose cyber incidents are arguably higher than those of a cloud service provider, because of reputation incentives created by long-term relationships and financial supervision.[62] When a cyber incident is unreported, this may prevent the regulator from enforcing the transfers that are defined in a strict liability regime.

In the supplementary appendix, we model the cloud service provider's incentives to conceal information on the cyber incident. When more information is hidden, this reduces the probability that firms pay compensations and increases the additional losses. If the cloud service provider's net transfer to banks is positive, we show that it does not disclose all information to avoid being liable.

Moral hazard has an ambiguous impact on banks' marginal costs of cyber incidents. On the one hand, banks expect to incur higher losses when more information is hidden. On the other hand, banks' marginal cost of compensating naive depositors is reduced, because the probability that firms pay compensation is lower. This implies that banks may sometimes benefit from moral hazard. Banks' marginal cost of cyber incidents may vary non-monotonically with the amount of information hidden by the cloud service provider. The potential non-monotonic relationship between banks' marginal costs and information disclosure may complicate the enforcement of a strict liability regime. This implies that a liability system should be combined with a regulation of information disclosure to increase payment system security. For instance, an option would be to impose specific penalties for the lack of information disclosure, as did the BCB for the payment system Pix.

The relationship between the liability system and investment incentives

cloud services, and between cloud services of different cloud service providers.

[61] 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%.

[62] See 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, whereas reporting cyber incidents is mandatory for banks in several countries.

may differ from our baseline model. If all depositors are sophisticated, increasing the cloud service provider's transfers to the banks and the depositors, respectively, is the best way to increase firms' investment. The latter invest more to protect themselves from the additional potential damage caused by imperfect information on cyber incidents. 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, which enables the cloud service provider to extract higher revenues from access.[63] On the other hand, banks may reduce their investment in security, which may increase the cloud service provider's losses.

Moral hazard also impacts outsourcing incentives. The variation of the total loss caused by the outsourcing with exogenous levels of investment changes. If the cloud service provider internalizes a higher share of the damage, 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 service provider 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 extracts lower rents, which reduces its incentives to enter the market.

7 Conclusion

In this paper, we compared several policy options to improve payment system security and interoperability. If security audits are very costly, we demonstrated that the optimal common strict liability regime in terms of security implies subsidizing the cloud service provider. We also showed that a shared responsibility model may sometimes improve payment system security, but this depends on the business model used for cloud outsourcing and depositor sophistication. The regulator should complete the regulatory framework with disclosure requirements, which may become effective only if some efforts are devoted for consumer education.

[63] See the online appendix O.1 for the full details.

Our work entails several limitations that would deserve further exploration in future research. In particular, we considered that the regulator is both benevolent and perfectly informed about the technology. Moreover, we assumed that criminals do not adapt their behavior to the legal framework. It would be also worthwhile to include in our model the social preferences for data privacy, which might be also important in assessing the benefits of relying on a public common infrastructure for payments. Finally, infrastructure sharing in electronic payments may also generate other external benefits, as the reduction of the costs of fighting money laundering and illicit activities, which are beyond the scope of this paper.

References

[1] Amir, E., Levi, S. & Livne, T. (2018): "Do firms underreport information on cyber-attacks? Evidence from capital markets," *Review of Accounting Studies*, 23(3), 1177–1206.

[2] Anand, K., Duley, C., Gai, A.P. (2022): Cybersecurity and Financial Stability. Working Paper.

[3] Anderson, R. and Moore, T. (2009): "Information security: where computer science, economics and psychology meet," *Philosophical Transactions of the Royal Society A*. 367(1898), 2717–2727.

[4] August, T. and Tunca, T.I. (2006) Network Software Security and User Incentives. Management Science, 52, 1703-1720.

[5] Armstrong, M. (1998), Network Interconnection in Telecommunications. The Economic Journal, 108: 545-564.

[6] Bank for International Settlements (2022): "Annual Economic Report," June.

[7] Bank of Canada (2019): "Financial System Review," 19–22.

[8] Bianchi, M., Bouvard, M., Gomes, R., Rhodes, A. & Shreeti, V. (2022): "Mobile Payments and Interoperability: Insights from the Academic Literature," *HAL Working Papers*.

[9] Bourreau, M., Cambini, C. & Hoernig, S. (2018): "Cooperative investment, access, and uncertainty," *International Journal of Industrial Organization*, 56, 78–106.

[10] Bouveret, A. (2018): Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund, Working Paper No. 18/143, Washington DC.

[11] Chande, N. & Yanchus, D. (2019): "The cyber incident landscape," *Bank of Canada Staff Analytical Note*, 2019(32).

[12] Chiu, J. & Wong, T.N. (2022): "Payments on digital platforms: Resiliency, interoperability and welfare," *Journal of Economic Dynamics and Control*, 142, 104173.

[13] Choi, J.P., Fershtman, C. and Gandal, N. (2010). Network Security: Vulnerabilities and Disclosure Policy. The Journal of Industrial Economics, 58: 868-894.

[14] Covert, E. (2021): "Case Study: AWS and Capital One.," *System Weakness*.

[15] Creti, A. & Verdier, M. (2014): "Fraud, investments and liability regimes in payment platforms," *International Journal of Industrial Organization*, 35, 84–93.

[16] Daughety, A.F. & Reinganum, J.F. (1995): "Product safety: liability, R&D, and signaling," *The American Economic Review*, 1187–1206.

[17] Daughety, A.F. & Reinganum, J.F. (2005): "Secrecy and safety," *American Economic Review*, 95(4), 1074-1091.

[18] Daughety, A.F. & Reinganum, J.F. (2013): "Economic analysis of products liability: Theory," *Research handbook on the economics of torts*, 69–96.

[19] De Cornière, A. & Taylor, G. (2020): "A model of information security and competition," *TSE Working Paper*, 21-1285.

[20] Doğan, P. (2009): "Vertical networks, integration, and connectivity," *Journal of Economics & Management Strategy*, 18(2), 347–392.

[21] Doganoglu, T., and Wright, J. (2006). Multihoming and compatibility. International Journal of Industrial Organization, Volume 24, Issue 1, pp: 45-67.

[22] D'Silva, D., Filková, Z., Packer, F. & Tiwari, S. (2019): "The design of digital financial infrastructure: lessons from India," *BIS Paper*, 10.

[23] Duffie, D. and Younger, J. (2019): Cyber runs. Hutchins Center Working Paper 51, Brookings Institution.

[24] European Banking Authority (2019): "EBA guidelines on ICT and security risk management," *Internal Governance Final Report*, 04.

[25] Eisenbach, T., Kovner, A., Lee, M.J. (2022): Cyber risk and the US financial system: A pre-mortem analysis. Journal of Financial Economics. vol 145 (3), 802-826.

[26] Federal Reserve System, Federal Deposit Insurance Corporation, & Comptroller of the Currency (2021): "Proposed Interagency Guidance on Third-Party Relationships: Risk Management," *US Federal Register*, 15308.

[27] Foros, Ø. & Hansen, B., (2001): "Competition and compatibility among Internet service providers," *Information Economics and Policy*, 13(4), 411–425.

[28] Foros, Ø., Hansen, B. Vergé, T. (2023): Co-operative investment by downstream rivals: network sharing in telecom markets. Journal of Regulatory Econonomics 64, 34–47.

[29] Financial Stability Board (2019): "Third-party dependencies in cloud services: considerations on financial stability implications," *FSB Publication*, 9.

[30] Gal-Or, E., Ghose, A. (2005). The Economic Incentives for Sharing Security Information. Information Systems Research 16, no. 2: 186–208. http://www.jstor.org/stable/23015911.

[31] Garratt, R. & Schilling, L. (2022): "Optimal Data Security with Redundancies," *Working Paper SSRN*, 4138065. doi:10.2139/ssrn.4138065

[33] Gordon, L. A.; Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security. 5 (4): 438–457.

[33] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. Journal of Accounting and Public Policy, 22, 461-485.

[34] Grabowski, M. (2021): "Legal Aspects of "White-Label" Banking in the European, Polish and German Law. *Journal of Risk and Financial Management*, 14(6), 280.

[35] Hirshleifer, J. (1983). From weakest-link to best-shot: The voluntary provision of public goods. Public Choice 41(3), 371-386.

[36] Horvath, V., Klaver, M., Roosendaal, A., Cave, J., & Robinson, N. (2014): "Data and security breaches and cyber-security strategies in the EU and its international counterparts," *EU Publications Office*.

[37] House of Commons Treasury Committee (2019). "IT failures in the financial services sector.," *Second Report of Session*, 2019–20.

[38] Hylton, Keith N. and Haizhen Lin, H. 2014. Innovation and optimal punishment, with antitrust applications. Journal of Competition Law & Economics, Volume 10, Issue 1, March 2014, Pages 1–25.

[39] International Data Corporation (2018): "Worldwide Public Cloud Services Spending Forecast to Reach $160 Billion This Year, According to IDC," *Business Wire.*

[40] Inderst, R. & Peitz, M. (2012): "Market asymmetries and investments in next generation access networks," *Review of Network Economics*, 11(1).

[41] Jacob, J. & Lovat, B. (2016): "Multiple tortfeasors in high risk industries: how to share liability?," *BETA Working Paper*, 35.

[42] Jullien, B. and Lefouili, Y. and Riordan, M. H., Privacy Protection, Security, and Consumer Retention (June 1, 2020). Available at SSRN: https://ssrn.com/abstract=3655040.

[43] Kahn, C.M. & Roberds, W. (2008): "Credit and identity theft," *Journal of Monetary Economics*, 55(2), 251–264.

[44] Kahn, C.M., Rivadeneyra, F. & Wong, T.N. (2020): "Eggs in one basket: security and convenience of digital currencies," *FRB St. Louis Working Paper*, 2020-032.

[45] Kashyap, A.K. and Wetherilt, A. (2019): Some Principles for regulating cyber risk. AEA Papers and Proceedings 109, 482-87.

[49] Malueg, D.A. & Schwartz, M. (2006): "Compatibility incentives of a large network facing multiple rivals," *The Journal of Industrial Economics*, 54(4), 527–567.

[47] Lam, W.M.W. (2016): "Attack-prevention and damage-control investments in cybersecurity," *Information Economics and Policy*, 37, 42–51.

[48] Lam, W.M.W. and Seifert, J. (2023), Regulating Data Privacy and Cybersecurity. Journal of Industrial Economics, 71: 143-175.

