Cyber Security and Cloud Outsourcing of Payments

Noé Ciet [1]
Marianne Verdier[1]

[1]CRED (TEPP), Université Paris-Panthéon-Assas

EEA
August 31, 2023

Motivation : Outsourcing of banks' activities and cyber risk

Cloud-based Third-Party Providers in the banking sector (TPPs).

- Definition of TPPs (AWS, Stripe, Modo) :

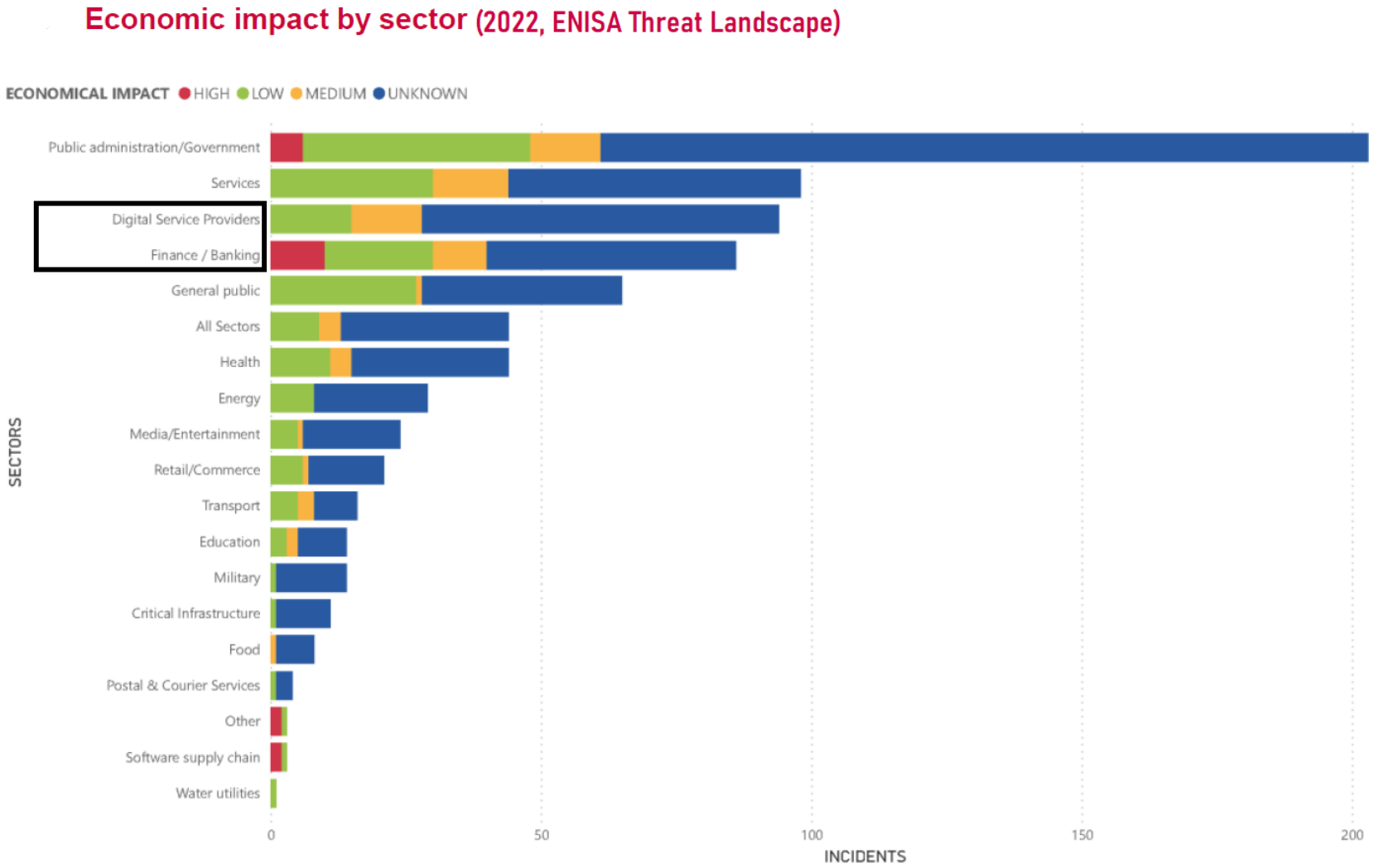
  'Any party [...] that directly obtains, processes, stores, or transmits customer information on an institution's behalf.'[1]

Cyber risk is a concern for banks and supervisors (BoE survey, 2022)

