# Optimal Data Security with Redundancies

Rod Garratt* and Linda M. Schilling†

March 15, 2024

**Abstract**

We provide an economic analysis of how the observation of data by multiple parties (redundancies) affect private and socially optimal investment in data security. Our use case is the current banking system where payment transaction data is observed by at least the sending and the receiving institution. Redundancies cause free-riding, and under investment relative to the social optimum which increases the chance of cyber attacks. We show that an optimally protected third party, e.g. a regulator that observes all payment data, can increase overall data security beyond the level provided by the social planner even though all private entities shirk upon its entry. This holds because the information environment that results from providing a third redundancy is inherently different than the information environment the social planner is faced with. Key words: cyber attacks, data security, backups, free riding, redundancy, DLT
JEL codes: D8, G28

*email: rodney.garratt@bis.org, Bank for International Settlements
†email: lindas@wustl.edu; Olin Business School at Washington University in St Louis, CEPR and FTG. We thank Cyrus Mevorach (Olin) for excellent research assistance.

# 1 Introduction

Data is a valuable resource for financial institutions (FIs). It is essential for their operations and FIs have legal and financial incentives to prevent data loss and keep data private. Nevertheless, there is evidence that firms crucially underinvest in data security and neglect the costs to society. The Online Trust Alliance claims that up to 65% of US banks are 'extremely' vulnerable to cyber attacks (IBS Intelligence, 2017).

Data security investment may be suboptimal due to a free-rider problem. When multiple parties have access to the same data, each party may rely on the other to protect the data. In such circumstances, expenditures that achieve a social optimum may require government action or policies by government participants that reflect private incentives to free ride.

We refer to the way that data is stored and backed up across the financial system as an information structure. We focus on information structures that are exogenously generated by payment flows. Hence the data structure depends on how banks interact in terms of payments and the system through which payments are made. We consider information structures generated by the existing banking system and those associated with distributed ledger technology (DLT) systems.

The existing banking system is composed of multiple (distinct) participants, each of whom keeps a record of its own transactions. This means each participant knows everything about the transactions they make and part of what there is to know about transactions others make. Payments are made through one of multiple financial market infrastructures (eg Fedwire, CHIPS or ACH) and hence some aspects of payment data is obtained and stored by these entities.

We consider two cases that relate to the existing banking system. First we assume the infrastructure provider keeps no records (or the data provided to the infrastructure providers is not sufficiently detailed to provide a stand-alone record). In this case, a complete record of all transactions may be obtained by combining the records of any group that consists of all but one bank. This follows from the fact that any individual bank's records can be reconstructed from the records of all the banks it transacts with. Individual banks may not protect their data optimally, since private costs do not reflect the costs borne by others. Specifically, we show that banks protect their data less than would be optimal under a planner's solution.

Second we consider the case where a single entity (eg Fedwire) observes all transactions. Now, there are two ways to recover all data; Fedwire's records or the collective individual records of any group that consists of all but one bank. We assume Fedwire, as a public entity, seeks to maximise the social welfare of the system, by optimally choosing its level of security while internalising the impact its protection choices have on the actions of others.

Without Fedwire being present, all private banks under invest in data security relative to the social optimum. One might therefore ask whether adding an additional publically minded entity can improve overall security, and move security closer to the social optimum. We show that when Fedwire sets positive levels of data security it does in fact cause banks to further shirk by individually reducing their investment in data security, however the overall impact on welfare (accounting for Fedwire's security expenditures) is positive.

We also provide an impossibility result, namely that Fedwire cannot choose a level of security that induces a response by the private banks that generates the socially optimum level of security. Hence, some public intervention in the form of regulation is required to obtain a social optimum.

### 1.1 Literature

This paper contributes to the literature on the value of information (Feltham, 1968; Hirshleifer, 1978; Morris and Shin, 2002; Angeletos and Pavan, 2007), the economic literature on incentives involved with attacking blockchains (Biais, Bisiere, Bouvard, and Casamatta, 2019; Ebrahimi, Routledge, and Zetlin-Jones; Budish, 2018; Schilling, 2019; Huberman, Leshno, and Moallemi, 2021), the literature discussing the economic value of data as source of information (Begenau, Farboodi, and Veldkamp, 2018; Farboodi, Mihet, Philippon, and Veldkamp, 2019; Farboodi and Veldkamp, 2020, 2021; Farboodi, Singal, Veldkamp, and Venkateswaran, 2022) and the computer science literature on backups and redundancies (Ghaffarzadegan, 2008; Littlewood and Strigini, 2004; Jia, Xin, Wang, Guo, and Wang, 2018; AlZain, Soh, and Pardede, 2012).

## 2 Model

Unless specified, we consider one-period games. Later when adding the government, we consider two-stage games.

## 2.1 Entities and Information

Let $\mathcal{I}$ denote the set of all data. This can include payment information, such as transaction amounts, names of transactors, time and date stamps and any other customer information that might be recorded in the records of financial institutions. $\mathcal{N}$ is the set of all entities in the economy that observe information. In general these entities could include banks, central banks and, in the case of DLT systems, miners or proof-of-stake validators. Let $N = |\mathcal{N}|$ denote the number entities. A transaction requires a sender and a receiver where sending and receiving happens in the same time period. All transactions are truthful via electronic means. Therefore, every transaction is observed by at least one entity, and is observed by two entities if the sender and the receiver are customers of different entities.