[49] Malueg, D.A. and Schwartz, M. (2006). Compatibility Incentives of a Large Network Facing Multiple Rivals. The Journal of Industrial Economics, 54: 527-567.

[50] Matutes, C. & Padilla, A.J. (1994): "Shared ATM networks and banking competition," *European Economic Review*, 38(5), 1113–1138.

[51] Reserve Bank of New Zeland (2020): "Risk management guidance on cyber resilience and views on information gathering and sharing," *Consultation Paper.*

[52] Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S. & Hopkins, P.P. (2011): "The cloud: understanding the security, privacy and trust challenges," *RAND Corporation.*

[54] Rochet, J.C. (2003): "The theory of interchange fees: a synthesis of recent contributions," *Review of Network Economics*, 2(2).

[54] Rochet, J.C., Vives, X. (2004): "Coordination Failures and the Lender of Last Resort: Was Bagehot Right after All?," Journal of the European Economic Association, Volume 2, Issue 6, pp. 1116–1147.

[55] Southwell, A.H., Vandevelde, E., Bergsieker, R. & Bisnar Maute, J. (2017): "Gibson Dunn Reviews US Cybersecurity and Data Privacy," *The CLS Blue Sky Blog (Columbia Law School).*

[56] Stadler, M., Trexler, C.T. & Unsorg, M. (2022): "The perpetual trouble with network products: why IT firms choose partial compatibility," *Networks and Spatial Economics*, 1–11.

[57] Valletti, T.M. & Cambini, C. (2005): "Investments and network competition," *RAND Journal of Economics*, 446–467.

[58] Verdier, M., (2011): "Interchange fees in payment card systems: a survey of the literature," *Journal of Economic Surveys*, 25(2), 273–297.

Appendix

Appendix A: the social planer's decisions

Appendix A.1: proof of Proposition 1 - Welfare-maximizing investments

Social welfare $W(z)$ is the sum of depositor surplus, the banks' profits and the cloud service provider's profit, where $z \in \{0, 1\}$ represents banks' symmetric outsourcing decisions. This function neither depends on deposit prices nor access fees, which are transfers between players. The social planner maximizes

$$W(z) = u_0 + \frac{\beta(1+z)}{2} - \frac{t}{4} - h(s_i(z))L(z) - k_b s_i^2 - \frac{z k_c s_c^2}{2}. \tag{15}$$

Since banks have identical costs, the social planner chooses symmetric levels of security investments for both banks $s_b^w(z)$ given by

$$s_b^w(0) = \frac{\sigma l}{2k_b} \tag{16}$$

and

$$s_b^w(1) = \theta\alpha s_b^w(0).$$

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

$$s_c^w = \frac{\alpha}{\kappa}(1-\theta)s_b^w(0),$$

with $\kappa = k_c/2k_b$. Since a bank and the cloud service provider contribute respectively in share θ and $1-\theta$ to payment system security with cloud outsourcing, the total security of the payment system $s^w(z)$ is such that $s^w(0) = s_b^w(0)$ and

$$s^w(1) = \alpha(\theta^2 + \frac{(1-\theta)^2}{\kappa})s^w(0). \tag{17}$$

From Eq.(17), we have $s^w(1) \geq s^w(0)$ if and only if $\theta^2\alpha \geq 1$ or if $\theta^2\alpha < 1$ and

$$\kappa \leq \kappa_s \equiv \frac{(1-\theta)^2\alpha}{1-\theta^2\alpha},$$

where $\kappa_s \geq 0$. This completes the proof of Proposition 1.

Appendix A.2: proof of Proposition 2 - Welfare-maximizing outsourcing decisions

Social welfare increases if both banks join the cloud and become compatible if and only if $W(1) > W(0)$. Replacing for $s_b^w(0)$, $s_b^w(1)$ and $s_c^w(1)$ given in Eq.(16) into $W(z)$ given in Eq.(15), this happens if and only if $\beta > \max\{0, \beta_w\}$, with

$$\beta_w = 2(v(\alpha-1)l - \frac{(\sigma l)^2}{4\kappa k_b}((\alpha(1-\theta))^2 + \kappa(\theta\alpha^2 - 1))), \tag{18}$$

where $\beta_w \equiv 2(\Delta L_w + \Delta C_w)$. This completes the proof of Proposition 2.

If $\beta_w < 0$, cloud outsourcing increases welfare for any level of network effects. Solving for κ in Eq.(18), we have that $\beta_w < 0$ if and only if $\kappa < \kappa_w$, where

$$\kappa_w \equiv \frac{\sigma^2(1-\theta)^2\alpha^2 l^2}{4vk_b(\alpha-1)l - \sigma^2 l^2(\alpha^2\theta^2 - 1)} > 0.$$

Note that $\kappa_w > 0$ from Assumption (A1) and $h > \sigma$. Rearranging this expression with $C_b(s_b^w(0)) \equiv (\sigma l)^2/(4k_b)$ gives

$$\kappa_w = \frac{(1-\theta)^2\alpha^2 C_b(s_b^w(0))}{(1-\alpha^2\theta^2)C_b(s_b^w(0)) + (\alpha-1)vl}.$$

Factorizing by $\kappa_s = (1-\theta^2\alpha)/(1-\theta)^2\alpha$ and assuming that $\alpha\theta^2 \neq 1$ gives

$$\kappa_w = \kappa_s \frac{(1-\alpha\theta^2)\alpha C_b(s_b^w(0))}{(1-\alpha\theta^2)\alpha C_b(s_b^w(0)) + (\alpha-1)(vl - C_b(s_b^w(0)))},$$

with $vl > C_b(s_b^w(0))$ from Assumption (A1) and $v > \sigma$. Therefore, if $\kappa_s > 0$ and $\alpha > 1$, we have $\kappa_w < \kappa_s$. If $\alpha = 1$, we have $\kappa_w = \kappa_s$. This proves the additional remark after Proposition 2.

Appendix B: bank prices

We denote by $Z = (z_i, z_j, \gamma)$ the vector representing banks' decisions to join the cloud and become compatible, where $z_i = 1$ if bank $i \in \{A, B\}$ joins the cloud and $\gamma = 1$ if they become compatible (resp., $\gamma = 0$ without compatibility). Following the notations of the paper, we have $z = z_i = z_j = 1$ if both banks join the cloud and become compatible, and $z = z_i = z_j = 0$ if banks do not join the cloud.

At the equilibrium, depositors' expectations are fulfilled and each bank $i \in \{A, B\}$ faces a total demand $N_i(Z)$ equal to

$$N_i(Z) = \frac{1}{2} + \frac{p_j - p_i - \mu h_i L_d(z_i) + \mu h_j L_d(z_j)}{2\tau(z, \beta)}, \tag{19}$$

At the competition stage, each bank i chooses p_i to maximize

$$\pi_i(f^a, f^c, Z) = (p_i - z_i f^a - h_i L_b(z_i))N_i(Z) - \gamma f^c - C_b(s_i). \tag{20}$$

Solving for the first-order conditions of banks' profit maximization gives

$$p_i^*(Z) = \tau(z, \beta) + h_i L_b(z_i) + \frac{(2z_i + z_j)f^a}{3} - \frac{h_i \rho_b(z_i) - h_j \rho_b(z_j)}{3}. \tag{21}$$

Replacing for $p_i^*(Z)$ and $p_j^*(Z)$ into Eq.(20), each bank $i \in \{A, B\}$ makes profit

$$\pi_i(f^a, f^c, Z) = \frac{(\tau(z, \beta) - ((z_i - z_j)f^a + h_i \rho_b(z_i) - h_j \rho_b(z_j))/3)^2}{2\tau(z, \beta)} - \gamma f^c - C_b(s_i). \tag{22}$$

If banks make symmetric outsourcing decisions, the access fee f^a does not impact their equilibrium profits. To simplify the notations, when possible, we refer to banks' profits in subgame c where $Z = (1, 1, 1)$ by

$$\pi_i(f^a, f^c, Z) = \pi_i(f^c, 1),$$

and the number of consumers who join bank i by $N_i(1)$.

In addition, we denote banks' profits in subgame n where $Z = (0, 0, 0)$ by

$$\pi_i(f^a, f^c, Z) = \pi_i(0),$$

and the number of consumers who join bank i by $N_i(0)$.

If banks join the cloud but do not become compatible, we have $Z = (1, 1, 0)$. In that case, banks' profits do not depend on the compatibility fee and we denote them by

$$\pi_i(f^a, f^c, Z) = \pi_i(\overline{c}),$$

and the number of consumers who join bank i by $N_i(\overline{c})$.

If only bank j joins the cloud, we have $Z = (0, 1, 0)$. In that case, banks' profits do not depend on the compatibility fee. We denote bank i's profit when its competitor joins the cloud by

$$\pi_i(f^a, f^c, Z) = \pi_i(f^a, \overline{c}_i),$$

and the number of consumers who join bank i by $N_i(\overline{c}_i)$.

Appendix C: proof of Lemma 1 - cloud fees

The cloud service provider chooses the fees f^a and f^c that maximize its profit, which equals $\pi_C^c(f^c, 1)$ given in Eq.(4) if both banks join the cloud and become compatible, and $\pi_C^o(f^a, \overline{c}_i)$ in Eq.(5) if only bank j joins the cloud.

Case 1: Both banks join the cloud: If both banks A and B store their payment transactions 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 $\pi_C^c(f^c, f^a, 1)$ given in Eq.(4), under the constraint that both banks prefer to be compatible. Therefore, the maximization problem of the cloud service provider is equivalent to:

$$\begin{aligned} \max_{f^c,\, f^a} \quad & 2f^c + f^a \\ \text{s.t.} \quad & \pi_i(f^c, 1) \geq \pi_i(\overline{c}) \qquad \text{for i=\{A,B\}} && \text{(C1a)} \\ & \pi_i(f^c, 1) \geq \pi_i(f^a, \overline{c}_i) \quad \text{for i=\{A,B\}} && \text{(C2a)} \\ & \pi_C^c(f^c, f^a, 1) \geq 0. && \text{(C3a)} \end{aligned}$$

The constraints can be interpreted 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, banks may deviate by not using the compatibility service if their rival wants to use it and both banks join the cloud (constraints C1a). Second, each bank may deviate by remaining independent if its rival joins the cloud (constraints C2a). Finally, condition (C3a) states that the cloud service provider makes a positive profit.