- **Cyber risk with TPPs :** examples of Capital One 2019, AWS 2021.
- Cyber attacks are costly for banks and consumers
- Regulatory framework for cyber risk under construction (Security guidelines in the US, DORA in the EU)

1. Board of the governors of the Federal Reserve, Interagency Guidelines Establishing Information Security Standards

Illustration : cyber risk in the financial sector



- Economic impact : the direct financial loss incurred by agents and the damage to national security, defined by the European Union Agency for Cybersecurity

Research question & focus of the paper

Framework of the model

- Focus on the effect of cyber-risk on *consumer protection* (not financial stability) and payment services
- A TPP can provide two services :
  - *Data storage*
    security investments get shared between banks and TPP
  - *Interoperability of banks' payment systems*
    e.g., depositor using an app payment to send money abroad / across digital wallets

Research question

- Is outsourcing socially optimal ?
- Does it improve payment system security ?
- If not, can regulation achieve both outsourcing benefits and payment system security ?

Main results

1. Efficiency of outsourcing decisions with cyber risk
   - Banks may sometimes under outsource their payment services even when there are interoperability benefits
2. Effect of outsourcing on depositor surplus.
   - Outsourcing may improve depositor surplus only if sufficient increase in security.
   - Without any regulation, under investment problem with respect to the first-best + inefficient sharing of the investment burden between the TPP and banks.
3. Effect of regulation on payment system security.
   - Some regulation instruments (the supervision of outsourcing agreements, a liability regime, a shared responsibility model, a public provision of the infrastructure) may partially improves payment system security and / or outsourcing decision

Literature overview

Cybersecurity

- **investment** : De Corniere and Taylor, 2021, Lam and Seifert, 2023, survey by Anderson et al., 2009
- **in payments** : Kahn and Roberds, 2008, Kahn, Rivadeneyra and Wong, 2020, Garratt and Schilling, 2022, Creti and Verdier, 2014
- **and financial stability** : Anand, Duley and Gai, 2022, Duffie and Younger, 2019, Eisenbach et al., 2022

Network industries

- **interoperability** : e.g., Foros and Hansen, 2001, Doganoglu and Wright, 2006, survey by Bianci et al., 2022
- **co-investments** : Inderst and Peitz, 2012, Bourreau et al., 2018

Product liability

Jacob and Lovat, 2016, survey by Daughety and Reiganum, 2013

Roadmap of the presentation

1. The model
2. The first-best outsourcing decisions
3. The private outsourcing decisions and depositor surplus
4. The outsourcing decisions with endogenous investments
5. Comparison of various regulatory frameworks