Replacing for $\pi_i(f^c, 1)$ and $\pi_i(\overline{c})$ defined above into (C1a), we find that the constraints (C1a) are equivalent to $f^c \leq f^{c*}$, where

$$f^{c*} \equiv \frac{\beta}{2}\left(1 - \frac{(\Delta h(1)\rho_b(1)/3)^2}{t\tau(1,\beta)}\right). \tag{24}$$

Since $\pi_C^c(f^c, f^a, 1)$ is increasing with f^c, the cloud service provider chooses the compatibility fee f^{c*} such that both banks join the cloud.

Replacing $\pi_i(f^{c*}, 1) = \pi_i(\overline{c})$ and $\pi_i(f^a, \overline{c}_i)$ into (C2a), we find that the constraint (C2a) is equivalent to $(f_i^{a*} - f^a)(f^a + \tau_1) \geq 0$, with

$$f_i^{a*} = h_i^n \rho_b(0) - h_i^c \rho_b(1),$$

and $\tau_1 \equiv 6(t-\beta) - h_i^c\rho_b(1) + 2h_j^c\rho_b(1) + h_i^n\rho_b(0)$. From Assumption (A1), we have that $\tau_1 \geq 0$ and $\tau_1 \geq f_i^{a*}$. Therefore, the constraint (C2a) is satisfied if and only if $f^a \in (-\tau_1, f_i^{a*})$. Since $\pi_C^c(f^c, f^a, 1)$ is increasing with f^a, the cloud service provider 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 $h^n(s_i) = v - \sigma s_i$ and $h^c(s_i, s_c) = v - \sigma(\theta s_i + (1-\theta)s_c)$ in f_A^{a*} and f_B^{a*}, we find that $f_B^{a*} \geq f_A^{a*}$ is equivalent to

$$(s_A - s_B)(\rho_b(0) - \theta\rho_b(1)) \geq 0. \tag{25}$$

To conclude, if $s_A \geq s_B$, the cloud service provider chooses an access fee equal to f_A^{a*} (resp., f_B^{a*}) if $\theta\rho_b(1) \leq \rho_b(0)$ (resp., < 0) and $\pi_C^c(f^{c*}, f_A^{a*}, 1) \geq 0$. Otherwise, if $\pi_C^c(f^{c*}, f_A^{a*}, 1) < 0$, it does not serve both banks.

Case 2: only bank B joins the cloud: If only bank B joins the cloud, the cloud service provider chooses the access fee f^a that maximizes its profit $\pi_C^o(f^a, \overline{c}_A)$ given by Eq.(5), under the constraint that no bank deviates from the situation in which only bank B joins the cloud. The maximization problem of the cloud service provider is

$$\begin{aligned} \max_{f^a} \quad & \pi_C^o(f^a, \overline{c}_A) \\ \text{s.t.} \quad & \pi_B(f^a, \overline{c}_A) \geq \pi_B(0) && \text{(C1b)} \\ & \pi_A(f^a, \overline{c}_A) \geq \pi_A(\overline{c}) && \text{(C2b)} \\ & \pi_C^o(f^a, \overline{c}_A) \geq 0. && \text{(C3b)} \end{aligned}$$

The constraints are interpreted as follows. If bank A does not join the cloud, bank B can deviate by refusing to join the cloud as well, such that both banks are independent (constraint C1b). Second, bank A can deviate by joining the cloud too without becoming compatible (constraints C2b). Indeed, bank A never buys the compatibility service when bank B does not buy it. Third, the cloud service provider must make a positive profit (constraint C3b).

Following the analysis of the constraint (C2a) in Case A, since from constraint (C1a) $\pi_A(f^{c*}, 1) = \pi_A(f^a, \overline{c})$, we conclude that the constraint (C2b) is equivalent to $f^a \leq f_B^{a*}$, with $f_B^{a*} = h_B^n\rho_b(0) - h_B^c\rho_b(1)$. In addition, the constraint (C1b) is equivalent to $f^a \geq f_A^{a*}$.

We now determine the maximum of $\pi_C^o(f^a, \overline{c}_A)$ with respect to f^a and show that the constraint (C1b) is binding. Differentiating $\pi_C^o(f^a, \overline{c}_A)$ with respect to f^a, we find that $\partial \pi_C^o / \partial f^a = (f_m^a - f^a)/(3(t-\beta))$, with

$$f_m^a \equiv \frac{3(t-\beta) + h_B^c L_c(1) - h_B^c \rho_b(1) + h_A^n \rho_b(0)}{2}.$$

Since π_C^o is concave in f^a, this function reaches a maximum at $f^a = f_m^a$. From Assumption (A1), we have $f_m^a - f_B^{a*} \geq 3(t-\beta)/2 - h_B \rho_b(0) \geq 0$. Therefore, the constraint (C1b) is binding. The constraints (C1b) and (C2b) imply that the cloud service provider sets an access fee equal to $f^{a*} = f_B^{a*}$ if $f_B^{a*} \geq f_A^{a*}$ and if constraint (C3b) holds. From the analysis conducted in Case A of this appendix, this is equivalent to $s_B < s_A$ if $\rho_b(0) > \theta \rho_b(1)$, and $s_B \geq s_A$ otherwise. If constraint (C3b) is not satisfied, the cloud service provider never prefers to serve one bank rather than two banks.

We now show that from the constraint (C3b), it must be that $s_B < s_A$. A necessary condition for condition (C3b) to hold is that $f^{a*} = f_B^{a*} > 0$. We have $f_B^{a*} = h_B^n \rho_b(0) - h_B^c \rho_b(1)$, which is decreasing with h_B^c, and therefore increasing with s_c. Since $s_c \leq v/\sigma$, we have

$$f_i^{a*} \leq f_B^{a*}|_{s_c = v/\sigma} = (v - \sigma s_B)(\rho_b(0) - \theta \rho_b(1)).$$

If $\rho_b(0) < \theta \rho_b(1)$, we have $f_B^{a*}|_{s_c = v/\sigma} < 0$, which implies that $f_B^{a*} < 0$. Therefore, if $\rho_b(0) < \theta \rho_b(1)$, the cloud service provider cannot make a positive profit by only serving bank B.

To conclude, from Eq.(25), if $\rho_b(0) > \theta \rho_b(1)$ and (C3b) holds, the cloud service provider sets an access fee equal to f_B^{a*} when only bank B joins the cloud, with $s_B < s_A$. Otherwise, it does not only serve one bank.

Appendix D: proof of Proposition 3 - Cloud service provider entry

We are now able to determine the number of banks that the cloud service provider prefers to serve at the equilibrium of stage 3. If $\rho_b(0) < \theta \rho_b(1)$, the cloud service provider always prefers to serve both banks when it makes a positive profit. If $\rho_b(0) \geq \theta \rho_b(1)$, the cloud service provider faces a non-trivial trade-off between serving both banks or the sole bank B. 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 only serves bank B.

Suppose that the cloud service provider only serves bank B. We start by determining the cloud service provider's profit. Replacing p_A and p_B given

in Eq.(21) into $N_B(\overline{c}_A)$ gives

$$N_B(\overline{c}_A) = \frac{t - \beta - (f_B^{a*} + h_B^c \rho_b(1) - h_A^n \rho_b(0))/3}{2(t-\beta)}.$$

Since $f_B^{a*} = h_B^n \rho_b(0) - h_B^c \rho_b(1)$, we have that $N_B(\overline{c}_A) = N_B(0)$. Therefore, the cloud service provider's profit of only serving bank B equals

$$\pi_C^o(\overline{c}_A) = \Phi(\overline{c}_A) N_B(0) - C_c(s_c),$$

where

$$\Phi(\overline{c}_A) = f_B^{a*} - h_B L_c(1)$$

denotes the cloud service provider's margin, which must be positive whenever serving a single bank may be profitable.

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

$$\pi_C^c(f^{c*}, f_A^{a*}, 1) = 2f^{c*} + f_A^{a*} - h_B^c L_c(1) + (h_B^c - h_A^c) L_c(1) N_A(1) - C_c(s_c),$$

with $f_A^{a*} = h_A^n \rho_b(0) - h_A^c \rho_b(1)$. Replacing for $\Phi(\overline{c}_A) = f_B^{a*} - h_B^c L_c(1)$, since $h_B^c - h_A^c = \theta(h_B^n - h_A^n)$, the cloud service provider's profit of serving both banks is given by

$$\pi_C(1) = \Phi(\overline{c}_A) + \Phi(1) - C_c(s_c),$$

where

$$\Phi(1) \equiv 2f^{c*} - (f_B^{a*} - f_A^{a*}) + \theta(h_B^n - h_A^n) N_A(1) L_c(1), \tag{27}$$

and $f_B^{a*} - f_A^{a*} = \theta(h_B^n - h_A^n)(\rho_b(0) - \theta\rho_b(1))$. For the cloud service provider to make a positive profit when it serves both banks, it must be that $\Phi(\overline{c}_A) \geq -\Phi(1)$. The cloud service provider's profit is higher when it serves both banks than when it serves only bank B if and only if $\pi_C(1) \geq \pi_C(\overline{c}_A)$, which is equivalent to

$$\Phi(1) + N_A(0)\Phi(\overline{c}_A) \geq 0.$$

If $\Phi(1) \geq 0$, since $N_A(0)\Phi(\overline{c}_A) \geq 0$, the cloud service provider makes a higher profit when it serves both banks than when it only serves bank B. This is in particular the case if banks invest the same amount of security at stage 2. Therefore, no bank joins the cloud alone if banks invest the same amount of security at stage 2.

If $\Phi(1) < 0$, the cloud service provider prefers to serve only one bank if and only if $\Phi(1) + N_A(0)\Phi(\overline{c}_A) < 0$. It is sufficient to show that it is possible to have $\Phi(1) < 0$ and $\Phi(1) + N_A(0)\Phi(\overline{c}_A) < 0$. Since

$$\Phi(1)|_{\beta=0} = \theta N_A(1) L_c(1) - \rho_b(0) + \theta \rho_b(1),$$

if θ is close to zero, we have $\Phi(1)|_{\beta=0} < 0$. This implies that $\Phi(1)$ may sometimes be negative. If $L_c = 0$ and $\beta = 0$, we have

$$\Phi(1) + N_A(0)\Phi(\overline{c}_A) = -(1 - N_A(0)) f_B^{a*} < 0.$$

Therefore, it is possible to have $\Phi(1) < 0$ and $\Phi(1) + N_A(0)\Phi(\overline{c}_A) < 0$. In that case, the cloud service provider makes a higher profit by serving a single bank.

To summarize, the cloud service provider chooses to enter the market if and only if $\max\{\pi_C^o(\overline{c}_A), \pi_C^c(1)\} > 0$. It only serves bank B if $\Phi(1) + N_A(0)\Phi(\overline{c}_A) < 0$ and $\pi_C^o(\overline{c}_A) > 0$. It serves both banks if $\pi_C^c(1) > 0$ and $\Phi(1) + N_A(0)\Phi(\overline{c}_A) > 0$.

If banks invest symmetric amounts in security, we have $\pi_C^c(1) > 0$ and $\pi_C^o(\overline{c}_A) > 0$ if and only if $\beta > \widehat{\beta}$, where

$$\widehat{\beta} \equiv h^c \rho_c(1) - h^n \rho_b(0) + C_c(s_c). \tag{28}$$

This completes the proof of Proposition 3.

Appendix E: proof of Proposition 4 - Comparison of private outsourcing decisions to the first-best

Replacing for $s_b^*(1)$ and s_c^* given in Eq.(12) and Eq.(13) into Eq.(14), we find that

$$\beta^w = 2(L(1) - L(0)) - \frac{\sigma^2}{2k_c}(\theta^2 L(1)^2 - L(0)^2 + \frac{(1-\theta)^2 L(1)^2}{\kappa}) \tag{29}$$

and

$$\widehat{\beta} = v(\rho_c(1) - \rho_b(0)) - \frac{\sigma^2}{k_c}(\frac{\theta(\theta\rho_c(1) - \rho_b(0))}{3} + \frac{(1-\theta)^2 \rho_c(1)^2}{4\kappa}). \tag{30}$$

The difference between β^w and $\widehat{\beta}$ may either be positive or negative. To illustrate why, we assume that banks fully internalize the damage. Replacing for $\rho_c(1) = \rho_b(1) = L(1) = \alpha l$ and $\rho_b(0) = l$ into $\widehat{\beta}$ in Eq.(30), we find that

$$\beta^w - 2\widehat{\beta} = \frac{\sigma^2 l^2}{2k_b}(1 - \theta\alpha)^2 > 0.$$

This implies that there is over-outsourcing, because the cloud service provider does not internalize the effect of its entry decision on banks' investment costs.

In contrast, suppose that the cloud service provider cannot extract revenues from access. Replacing for $\rho_c(1) = \rho_b(0) = l$, $\rho_b(1) = 0$, and setting $L(1) = L(0)$ into β^w given in Eq.(29) and into $\widehat{\beta}$ in Eq.(30), we find that

$$\beta^w - \widehat{\beta} = -\frac{\sigma^2 l^2}{4k_b\kappa}(2\kappa(\theta^2 - 1) + (1-\theta)^2).$$

This expression is negative if κ sufficiently low, that is, if there are sufficient efficiency gains in the first-best with cloud outsourcing. In this case, banks under-invest in security compared to the first-best and the cloud service provider cannot take advantage of this situation by raising the access fee, which reduces its incentives to enter the market. In that case, there is under-outsourcing. This completes the proof of Proposition 4.

Appendix F: proof of Proposition 5 - Depositor surplus

With symmetric outsourcing decisions (that is, if $z \in \{0, 1\}$), banks invest the same amount of security $s_b(z)$. Therefore, each bank obtains half of the market, and their outsourcing decisions have no impact on the depositors' transportation costs. Moreover, in that case, the access fee f_i^{a*} given in Eq.(10) is equal to $f_j^{a*} = f^{a*}$.

Given that only a proportion μ of depositors are sophisticated, the average expected depositor surplus $DS(z)$ equals $u(1/2) - \mu h^k L_d(z)$, where $u(1/2)$ is given by Eq.(1) and $k = n$ or $k = c$, respectively, if outsourcing decisions are symmetric. Replacing for p_i^* given in Eq.(7), the average expected depositor surplus equals

$$DS(z) = u_0 - \tau(0) + (1-z)\frac{\beta}{2} - h^k\rho_b(z) - zf^{a*}, \tag{31}$$

with $f^{a*} = h(s_b(1))\rho_b(0) - h(\theta s_b(1) + (1-\theta)s_c)\rho_b(1)$ given in Eq.(10). Therefore, depositor surplus increases when both banks join the cloud and become compatible if and only if $DS(1)) - DS(0) \geq 0$, where

$$DS(1) - DS(0) = \frac{-\beta}{2} + (h(s_b(0)) - h(s_b(1)))\rho_b(0).$$

Replacing for $h(s_b(z)) = v - \sigma s_b(z)$, depositor surplus is higher when banks join the cloud and become compatible if and only if $\beta/2 \leq \sigma\rho_b(0)(s_b(1) - s_b(0))$, and it is lower otherwise. This completes the proof of Proposition 5.

Appendix G: proof of Lemma 2 - security investments

The first-order conditions: For $i \in \{A, B\}$ and $j \neq i$, we denote by $\tilde{p}_i^*$ and by $\tilde{\pi}_i^*(s_i, s_j)$ 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 with respect to s_i gives

$$\frac{\partial \tilde{\pi}_i^*}{\partial s_i} = \frac{\partial \pi_i}{\partial s_i} + \frac{\partial \pi_i}{\partial p_j}\frac{\partial \tilde{p}_j^*}{\partial s_i} + \frac{\partial \pi_i}{\partial f_a}\frac{\partial f^{a*}}{\partial s_i} + \frac{\partial \pi_i}{\partial f_c}\frac{\partial f^{c*}}{\partial s_i} = 0. \tag{32}$$

From Appendix C - Case B, if only bank B outsources, the cloud service provider can only set $f^a = f_B^{a*}$ such that $\pi_B(f^a, \overline{c}_A) = \pi_B(0)$, which implies that $\pi_A(f^a, \overline{c}_A) = \pi_A(0)$. Therefore, it is sufficient to study banks' investments decisions when they set symmetric outsourcing decisions.

In Eq.(32), 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.(32), the profit-maximizing levels of security are given by

$$\sigma\theta\frac{\rho_b(z)}{3}(1 - \frac{\rho_b(z)\Delta h(z)}{3\tau(0,\beta)}) = k_b s_i(z) \tag{33}$$

where $\Delta h(z) = h(s_i(z)) - h(s_{-i}(z))$. Solving for $s_i(z)$, since $\Delta h(z) = 0$ in a symmetric equilibrium, we obtain the profit-maximizing levels of investment in security given in Lemma 2, which we denote by $s_A^*(z) = s_B^*(z) = s_b^*(z)$. We proceed by showing that the subgame in which banks choose their security investments admits a unique Nash equilibrium which is symmetric.

Case 1: interior solution for bank j If there exists a Nash equilibrium such that both banks choose interior solutions for security investments, banks' best responses are given by Eq.(33). Since banks' costs functions are identical, banks' best responses are symmetric and given by

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

The solution is interior if and only if $h(s_i^*(z)) \in (0, \overline{h})$.

Since $s_c \leq v/\sigma$, this is equivalent to $s_i^*(1) \in (0, v/\sigma)$. If both banks join the cloud (i.e., $z = 1$), we have $s_i^*(1) = \sigma\theta\rho_b(1)/3k_b > 0$ from Eq.(12).

Moreover, since $\theta \in (0,1)$ and $0 < \sigma < v$, we have $\sigma\theta < v$. This implies that $(\sigma/\overline{h})s_i^*(1) < (\sigma/v)v\rho_b(1)/3k_b$. The right-hand term of this inequality is always lower than 1 from Assumptions (A1) and $\sigma/v < 1$. Therefore, we conclude that $s_i^*(1) < v/\sigma$.

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

Case 2: minimum investment of bank j. Suppose that bank j chooses not to invest in cyber-security (i.e., it chooses $s_j = 0$). Replacing for $\Delta h(z)$ if bank i invests s_i and bank j invests 0, the optimal investment of bank i, denoted by $s_i^m(z)$ in this case, is given by

$$s_i^m(z) = \frac{3\sigma\theta\rho_b(z)\tau(0,\beta)}{9k\tau(0,\beta) - (\sigma\theta\rho_b(z))^2},$$

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

Case 3: maximum investment of bank j. Suppose that bank j chooses a maximum level of investment in cyber-security (i.e., $s_j = v/\sigma$). Replacing for $\Delta h(z)$ if bank i invests s_i and bank j invests v/σ in Eq.(33), the optimal investment of bank i, denoted $s_i^M(z)$ in this case, is given by

$$s_i^M(z) = \frac{\sigma\theta\rho_b(z)(3\tau(0,\beta) - \theta h\rho_b(z))}{9k\tau(0,\beta) - (\sigma\theta\rho_b(z))^2} \ ,$$

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 $s_i^M \in (0, v/\sigma)$. Therefore, from Case A, the best response of bank j consists in choosing an interior solution for its security investment. Since $d\pi_j/ds_j|_{(s_i=s_i^M, s_j=v/\sigma)} < 0$, bank j has an incentive to deviate from the strategy $s_j = v/\sigma$, and the pair

of strategies ($s_i = s_i^M, s_j = v/\sigma$) does not constitute a Nash equilibrium. By symmetry, the pair of strategies ($s_i = v/\sigma, s_j = s_i^M$) 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 $s_b^*(z)$ in Eq.(12).

Appendix H: comparative statics

Appendix H.1: comparative statics with respect to μ

Since β^w is independent of μ, the difference $\beta^w - \widehat{\beta}$ is decreasing with μ the proportion of sophisticated depositors if and only if $\partial\widehat{\beta}/\partial\mu > 0$. Taking the total derivative of Eq.(14) with respect to μ gives

$$\frac{d\widehat{\beta}}{d\mu} = \frac{\partial\widehat{\beta}}{\partial\mu} + \frac{\partial\widehat{\beta}}{\partial s_c}\frac{\partial s_c^*}{\partial\mu} + \frac{\partial\widehat{\beta}}{\partial s_b}\frac{\partial s_b^*(1)}{\partial\mu}.$$

From the envelope theorem, the second term of this equation is null at $s_c = s_c^*$. Since $\partial s_b^*(1)/\partial\mu = \sigma\theta L_d(1)/(3k_b)$ from Eq.(12), at $s_c = s_c^*$ and $s_b = s_b^*(1)$, we have that

$$\frac{d\widehat{\beta}}{d\mu} = h(\theta s_b^*(1) + (1-\theta)s_c^*)L_d(1) - h(s_b^*(1))L_d(0) + \frac{\sigma^2\theta L_d(1)}{3k_b}(\rho_b(0) - \theta\rho_c(1)).$$

The first effect corresponds to the direct effect and is positive if cloud outsourcing increases the expected loss. Therefore, with exogenous investments in security, a higher proportion of sophisticated depositors decreases $\beta^w - \widehat{\beta}$ (and thus, reduces the over-outsourcing) if cloud outsourcing increases the expected loss of depositors. With endogenous investments in security, there is an indirect effect which is positive if $\rho_b(0) - \theta\rho_c(1) > 0$ and negative otherwise. If $\rho_b(0) - \theta\rho_c(1) > 0$, when banks increase their investments in security, this reduces the cloud service provider's incentives to enter the market.