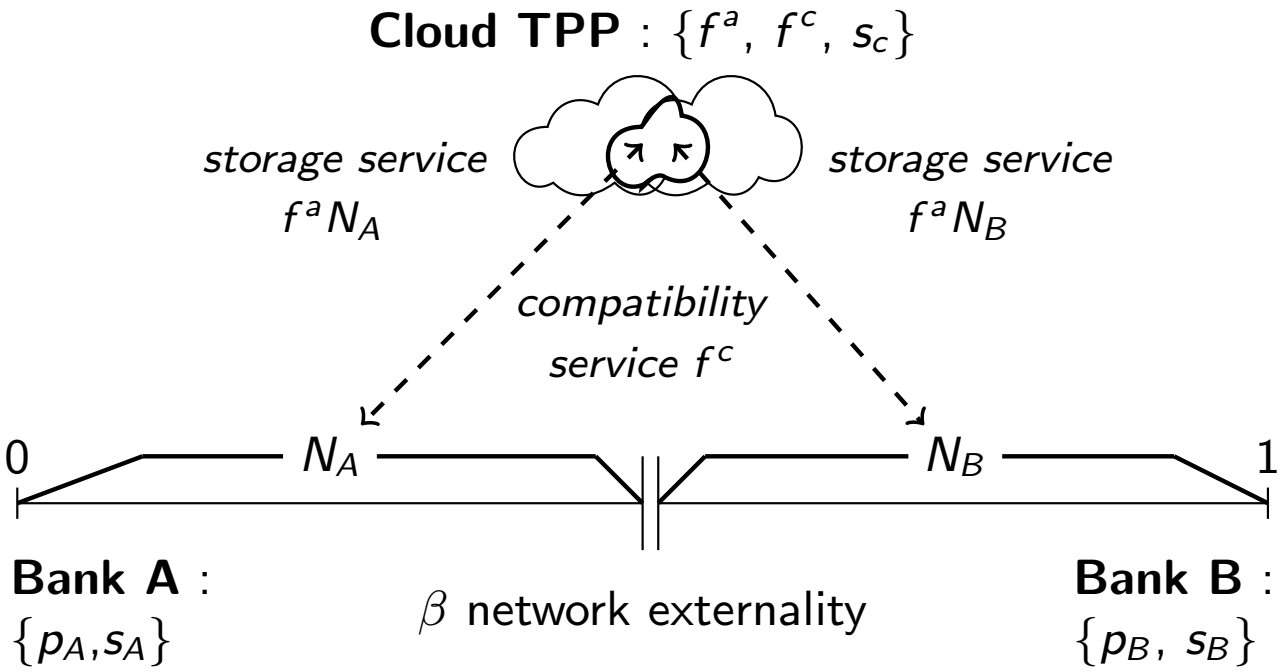
Main ingredients of the baseline model

1. Depositors choose between two competing banks on the Hotelling line
2. Fixed fees to open a bank account
3. Quality of service : payment system security - depends on costly investments in security
4. Only a fraction of depositors is sophisticated enough to assess cyber risk
5. Depositors make payments with all compatible depositors (network externalities)
6. Banks may outsource their payment systems to a TPP and enjoy the benefits of interoperability
7. If there is outsourcing, cyber risk depends on the TPP's investment and on banks' investment

Illustration : baseline model

Upstream decisions

Downstream competition



Cyber risk Bank k

$$h_k^n = h - \sigma s_k \xrightarrow[\text{(storage service)}]{\text{if outsourcing}} h_k^o = h - \sigma(\theta s_k + (1-\theta)s_c)$$

Investment cost

$$C_b = k_b s_A^2/2 \qquad C_c = k_c s_c^2/2 \qquad C_b = k_b s_B^2/2$$

Main ingredients : the losses from cyber-incidents

- Net losses per depositor (after transfers) are shared between the depositors, the banks and the TPP :
  - L_d for depositors, L_b for the bank, L_c for the TPP, and L the total loss (gross loss l without outsourcing)
- Two effects of outsourcing on banks & depositors' losses :
  1. Increase in gross losses, which are multiplied by α
  2. Possible transfers from the TPP, when defined by the liability system

Only a proportion $\mu \in (0, 1)$ of depositors are *sophisticated* and care about payment system security

Timeline

1. **Stage 1 : Security investments :**
   The TPP chooses its level of security s_c and each bank $i \in \{A, B\}$ chooses its level of security s_i.

2. **Stage 2 : Outsourcing decisions :**
   The TPP chooses the access fee f^a and the compatibility fee f^o.
   Each bank decides whether or not to outsource its payment services and whether to buy the compatibility service.

3. **Stage 3 : Competition for deposits** :
   Each bank $i \in \{A, B\}$ chooses the price p_i of deposit accounts.

4. **Stage 4 : Cyber incident and losses :**
   With probability $h_i(s_i, s_c, \theta)$, a cyber incident occurs in the payment system of bank $i \in \{A, B\}$.
   The depositors, the banks and the TPP incur losses.

First-best investment in security

Government decides on security investments and outsourcing

Optimal security investments : Marginal benefit = marginal cost

- No outsourcing : $(s_b^n)^w = \frac{\sigma l}{2k_b}$
- Outsourcing : $(s_b^o)^w = \theta\alpha(s_b^n)^w, \qquad (s_c)^w = \frac{2k_b}{k_c}(1-\theta)\alpha(s_b^n)^w$

Total security is higher under outsourcing if either

- $\theta(s_b^o)^w > (s_b^n)^w$
- $\theta(s_b^o)^w \leq (s_b^n)^w$ and $k_c < k_s \equiv 2k_b\frac{(1-\theta)^2\alpha}{1-\theta^2\alpha}$

$\rightarrow$ Bank investment is higher with outsourcing ($\theta^2\alpha > 1$) because of higher expected losses,
$\rightarrow$ or, the TPP investment compensates for lower bank investment :
In particular, if $\theta = 0$ and $\alpha = 1$, the condition is that outsourcing avoids a *duplication of investment costs*, that is :

$$k_c < 2k_b$$

First-best benchmark in outsourcing

Effect of outsourcing on :

$$\text{Expected damage :} \quad \Delta L^w = h_c((s_b^o)^w, (s_c^o)^w)\alpha I - h_n((s_b^n)^w)I$$

$$\text{Security costs :} \quad \Delta C^w = k_b((s_b^o)^w)^2 - ((s_b^n)^w)^2) + \frac{k_c((s_c)^w)^2}{2}$$