Both effects may either be positive or negative. For instance, if the realized damage of depositors is independent of outsourcing (i.e., $L_d(1) = L_d(0)$), the direct effect is positive if $2\theta\kappa\rho_b(1) - 3(1-\theta)\rho_c(1) > 0$, and the indirect effect is positive if $\rho_b(0) - \theta\rho_c(1) > 0$. Also, if $(2\theta\kappa)\rho_b(1) - 3(1-\theta)\rho_c(1) < (2\kappa\theta/(1-\theta))(\theta\rho_c(1) - \rho_b(0))$, the indirect effect outweighs any positive direct effect.

Appendix H.2: comparative statics with respect to θ

The total derivatives of β^w and $\widehat{\beta}$ with respect to θ are the sum of a direct

effect (θ impacts the sharing of security investments) and an indirect effect that goes through the choice of security investments.

The total derivative of β^w with respect to θ corresponds only to the direct effect, because the socially optimal levels of security are chosen to maximize social welfare, which equals $\beta - \beta^w$. The direct effect is given by

$$\frac{d\beta^w}{d\theta} = \frac{\theta\sigma^2 L(1)^2}{\kappa k_b}(\frac{1-\theta}{\theta} - \kappa), \tag{34}$$

and it is positive if and only if $\theta < 1/(1+\kappa)$. Therefore, β^w increases with θ if and only if the relative contribution of the cloud service provider $(1-\theta)/\theta$ is higher than its relative efficiency κ.

The total derivative of $\widehat{\beta}$ with respect to θ is the sum of a direct effect and the indirect effect of θ on banks' investment in security. The effect that goes through the cloud service provider's investment is null, because the optimal level of cloud security is chosen to maximize the cloud service provider's profit, which equals $\beta - \widehat{\beta}$. The total derivative of $\widehat{\beta}$ with respect to θ is given by:

$$\frac{d\widehat{\beta}}{d\theta} = \frac{\theta\sigma^2\rho_c(1)^2}{2\kappa k_b}(\frac{1-\theta}{\theta} - \frac{2\rho_b(1)}{3\rho_c(1)}\kappa) - \frac{\sigma^2}{3k_b}(\theta\rho_c(1) - \rho_b(1)). \tag{35}$$

The direct effect is positive if and only if $\theta < 3\rho_c(1)/(3\rho_c(1) + 2\kappa\rho_b(1)) < 1$ (see the first term of (35)). We see that the direct effect is positive if and only if the relative contribution of the cloud service provider is higher than its relative efficiency, multiplied by the weight $2\rho_b(1)/(3\rho_c(1))$. This weight represents how investments in cyber security are shared between banks and the cloud service provider when banks choose their investments in security. Whenever this factor is greater than one, banks under-invest relatively more than the cloud service provider.

The indirect effect is positive if and only if $\theta < \rho_b(1)/\rho_c(1) < 1$ (see the second term of (35)). We conclude that for low values of θ, the total derivative of $\widehat{\beta}$ with respect to θ is positive. For high values of θ, the total derivative of $\widehat{\beta}$ with respect to θ is negative.

The resulting effect of a higher θ on the distortion between the private outsourcing decisions and the social optimum depends on the efficiency gains associated with cloud outsourcing. A higher θ has a direct effect and an indirect effect on the total derivative of $\beta^w - \widehat{\beta}$ with respect to θ. From

the analysis of (34) and (35), the direct effect of θ on the total derivative of $\beta^w - \widehat{\beta}$ is given by

$$\frac{\theta\sigma^2}{2k_b}(2(L(1)^2 - (\rho_c(1))^2)(\frac{1-\theta}{\theta\kappa} - 1) - (\rho_c(1))^2(1 - \frac{2\rho_b(1)}{3\rho_c(1)})),$$

and it is positive if and only if

$$\theta < \frac{1}{1+\kappa}(1 - \frac{\kappa\rho_c(1)(3\rho_c(1) - 2\rho_b(1))}{6(1+\kappa)L(1)^2 - \rho_c(1)(3\rho_c(1) + 2\kappa\rho_b(1))}).$$

The indirect effect of θ on the total derivative of $\beta^w - \widehat{\beta}$ is positive if and only if $\theta\rho_c(1) > \rho_b(1)$.

The resultant of the direct and the indirect effect depends on the efficiency gains associated with cloud outsourcing. We find that the total derivative of $\beta^w - \widehat{\beta}$ with respect to θ is decreasing with κ. It is close to infinity when κ is close to zero. Also, when κ is very high, it has the same sign as $-3L(1)^2 + \rho_c(1)\rho_b(1)$, which is negative since $L(1) > max\{\rho_c(1), \rho_b(1)\}$. Therefore, there exists $\widehat{\kappa}(\theta) > 0$ such that this function is positive if and only if $\kappa < \widehat{\kappa}(\theta)$. The direct effect is decreasing with κ and the indirect effect is independent of κ (more precisely of k_c).

Also, when θ close to 1, the total derivative of $\beta^w - \widehat{\beta}$ has the same sign as $-3L(1)^2 + \rho_b(1)(2\rho_c(1) - \rho_b(0))$, which is negative, and, when θ close to 0, it is positive if and only if $\kappa \leq 3(2L(1)^2 - \rho_c(1)^2)/2\rho_b(0)\rho_b(1)$.

Appendix I: proof of Propositions 6 - liability rules

Appendix I.1: the liability rules and the marginal costs

The liability regime impacts banks' marginal cost, which include internalization effects, that is, we have

$$\rho_b(1) = \alpha l_b + \eta_d + \eta_c - \gamma_b + \mu(\alpha l_d - \eta_d - \gamma_d).$$

If all depositors are sophisticated ($\mu = 1$), banks internalize perfectly the depositors' losses and pass on their marginal cost to the depositors through higher deposit prices. Therefore, the transfer to depositors η_d is neutral. If some depositors are naive, the banks internalize imperfectly the depositors' losses. Then, a higher transfer η_d increases their marginal cost, and therefore, their security investments. In contrast, higher compensations γ_b and γ_d from the cloud service provider reduce banks' investment incentives.

Similarly, the liability regime for cyber incidents impacts the cloud service provider's internalized marginal cost, that is, we have

$$\rho_c(1) = \alpha l_b + \eta_d + \gamma_d + \mu(\alpha l_d - \eta_d - \gamma_d).$$

The net compensation $\gamma_b - \eta_c$ given to the banks has no impact on the cloud service provider's marginal cost of cyber incidents, because it can be extracted through the access fee. If there is a positive proportion of naive depositors, the cloud service provider's investment can be increased by raising its transfer γ_d to depositors. Therefore, the compensations γ_b and γ_b are not equivalent instruments to increase the cloud service provider's investment incentives, because the banks and the depositors are not positioned at the same place in the vertical chain, respectively.

Appendix I.2: proof of Proposition 6

Replacing for

$$\rho_b(z) = L(z) - (1-\mu)L_d(z) - L_c(z)$$

into $s_b^*(z)$, $s_c^*(1)$ given in Eqs.(12)-(13) and $s_b^w(z)$ given in Proposition 1, we find that

$$3k_b \frac{s_b^w(z) - s_b^*(z)}{\sigma\theta} = \frac{L(z)}{2} + (1-\mu)L_d(z) + L_c(z), \tag{36}$$

with $\theta = 1$ if $z = 0$.

Replacing for $\rho_c(1) = \rho_b(1) + L_c(1)$ and $s_b^w(1)$ given in Proposition 1 gives

$$k_c \frac{s_c^w(1) - s_c^*(1)}{\sigma(1-\theta)} = (1-\mu)L_d(z). \tag{37}$$

We are now able to determine whether it is possible to find transfers such that banks' investments and the cloud service provider's investments are equal to their first-best levels of security investments.

Case 1: independent banks: Replacing for $z = 0$ and $L_c(0) = 0$ in Eq.(36), banks' investments in security are equal to their first-best levels of investment if and only if $\mu < 1$ and

$$\eta_d = l_d + \frac{l}{2(1-\mu)}.$$

Case 2: outsourcing banks: Replacing for $z = 1$, $L_d(1)$ and $L_c(1) \geq 0$ in Eqs.(36)-(37), firms' investments in security are equal to their first-best levels of investment if and only if we have

$$\eta_d + \gamma_d = \underline{\alpha} l_d,$$

and

$$\eta_c - \gamma_b - \gamma_d = \frac{\underline{\alpha} l}{2}.$$

Therefore, it is possible to find transfers that implement the first-best levels of security investments. However, since $\gamma_b + \gamma_d \geq 0$, this means that it is necessary that banks subsidize the cloud service provider, i.e., $\eta_c > 0$.

Appendix I.3: implementation of the first-best total level of security

The total level of security is equal to the first-best if and only if

$$\theta(s_b^w(1) - s_b^*(1)) + (1-\theta)(s_c^w(1) - s_c^*(1)) = 0,$$

which is equivalent to

$$\frac{\underline{\alpha} l}{2} + (1-\mu)(1 + \frac{3(1-\theta)^2}{2\kappa\theta^2})L_d(1) = -L_c(1).$$

If neither punitive damage nor subsidies are possible, we have $L_d(1) \geq 0$ and $L_c(1) \geq 0$. Therefore, it is not possible to find transfers to implement the first-best total level of payment system security.

If punitive damage are impossible, but subsidies are possible, the first-best total level of payment system security is implemented by subsidizing the cloud service provider, because it must be that $L_c(1) \leq 0$. Then, there exists a continuum of transfers which implement the first-best total level of security.

If punitive damage are possible, one possible liability regime consists of choosing $\gamma_d = 0$ and $\eta_d = \underline{\alpha}(l_d + l/2(1-\mu))$, such that banks offer depositors the optimal transfers under independence (adjusted for the higher damage $\underline{\alpha}$), and then $\gamma_b = 3\underline{\alpha} l(1-\theta)^2/4\kappa\theta^2 > 0$. Therefore, banks' under-investment when $\gamma_b > 0$ compensates for the extra damage internalized by the cloud service provider.

Therefore, if punitive damage are impossible, to implement the first-best total level of payment system security, it is necessary to subsidize the cloud

service provider. Otherwise, there exists a continuum of transfers that implement the first-best total level of payment system security. This completes the proof of Proposition 7.

Appendix J: Security standards

We denote by $h_w^c = h^c(s_c^w(1), s_b^w(1))$ and $h_w^n = h^n(s_b^w(0))$ the probability that a cyber incident occurs with first-best security investments. Similarly, let $h_b^c = h^c(s_c^*, s_b^*)$ the probability of that a cyber incident occurs with private security investments. From Eq.(18) Eq.(14), we have

$$\begin{aligned}\beta^w - \widehat{\beta} &= (2L-\rho_c)(1)h_w^c - (2L-\rho_b)(0)h_w^n + 2\Delta C_w - C_c(s_c^*(1)) \\ &\quad +(h^n(s_b^*(1)) - h_w^n)\rho_b(0) - (h_b^c - h_w^c)\rho_c(1). \end{aligned} \tag{38}$$

From Eq.(38), we can identify four biases in the entry decision of the cloud service provider. First, it under-estimates the benefits and costs of outsourcing on cyber-risk, because it over-values the benefits of compatibility and it internalizes too little damage with respect to the first-best. Second, it does not consider banks' investment costs. Third, firms' under-investment in security has an ambiguous effect on outsourcing, because both independent banks and outsourcing banks become more risky. Finally, it does not internalize the effect of outsourcing on banks' investments.[64]

If firms comply with security standards, i.e., if $s_c^*(1) = s_c^w(1)$ and $s_b^*(1) = s_b^w(1)$, $\beta^w - \widehat{\beta}$ in Eq.(38) is decreasing with security standards if and only if $(h^n(s_b^*(1)) - h^n(s_b^w(1)))\rho_b(0) - (h_b^c - h_w^c)\rho_c(1) > C_c(s_c^*) - C_c(s_c^w)$.

Replacing for $s_b^w(1)$, $s_c^w(1)$ given in Eq.(16), $s_b^*(1)$ and $s_c^*(1)$ given in Eq.(12) and Eq.(13), we find that this is equivalent to

$$\kappa \geq \frac{\theta(3L(1) - 2\rho_b(1))(\theta\rho_c(1) - \rho_b(0))}{6(1-\theta)^2(L(1) - \rho_c(1))^2}.$$

Appendix K: the shared responsibility regime

Stage 5 - Liabilities We denote by $h_i^{sr}(s_i) = \theta(\overline{h} - \sigma s_i)$ and by

$$h_c^{sr}(s_c) = (1-\theta)(\overline{h} - \sigma s_c)$$

[64] Replacing $h_w^n = h^n(s_b^w(1)) - (h^n(s_b^w(1)) - h_w^n)$ in Eq.(38), we note that the government's ability to internalize the effect of outsourcing on banks' investments increases $\beta^w - \widehat{\beta}$ by $(h^n(s_b^w(1)) - h^n(s_b^w(0)))\rho_b(0)$.

the probabilities that an attack occurs on the perimeter of an outsourcing bank $i \in \{A, B\}$, and on the perimeter of the cloud service provider, respectively.

Under a shared responsibility regime, the loss incurred by depositors equals $(L_d)_b^{sr} = \underline{\alpha} l_d - \eta_d$ if the cyber incident occurs in the bank's perimeter, and $(L_d)_c^{sr} = \underline{\alpha} l_d - \gamma_d$ otherwise. The loss incurred by banks either equals $(L_b)_b^{sr} = \underline{\alpha} l_b + \eta_d + \eta_c$ or $(L_b)_c^{sr} = \underline{\alpha} l_b - \gamma_b$, and the loss incurred by the cloud service provider either equals $(L_c)_b^{sr} = -\eta_c$ or $(L_b)_c^{sr} = \gamma_b + \gamma_d$.

Stages 3 and 4 - Prices and access fee At stage 4, when banks take symmetric outsourcing decisions, each bank $i \in \{A, B\}$ chooses the profit-maximizing deposit price $p_i^*(z)$ in Eq.(7), with

$$h(s_i(1))L_b(1) = h_b^{sr}(L_b)_b^{sr} + h_c^{sr}(L_b)_c^{sr}$$

and

$$\Delta h(1)\rho_b(1) = \Delta h(1)(\rho_b)_b^{sr},$$

with

$$(\rho_b)_b^{sr} = (L_b)_b^{sr} + \mu(L_d)_b^{sr}. \tag{39}$$

At stage 3, suppose that the cloud service provider serves both banks. We replace in Appendix C the expected damage internalized by banks when they outsource under a common responsability regime $h^c(s_i, s_c)\rho_b(1)$ by

$$h_i^{sr}(\rho_b)_b^{sr} + h_c^{sr}(\rho_b)_c^{sr}.$$

Therefore, if $s_i \geq s_j$, the cloud service provider sets an access fee equal to

$$(f^{a*})^{sr} = h_i^n \rho_b(0) - (h_i^{sr}(\rho_b)_b^{sr} + h_c^{sr}(\rho_b)_c^{sr}),$$

with $(\rho_b)_b^{sr}$ given in Eq.(39) and $(\rho_b)_c^{sr} = (L_b)_c^{sr} + \mu(L_d)_c^{sr}$.

It sets a compatibility fee

$$f^{c*} = (\beta/2)(1 - ((h_i^{sr} - h_j^{sr})\rho_b(1)/3)^2/t\tau(1, \beta)).$$

Therefore, the cloud service provider makes profit $\pi_c^{sr}(1) = \beta - \widehat{\beta}^{sr}$, where

$$\widehat{\beta}^{sr} = h_i^{sr}(\rho_c)_b^{sr} + h_c^{sr}(\rho_c)_c^{sr} - h_i^n \rho_b(0) + C_c(s_c), \tag{40}$$

with $(\rho_c)_b^{sr} = (\rho_b)_b^{sr} + (L_c)_b^{sr}$, and $(\rho_c)_c^{sr} = (\rho_b)_c^{sr} + (L_c)_c^{sr}$.

Stages 1 and 2 - Equilibrium investments Solving for the first-order condition of each bank's profit maximization with respect to s_i, and given that $(\rho_b)_b^{sr} = \rho_b(1) + \gamma_b + \mu\gamma_d$, the profit-maximizing levels of investment in security are given by

$$s_b^{sr}(1) = s_b^*(1) + \sigma\theta\frac{\gamma_b + \mu\gamma_d}{3k_b}.$$

Solving for the first-order condition of the cloud service provider's profit-maximization, given that $(\rho_c)_c^{sr} = \rho_c(1) - (1-\mu)\eta_d$, the cloud service provider's investment is given by

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

Optimal liabilities Replacing for $z = 1$, $L_d(1) = (L_d)_b^{sr}$ and $L_c(1) = (L_c)_b^{sr}$ in Eq.(36), and for $z = 1$ and $L_d(1) = (L_d)_c^{sr}$ in Eq.(37), firms' investments are equal to the first-best if and only if

$$\gamma_d = \underline{\alpha} l_d,$$

and

$$\eta_c = \frac{\underline{\alpha} l}{2} + (1-\mu)(\underline{\alpha} l_d - \eta_d).$$

With a shared responsibility model, we find that γ_d is higher than under a common responsibility system, because the cloud service provider directly considers the benefits of its investment for myopic depositors.

Also, replacing for $\gamma_d = \underline{\alpha} l_d - \eta_d$ given in Appendix I.2, in our benchmark model we have $\eta_c = \underline{\alpha} l/2 + (\underline{\alpha} l_d - \eta_d) + \gamma_b$. Therefore, η_c decreases under the shared responsibility model if and only if $\underline{\alpha} l_d - \eta_d \geq 0$, and η_d increases under a shared responsibility model if and only if $\eta_c < \underline{\alpha} l/2$.

Banks' total liability, which equals $\eta_d + \eta_c$ under a shared responsibility model and $\eta_d + \eta_c - \gamma_b$ under a common responsibility model, decreases if and only if η_d under a shared responsibility model is lower than $\underline{\alpha} l_d$, and it increases otherwise.

Finally, the total level of security is higher than the first-best if and only if

$$\eta_c \geq \frac{\underline{\alpha} l}{2} + (1-\mu)(L_d^b(1) + \frac{3(1-\theta)^2}{2\kappa\theta^2} L_d^c(1)),$$

which implies that the bank compensates the cloud service provider when a cyber incident occurs in its perimeter.

Appendix L - Public cloud infrastructure

We assume that the public structure is managed by a regulator. We start by studying the fees set by the regulator when banks are compatible, before providing the conditions such that the fees set by a regulator are identical to the private case if one bank only can outsource. Finally, we show that banks' investments are identical to the private case if both banks join the cloud or if $t < 2\beta$.

Fees when banks are compatible: If both banks join the cloud and become compatible, social welfare is independent of the access and compatibility fees. Therefore, from Appendix C, the regulator may set any compatibility fee $f_w^c \in (0, f^{c*})$, where f^{c*} in Eq.(9) represents the maximum compatibility fee that may be chosen by the private cloud service provider, and any access fee $f_w^a(1) \in (0, \min\{f_A^{a*}, f_B^{a*}\})$, with $f_A^{a*} = h_A(\rho_b(0) - \rho_b(1))$ the maximum fee such that bank A uses the storage service.

Fees when only bank B outsources: If only bank B joins the cloud, social welfare depends on the access fee. From the incentive constraints (C1b) and (C2b) given in Appendix C, the public platform, as the private cloud service provider, is constrained to set $f_a \in \{f_A^{a*}, f_B^{a*}\}$ with $f_B^{a*} > f_A^{a*}$, such that bank A earns a higher (positive) profit when it is the only independent bank than when both banks outsource their storage service, and bank B earns a higher (positive) profit when it is the only bank outsourcing than when both banks are independent. Thus, excluding investment costs, the regulator chooses $f_w^a(\overline{c}_A) \in \{f_A^{a*}, f_B^{a*}\}$ which maximizes

$$W(\overline{c}_A, f^a) = u_0 - \frac{t-2\beta}{2}((N_A(\overline{c}_A))^2 + (N_B(\overline{c}_A))^2) - l(h_A(0)N_A(\overline{c}_A) + \alpha h_B(1)N_B(\overline{c}_A)),$$

where $N_A(\overline{c}_A)$ and $N_B(\overline{c}_A)$ are given in Eq.(19). If $t \neq 2\beta$ let

$$f_w^a(\overline{c}_A) \equiv h_A\rho(0) - h_B\rho(1) + H$$

and

$$H = 3l(\underline{\alpha}h_B(1) - h_A(0))(\frac{t-\beta}{t-2\beta}).$$

Differentiating $W(\overline{c}_A)$ with respect to f^a, we find that

$$\frac{\partial W(\overline{c}_A, f^a)}{\partial f^a} = \frac{(t-2\beta)(f_w^a(\overline{c}_A) - f^a)}{18(t-\beta)^2},$$

and

$$\frac{\partial^2 W(\overline{c}_A, f^a)}{\partial^2 f^a} = \frac{-(t-2\beta)}{18(t-\beta)^2}.$$

If $t = 2\beta$, we have $\partial W(\overline{c}_A)/\partial f^a = l(\underline{\alpha} h_B(1) - h_A(0))/3t$.