Outsourcing is optimal if and only if

$$\beta/2 > max(0, \Delta L^w + \Delta C^w),$$

with $\Delta L^w + \Delta C^w \leq 0$ equivalent to $k_c < k_w$, with $k_w \leq k_s$

$\rightarrow$ If $k_c \geq k_s$, outsourcing decreases security : data storage decreases welfare
$\rightarrow$ If $k_c \in (k_w, k_s)$, outsourcing increases security because of higher losses caused by cyber-incidents : data storage decreases welfare
$\rightarrow$ If $k_c \leq k_w$, data storage increases security without strong effect on losses

Private equilibrium (1) : downstream competition

Banks compete for deposits, for a given level of security differentiation
Deposit price of bank i :

$$p_i^* = t + \underbrace{h_i L_b + z f^a}_{\text{marginal cost}} - \underbrace{(1-z)\beta}_{\substack{\text{network effect} \\ \text{(if incompatibility)}}} - \underbrace{\frac{h_i - h_j}{3}\rho}_{\substack{\text{security} \\ \text{differentiation}}}$$

with $z = 1$ if outsourcing, and

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

represent banks' marginal cost of cyber incidents, including the internalization of the sophisticated depositors' losses.

- Banks benefit from compatibility : without compatibility, they take into account the positive value of attracting depositors on their total demand
- Market failure : banks only internalize the damage of sophisticated depositors

Private equilibrium (2) : fees

- The compatibility fee f^{c*} : banks' additional surplus of compatibility .
- The access fee f^{a*} : minimal such that the the bank with the lowest willingness-to-pay for the TPP's services joins the TPP. It equalizes the expected marginal cost of cyber incidents with and without TPP :

$$h_i^o \rho^o + f_i^{a*} \equiv h_i^n \rho^n,$$

  with o the cloud outsourcing case (n the no-outsourcing case)
- The TPP internalizes banks' marginal costs of cyber incidents

Private equilibrium (3) : the outsourcing decision

The outsourcing decision is made by the TPP, because it extracts the banks' additional profit of outsourcing : outsourcing occurs. It enters the market if it makes a positive profit

The TPP's profit :

- Benefit of serving both banks if compatible : network effects + access fee, $\beta + f^{a*}$
- Cost of serving both banks : the expected cost of damage and the cost of security investment, $h^o(s_c, s_b^c)L_c + C_c(s_c)$.

The TPP makes a positive profit iff $\beta \geq \max\{0, \widehat{\beta}\}$, with

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

and $\overline{\rho}^o \equiv \rho^o + L_c$ the total marginal cost of cyber incidents internalized by the TPP.

The distortions with respect to the first best

Proposition :

With exogenous investment, there may be over-outsourcing or under-outsourcing with respect to the first-best.

Three sources of distortions for given investments :

1. **Compatibility (+ outsourcing)**. *Banks do not internalize the compatibility benefit of rival depositors* : excessive outsourcing (Foros and Hansen, 2001).
2. **Costs of security (+)/(−)**. *The TPP do not internalize the effect of outsourcing on banks' investments costs*. Optimally, banks should outsource iff
$$\beta/2 \geq \Delta C^w,$$
with
$$\Delta C^w = 2(C_b((s_b^o)^w) - C_b((s_b^n)^w)) + C_c(s_c).$$
3. **Losses caused by cyber risk (+)/(−)** *The TPP does not internalize the effect of outsourcing on myopic depositors' damages*. If myopic depositors face higher damage under outsourcing, the TPP underestimates the change in losses caused by outsourcing w.r.t the first-best, i.e.,
$$h^n L_d^n > h^o L_d^o$$

Outsourcing, banks' profits and depositor surplus

Proposition :

Suppose that banks invested symmetric levels of security at stage 2.

- Banks' profit increases with cloud outsourcing if and only if it reduces their security investments (i.e., if $s_b^o \leq s_b^n$).
- Depositor surplus is higher with cloud outsourcing if and only if

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

$\rightarrow$ Depositor surplus may only increase with a higher level of security.

With endogenous investments :

Three distortions induce under-investments

1. Banks internalize the negative effect of their investment on their rival downstream price
2. Banks do not internalize the damage of the TPP + myopic depositors
3. The TPP only fails to internalize the damage to myopic depositors

$\rightarrow$ Inefficient sharing of investment : TPP investment too high.

Consequence on outsourcing decision, w.r.t the exogenous investments case :

1. **Share of the TPP too high** = less outsourcing (less entry by the TPP)
2. **Banks under-invest...** both when they outsource and when they don't. Ambiguous effect on outsourcing : TPP faces additional risk, but earns higher revenues from its storage service if it contributes to most of the security

Comparison of various regulatory frameworks

We finally discuss in the paper several regulatory remedies :

1. *Regulatory control of outsourcing agreements*
   - Inefficient if bias towards under-outsourcing
2. *Liability regime*
   - Optimal to make banks fully liable (even towards the TPP), because the TPP internalizes banks' damages
   - Insufficient, because downstream competition implies that banks under-invest
3. *Shared responsibility model* (delimitation of liability perimeters ex ante)
   - increases banks' investment : banks can no longer rely on TPP liability when they are liable, and depositors become more sensitive to banks' investments
   - decreases the TPP's investment : banks no longer pay depositors when the TPP is liable
4. *Security standards*
   - cannot implement first-best outsourcing, because the TPP imperfectly internalizes the banks' cost of outsourcing

Conclusion

Without cyber risk : banks over outsource their payment services

- compatibility softens competition $\rightarrow$ depositors are worse off

With cyber risk : banks may sometimes under outsource their payment services :

- This is inefficient if outsourcing improves security and avoids a duplication of costs
- The vertical relationship may limit private incentives to outsource in various ways, and calls for a combination of regulatory instruments

The liability regime and the welfare-maximizing level of security :

Implementing the First-Best security levels :

- $L_d = 0$ (full depositor coverage)
- $L_c = \frac{-\alpha l}{2}$ (penality from banks to the TPP or any other party)

$\rightarrow$ Full depositor insurance corrects the market failure due to consumer myopia.
$\rightarrow$ Banks must be more than fully liable, because (1) competition implies under-investment, (2) the share of payment system security borne by the TPP is inefficiently high with respect to the first best.

Outsourcing arrangements and payment system security

Let $\tilde{c}$ the public control over TPP investment under a regulation of access fees, such that

$$s_c \equiv s_c^* + (1-\theta)\frac{\tilde{c}}{k_c}$$

Let $\zeta = \left(\frac{\theta}{1-\theta}\right)^2 \frac{k_c}{6k_b}$ a measure of banks' relative contribution to security

With respect to the benchmark model (common responsibility) :

- If $\zeta(\gamma_b + \mu\gamma_d) < (1-\mu)\eta_b$, only the **regulation of access fees** increases the security of the industry
- If $\zeta(\gamma_b + \mu\gamma_d) \in ((1-\mu)\eta_b, (1-\mu)\eta_b + \tilde{c})$, the **regulation of access fees** increases the security of the industry more than a shared responsibility model
- If $\zeta(\gamma_b + \mu\gamma_d) \geq (1-\mu)\eta_b + \tilde{c}$, the **shared responsibility model** may increase the security of the industry more than a regulation of access fees

$\rightarrow$ The regulation of access fees always increases industry security (one bank's investment $x2$ w.r.t benchmark)
$\rightarrow$ Shared responsibility model increases security if bank contribution and TPP transfers are high, bank transfers are low

Appendix : example of cyber incident and outsourcing

- Cyber attack on Capital One through Amazon Web Services (AWS)
- Hacker : AWS former employee, in 07/2019
- 100M US + 6M Canadian customers affected
- Credit card applications stolen : Social security numbers, Payment history, credit scores...
- Class action cost 190 M$ + fine of 80 M$ to the OCC

DORA - Digital Operational Resilience Act

Not only guidelines (Fed, BoE), but regulatory requirements

5 pillars

- IT risk management
- Incident reporting
- Operational resilience tests
- Supervision of TTP
- Info and intelligence sharing

Only one fee

Comparison π_i^o (everybody outsource) vs π_i^o (the rival uses the storage service).
If fee paid by depositor :

$$f_i^{a**} = f_i^{a*} + 3(t-\beta)(\sqrt{\frac{t}{t-\beta}} - 1) + \rho_c(v^*)(h_i^o - h_j^o)(1 - \sqrt{\frac{t-\beta}{t}})$$

Three elements : storage (no compatibility) + benefit from compatibility + change (increase if $h_i^o > h_j^o$) of profit of bank i from the lower sensitivity of depositors to quality differences under compatibility
f fixed fee

$$f_i^{c**} = f^{c*} + (\pi_i^{st} - \pi_i^o)$$

with $(\pi_i^{st} - \pi_i^o)$ le marginal bnfit from storing, if rival j independent [2].

Conclusion : no change in security levels at the equilibrium, but threshold $\widehat{\beta}$ more complex to write

2. Proof : f_i^{c**} is such that $f_i^{c**} = \pi_i^o - \pi_i^o$, et $f^{c*} = \pi_i^o - \pi_i^{st}$.