Therefore, we distinguish three cases.

i) If $t > 2\beta$ and $f_w^a(\overline{c}_A) \in (f_A^{a*}, f_B^{a*})$, $W(\overline{c}_A)$ is strictly concave in f_a and the regulator can set the welfare-maximizing access fee $f_w^a(\overline{c}_A)$. In the absence of social cyber damages (i.e., $H = 0$), this implies that $N_A(\overline{c}_A) = N_B(\overline{c}_A) = 1/2$. Given that $(h_B - h_A)(1) = \theta(h_B - h_A)(0)$, we find that $f_1^a \in (f_A^{a*}, f_B^{a*})$ is equivalent to

$$\frac{H}{h_B(0) - h_A(0)} \in (\theta\rho_b(1), \rho_b(0)), \tag{41}$$

if $h_B(0) > h_A(0)$, and $H/(h_B(0) - h_A(0)) \in (\rho_b(0), \theta\rho_b(1))$ otherwise. Under this condition, the outsourcing minimizes the difference in security between banks without changing the security ranking among them, such that the public platform can reduce the average transportation costs (under participation constraints), at the cost of decreasing total network benefits.

ii) If $t > 2\beta$ and $f_w^a(\overline{c}_A) \notin (f_A^{a*}, f_B^{a*})$, such that condition (41) does not hold, the regulator is constrained by banks' incentives constraints, such that it sets $f^a = f_A^{a*}$ if $f_1^a < f_A^{a*}$, and $f^a = f_B^{a*}$ otherwise.

iii) if $t \leq 2\beta$, $W(\overline{c}_A)$ is convex in f_a. In the absence of incentive constraints, this implies that one bank should corner the market. Given the presence of banks' incentive constraints, the regulator sets $f^a = f_B^{a*}$ if $f_1^a < f_A^{a*}$ and $t < 2\beta$ or if $\alpha h_B(1) \geq h_A(0)$ and $t = 2\beta$, and it sets $f^a = f_A^{a*}$ otherwise.

To conclude, when only bank B outsources, the regulator sets an access fee $f^a = f_w^a(\overline{c}_A)$ if $t > 2\beta$ and condition (41) holds, and it is constrained to set $f^a = f_A^{a*}$ or $f^a = f_B^{a*}$ otherwise.

Security investments: When banks are compatible, the profit of each bank $i \in \{A, B\}$ $\pi_i(f^a, f^c, 1)$ given in Eq.(22) is independent of the access fee $f^a(1)$. Also, from f^{c*} in Eq.(9), if $f_w^c/f^{c*} \in (0, 1)$ the proportion of the compatibility benefit extracted by the regulator is symmetric across banks, f_w^c is also independent of banks' investment in the symmetric equilibrium. Therefore, at the equilibrium of the game, banks' investments are equal $s_b^*(1)$ in Eq.(12).

When only bank B can outsource and $f^a = \min\{f_A^{a*}, f_B^{a*}\}$, the conditions (C2a) and (C2b) given in Appendix C imply that $\pi_i(f^a, f^c, 1)$ the profit of

each bank $i \in \{A, B\}$ in Eq.(22) is equal to $\pi_i(0)$ if $f^a = f_B^{a*}$, and it is equal to $\pi_i(\overline{c})$ if $f_w^a(\overline{c}_A) = f_A^{a*}$. From Appendix G, banks set symmetric security investment $s_b^*(0)$ or $s_b^*(1)$ in Eq.(12) in each case. Therefore, $f_A^{a*} = f_B^{a*}$ at the equilibrium of the game, and the regulator can never serve only one bank.

Finally, when only bank B can outsource and $f^a = f_w^a(\overline{c}_A)$, banks' investments may be asymmetric at the equilibrium of the game if condition (41) holds and $t > 2\beta$.

Appendix M: the third-party provider's perimeter:

The welfare-maximizing choice of firms' perimeters: Suppose that the social planer is able to choose the banks' optimal share of the common infrastructure. From Eq.(15), the welfare $W(1) = \beta - \beta^w$ is convex in θ. Comparing $\beta - \beta^w$ in Eq.(18) with $\theta = 1$ and with $\theta = 0$, the difference is equal to

$$\frac{(\sigma l)^2}{2\kappa k_b}\underline{\alpha}^2(\kappa - 1).$$

Social welfare is maximized when banks hold a share θ of the common infrastructure equal to

$$\theta = \begin{cases} 0 & \text{if } \kappa < 1 \\ 1 & \text{otherwise.} \end{cases}$$

This policy does not maximize depositor surplus if $\kappa < 1$. From Eq.(31), the average utility of a depositor under outsourcing equals

$$DS(1) = u_0 - \tau(0) - h^n(s_b^*(1))\rho_b(0),$$

which is increasing with $s_b^*(1)$. Since $s_b^*(1)$ is increasing with θ, while the other terms of $DS(1)$ are independent of θ, we conclude that $DS(1)$ is increasing with θ. Therefore, depositor surplus is maximized when banks hold a share $\theta = 1$ of the common infrastructure.

The private choice of the firms' perimeter by the cloud service provider: Suppose that the cloud service provider may choose θ. From Eq.(29), the profit of the cloud service provider $\pi_c(1) = \beta - \widehat{\beta}$ is convex in θ. Comparing $\beta - \widehat{\beta}$ in Eq.(30) with $\theta = 0$ and with $\theta = 1$, the difference is equal to

$$(\sigma)^2\left(\frac{\rho_b(1)(\rho_c(1) - \rho_b(0))}{3k_b} - \frac{(\rho_c(1))^2}{2k_c}\right).$$

Therefore, $\pi_c(1)$ is maximized when banks hold a share θ of the common infrastructure equal to

$$\theta = \begin{cases} 0 & \text{if } \kappa < \kappa_p \equiv \frac{3\rho_c(1)}{4\rho_b(1)}(1 + \frac{\rho_b(0)}{\rho_c(1)-\rho_b(0)}) \\ 1 & \text{otherwise.} \end{cases}$$

We have $\kappa_p > 1$ if and only if

$$\rho_b(0) > \rho_c(1)(1 - \frac{3\rho_c(1)}{4\rho_b(1)}).$$

Therefore, the cloud service provider offers to store the maximum amount of data for an inefficiently high value of κ, that is, for an inefficiently low degree of efficiency gains.

Online Appendix

O-1: moral hazard and information disclosure

Extension of our model setup: We extend our model by assuming that at stage 5 of the game, the bank and the cloud service provider may conceal respectively an amount of information y_b and y_c from the other players. The total amount of information i concealed on the cyber incident depends on the sharing of security investments, that is, we have

$$y = \theta y_b + (1-\theta) y_c.$$

The cloud service provider's amount of hidden information $y_c \in (\underline{y_c}, \overline{y_c})$ depends on its cost $K(y_c) = k_I(y_c^2 - \underline{y_c}^2)/2$ of concealing information. We assume that $K(\underline{y_c}) = 0$, $K'(y_c) > 0$ and $K''(y_c) > 0$.[65] Both banks conceal the same exogenous amount of information y_b, which we normalize to $y_b \equiv 0$. This implies that $y = (1-\theta)y_c$.

If the cloud service provider does not disclose perfectly all 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 $q(y) \in (0,1)$, which is a decreasing convex function of y such that $q(0) = 1$, $q(1) \in (0,1)$, $q'(y) \leq 0$ and $q''(y) \geq 0$ for all $y \in ((1-\theta)\underline{y_c}, (1-\theta)\overline{y_c})$.

If the cloud service provider does not disclose all information, the amount of the losses incurred by the banks and the depositors, respectively, is multiplied by an endogenous factor $\alpha(y) \in (\underline{\alpha}, \overline{\alpha})$ and increases with the amount of hidden information. If all information is disclosed, we have $y = 0$ and $\alpha(0) = 1$. We further assume that $\alpha((1-\theta)\underline{y_c}) = \underline{\alpha}$ and $\alpha((1-\theta)\overline{v_c}) = \overline{\alpha}$.

With moral hazard, the losses $L_d(z, y_c)$, $L_b(z, y_c)$ and $L_c(z, y_c)$ depend on the amount of hidden information. Following a cyber incident, if a bank joins the cloud, each depositor claims compensation with probability q and incurs a loss

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

the bank incurs a loss

$$L_b(z, y) = \alpha(y) l_b + q(y)(\eta_d - \gamma_b + \eta_c),$$

[65] 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.

and the cloud service provider incurs a loss

$$L_c(z, y) = q(y)(\gamma_d + \gamma_b - \eta_c) + K(y), \tag{42}$$

We include into L_c the additional cost K of not disclosing cyber incidents to the other players.[66] The total loss caused by a cyber incident is

$$L(z, y) = \alpha(y)l + zK(y).$$

To ensure that the cloud service provider not to disclose either the minimum or the maximum level of information to the other players, we make one additional assumption:

- (A3): For all $y_c \in (\underline{y_c}, \overline{y_c})$, $L'_c(1, \underline{y_c}) < 0 < L'_c(1, \overline{y_c})$ and $L''_c(1, y_c) \geq 0$.

Stage 6: 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 $L_c(1, y_c)$, given in Eq.(42). If $L_c(1) = \gamma_d + \gamma_b - \eta_c$ the benchmark loss of the cloud service provider when there is no moral hazard is positive, with $\theta < 1$ the loss-minimizing level of information y_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

$$-(1 - \theta)q'(y^*)L_c(1) = k_I v_c^*, \tag{43}$$

where $y^* = (1 - \theta)y_c^*$. 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 $L_c(1) \leq 0$), it hides the minimum amount of information from the bank and depositors, that is, we have $y^* = (1 - \theta)\underline{y_c}$.

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

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 zy^*, where $z = 0$ for the bank that does not join the cloud, and $z = 1$ for its competitor if the latter joins the cloud.

With cloud outsourcing, the bank's internalized marginal cost is given by

$$\rho_b(1, y^*) = \alpha(y^*)(l_b + \mu l_d) + q(y^*)((1-\mu)(\eta_d + \gamma_d) - L_c(1)). \tag{44}$$

Around $y_c = y_c^*$, we have $d\rho_b(1)/dy_c = (1-\theta)\rho_b'(1)(y)$, with $\rho_b'(1)(y)$ the derivative of $\rho_b(1)$ with respect to y equals to:

$$(\rho_b(1))'(y) = \alpha'(y)(l_b + \mu l_d) - q'(y)(L_c(1) - (1-\mu)(\eta_d + \gamma_d)),$$

with $-q'(y)L_c(1) = k_I y^*$ from Eq.(43). To analyze how information disclosure impacts banks' marginal costs of cyber incidents and how it changes with the liability of the cloud service provider, we consider examples:

- **High proportion of sophistication of depositors:**
  If almost all depositors are sophisticated (μ close to 1), 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 decreases the bank's marginal cost.

- **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 ($\alpha'(y_c) = 0$). If the transfers received from the cloud service provider are low (i.e., $L_c(1)$ 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 liabilities from the cloud service provider decrease the bank's marginal cost.

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

Effect of compensations on banks' investments incentives: For $\gamma \in \{\gamma_b, \gamma_d\}$, the derivative of $s_b^*(z)$ in Eq.(12) with respect to γ is given by

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

From Eq.(44), $\partial\rho_b(v^*)/\partial\gamma_b = -q(v^*)$, and $\partial\rho_b(v^*)/\partial\gamma_d = -\mu q(v^*)$. Also, applying the implicit function theorem on Eq.(43), we have $\partial v^*/\partial\gamma > 0$ from Assumption (A2).

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

Effect of compensations on the cloud service provider's investments incentives: For this purpose, using $l = l_b + l_d$, we rearrange $\rho_b(v^*) = \alpha(v^*)l - (1-\mu)L_d(v^*) - L_c(v^*)$ in Eq.(13), such that

$$s_c^* = \sigma(1-\theta)\frac{\alpha(v^*)l - (1-\mu)L_d(v^*) + K(v^*)}{k_c}, \tag{45}$$

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.(45) with respect to γ is such that

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

We have $\partial\rho_b(v^*)/\partial\gamma_b = -q(v^*)$, and $\partial\rho_b(v^*)/\partial\gamma_d = -\mu q(v^*)$. Also, from Eq.(42), $\partial L_c(v)/\partial\gamma_b = q(v^*)$ and $\partial L_c(v)/\partial\gamma_d = q(v^*)$. From Eq.(43), at $v = v^*$, we have $\partial L_c(v)/\partial v = 0$. Finally, applying the implicit function theorem to Eq.(43), we have $\partial v^*/\partial\gamma > 0$ from Assumption (A2).

Using the definition of $\epsilon_{\rho_b}^v(v^*)$ given above, we have $ds_c^*/d\gamma_b > 0$ if $\epsilon_{\rho_b}^v(v^*) > 0$, 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.

Analysis of the liability system

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

distortions 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 their payment services, but could be problematic if banks do not rely on a joint payment infrastructure when this would be socially desirable.

O-2: Compatibility without a third-party

Fee setting by independent banks We assume that banks may decide to become interoperable without relying on the cloud service provider with a lower-quality technology. If the depositors make transactions with the customers of the same bank, the magnitude of network effects is β. In contrast, if the depositors of bank i make transactions with the depositors of bank j, the magnitude of network effects is $\beta_0 < \beta \in (0,1)$. Interoperability is therefore imperfect. Moreover, we assume that banks may decide to deploy a compatible payment system without relying on the third-party only if they do not store their data in the cloud. Using the same method as in our model, we find that the demand of bank i equals

$$N_i(z) = \frac{1}{2} + \frac{p_j - p_i - \mu h_i L_d(0) + \mu h_j L_d(0)}{2\tau(z, \beta_0)}, \tag{46}$$

with $\tau(z, \beta_0) = t - (1-z)\beta_0$.

Before the competition stage, banks may decide to become compatible without relying on the third-party and choose access fees. Different pricing schemes may be considered. Our model differs from Laffont, Rey and Tirole (1998) because we assume that payment transactions are free and the demand for payment transactions only banks' outsourcing decisions, because a depositor makes one transaction with all depositors who can be reached using the

bank's payment system.[67] Formally, in payment systems, this corresponds to the choice of an interchange fee, which may be paid by the receiving bank (the acquirer of the transaction) to the issuing bank. Therefore, a bank pays an access fee to receive a payment transaction initiated by the depositors of its competitor.

Banks may decide to set up a linear access charge, proportional to the number of depositors of the other bank. Or banks may decide to set up a usage fee, proportional to the number of total connections to the other bank ("interconnection fee"). If each bank $i \in \{A, B\}$ pays a fee $a_i > 0$ for accessing each depositor of its rival, and pays (or earn) on average a net interconnection fee $a_{ij} = -a_{ji}$ for each of the $2N_iN_j$ connections. We denote by $\tilde{a} = \{a_i, a_j, a_{ij}\}$.

At the competition stage, each compatible bank i chooses p_i to maximize

$$\pi_i(\tilde{a}) = (p_i - h_i L_b(0))N_i - C_i(\tilde{a}) - C_b(s_i). \tag{47}$$

with $N_i(1)$ given in Eq.(46) when $z = 1$, and

$$C_i(A) = a_i N_j(1) - a_j N_i(1) + 2a_{ij} N_i(1) N_j(1)$$

the cost of compatibility for bank i. Solving for the first-order conditions of banks' profit maximization gives

$$p_i^* = \tau(\beta_0) - h_i L_b(1) - a_i - a_j - \Delta_d(0)(\tau(\beta_0) - 2a_{ij}),$$

where

$$\Delta_d(z) = \frac{(h_i - h_j)(z)\rho_b(z)}{3\tau(z, \beta_0)}$$

measures security differentiation if $z = \{0, 1\}$ and a quality β_0. Note that $\Delta_d(z) \in (-1, 1)$. Replacing for p_i^* and p_j^* into Eq.(47), each bank $i \in \{A, B\}$ makes profit

$$\pi_i(a_i, a_{ij}) = \frac{\tau(z, \beta_0) - a_{ij}}{2}(1 - \Delta_d(0))^2 - a_i - C_b(s_i). \tag{48}$$

By symmetry from Eq.(48), the fee a_i charged by bank i to access its depositors does not impact bank j's profit, because any increase in fee revenues is fully offset by a more intense price competition.

[67] This assumption resembles the literature on two-way access in telecommunications networks (see Laffont, Rey and Tirole, 1998).

Solving for $\pi_i(a_i) = \pi_i^n$, with π_i^n the profit of bank i under independence given in Eq.(48) with $z = 0$ and $a_i = a_{ij} = 0$, bank j can set a connection fee such that $a_{ij} \leq a_{ij}^*$, with

$$a_{ij}^* = (\beta_0(1 - \frac{\tau(1,\beta_0)}{\tau(1,0)}(\Delta_d(0))^2) - 2f_i)(\frac{1}{1-\Delta_d(0)})^2,$$

Therefore, given that $\pi_j(a_j, a_{ij})$ is increasing with a_{ij} and independent from a_i, bank j wants to subsidize the access fee to its depositors a_i, in order to maximize the connection fee a_{ij}.

To conclude, at the equilibrium:

i) if only access fees are possible, banks are indifferent on the fees set, and banks can be compatible.

ii) if connection fees are possible, there is no equilibrium, because each bank can set a higher fee to deliver transactions to rival depositors than the fee set to emit transactions, in order to earn a positive margin on total inter-connections. For instance, it is not optimal for bank j to set $a_i^* = \beta_0(1-(\tau(1,\beta_0)/\tau(1,\beta_0))(\Delta_d(0))^2)/2$, and $a_{ij}^* = 0$, because it may earns more profit by decreasing its access fee, and setting a higher connection fee than its rival.

Fee setting by the cloud service provider If banks cannot charge for each connection, from Eq.(48) the maximum profit of bank i equals

$$\overline{\pi}_i = \frac{\tau(1,\beta_0)}{2}(1 - \Delta_d(0))^2 - C_b(s_i),$$

while the profit under cloud compatibility equals

$$\overline{\pi}_i = \frac{t}{2}(1 - \Delta_d(1,1))^2 - f^c - C_b(s_i).$$

Therefore, replacing for $\Delta_d(0) = \Delta_d(1)t\rho_b(0)/(\tau(1,\beta_0)\theta\rho_b(1))$, the cloud must set a fee $f^{c*} = \min\{f_i^{c*}, f_j^{c*}\}$, with

$$f_i^{c*} = \widehat{f^{c*}} + t\Delta_d(1,1)(1 - \frac{\rho_b(0)}{\theta\rho_b(1)})((1 + \frac{\rho_b(0)}{\theta\rho_b(1)})\frac{t\Delta_d(1,1)}{2\tau(q,\beta)} - 1)$$

and

$$\widehat{f^{c*}} = \frac{\beta(1-q)}{2}(1 - \frac{t}{\tau(q,\beta)}(\Delta_d(1,1))^2)$$

represents the compatibility fee set if different compatibility regimes has no effect on the security differentiation among banks (i.e., if $\rho_b(0) = \theta\rho_b(1)$). At the symmetric equilibrium, $f^{c*} = \beta(1-q)/2$, and the cloud service provider enters the market if and only if $\beta > \widehat{\beta}/(1-q)$, with $\widehat{\beta}$ given in Eq.(14) of the article.

NOTA NOE: f^{c*} is no longer equal across banks, and it impacts security decisions... Clearly, the unique equilibrium is symmetric if the cloud can discriminate among banks, but it is unclear otherwise. If banks can develop their compatibility system even when data is outsourced, I think it is easier (banks always outsource their data). I can check both cases.

O-3: public cloud and different timing

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.(**??**). Also, if banks outsource, but do not use the compatibility service, the profit of bank i equals π_{-i}^{st}, which is obtained by setting $v = \underline{v}$ and $z = 0$ in π_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.(12), 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 π_{-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.