Let $\mathcal{I}_i \subseteq \mathcal{I}$ denote the information observed by entity $i = 1, \dots N,\ i \in \mathcal{N}$. Observed information $\mathcal{I}_i$ is exogenous to $i$, that is, there is no data acquisition. A transaction $\tau$ is observed by bank $i \in \mathcal{N}$ if $\tau \in \mathcal{I}_i$.

## 2.2 Value of Information

Information $I_i$ is valuable to every entity $i \in \mathcal{N}$. Revenue $R(|I_i|)$ is strictly increasing in $|I_i|$, where $|\cdot|$ denotes the number of transactions in $I_i$. The value of information is homogeneous in the sense that revenue $R(|I_i|)$ only depends on the quantity of information $|I_i|$ and not on the content or quality of information $I_i$. Further, we assume revenue is independent of the number of entites that observe information $I_i$. An entity can earn revenue via information only if data $I_i$ is not compromised in the sense that either the data is not lost, or if it is lost, there exists at least one backup of the data. A backup stores information withour errors.

## 2.3 Attacks and Data Security

An attack on entity $i$ occurs when a malicious actor hacks the data base of entity $i$ and destroys its data (think of malware that corrupts the data set). If the lost data cannot be recovered from other entities in the system (see below), the firm loses revenue $R(|I_i|)$. Each entity chooses investment in data security to protect its information $I_i$ and therefore to reduce the chance of an attack. This gives rise to an important spill-over effect: entity $i$ knows about other entities that can serve as a backup of its information $I_i$ in case of an attack. Other entity's

investment in their data security has thus a positive spill-over effect on entity $i$, reducing its probability of data loss, and vice versa. This positive spill-over effect - on the other hand- will give rise to free-riding.

Let $c_i \geq 0$ denote entity $i$'s choice of investment in data security and let $f(|I_i|)$ denote the cost of one unit investment in data security. Investment in data security reduces profits by $-c_i \times f(|I_i|)$ and reduces the chance of an attack on entity $i$.

A successful attack on entity $i$ occurs with probability $\alpha(c_i) \in [0, 1]$, where $\alpha(\cdot)$ is twice differentiable, strictly decreasing and strictly convex in $i's$ investment in data security $c_i$. In addition, we make the following technical assumptions

**Assumption 2.1.** *It holds*
*(i).* $\lim_{c\to 0} \alpha(c) = 1$ *and* $\lim_{c\to\infty} \alpha(c) = 0$
*(ii).* $-\alpha'(0) = -\alpha'(0)(4\alpha(0) - 3\alpha^2(0)) > \frac{f(|I_i|)}{R(|I_i|)}$
*(iii).* $-\lim_{c\to\infty} \alpha'(c)(2\alpha(c) - \alpha^2(c)) = 0 < \frac{f(|I_i|)}{R(|I_i|)}$.

These assumptions can be relaxed but they lead to cases which are not empirically interesting. That is, these assumptions ensure that the cost of security is not so large that it never makes sense for banks to protect their data and no so infinitesimally small that they would choose an infinite amount of protection.

## 2.4 Data Recovery and chance of data loss

If an entity is successfully attacked, privacy is always lost but its data is not necessarily compromised.

**Definition 2.1** (Covers: Creating redundancy via backups)**.** *Entities $j = 1, \ldots m \in \mathcal{N}$, form a cover of information $I_i$ if their joint information sets include all the information in $I_i$*

$$I_i \subseteq \bigcup_{j=1}^{m} I_j,\ m < N,\ j \neq i \tag{1}$$

We rule out "on-us" transactions so that every transaction is across entities. Then a cover of $I_i$ is generated by the union of all the entities it transacts with. Likewise, there may be a third party, for instance, a payment infrastructure like Fedwire, that sees all the transactions. Suppose that all entities transact with all other entities. Then, in the case without Fedwire each data set $I_i$ would have

two covers: $I_i$ and $\bigcup_{j \neq i} I_j$ and in the latter case with Fedwire it would have three covers, where the third cover is the information set of the third party.

As an important property: If all transactions occur across entities, each transaction is observed by at least two parties. Therefore, the transaction matrix is complete. Therefore, data $I_i$ is non-recoverable only if *all* covers of $I_i$ are jointly successfully attacked. If at least one cover of $I_i$ was not attacked, then we assume that entity $i$ can recover data $I_i$ at zero costs via any one of its non-attacked covers.[1] The possibility of data recovery through third institutions creates an additional dimension for how entity's think about data. On the one hand, more data is more valuable and therefore better, and worth protecting more. On the other hand, data can be observed by multiple parties, and this redundancy lowers an institutions' incentive to protect data.

We can write firm revenue as

$$\Pi_i(I_i, c_i, \alpha(\cdot), c_1, \ldots, c_N) = (1 - \mathbb{P}(I_i \text{ compromised}))R(|I_i|) - c_i\, f(|I_i|) \quad (2)$$

where the probability that $i$'s data is compromised equals the probability that all covers of a (subset of) $i$'s data were successfully attacked, that is, $i$ loses access to some of its data.[2] At this point we cannot pin down the probability of data loss further since it varies depending on how much information an entity observes and by how many parties that information is observed. We therefore next proceed to considering concrete information systems.

# 3 Analysis: data protection in different information systems

We consider two models that approximate the information structures of real data systems. The first model assumes that every transaction is observed by exactly two institutions. There is no third party payment infrastructure that might additionally observe the data or the transaction data that is passed through the third party payment infrastructure is not sufficiently detailed to act as a cover for any entity, or imply a privacy breach. We call this the model with double covers and information segmentation, since no single entity forms a full cover,

[1] This would have to be a legal requirement (e.g. data protection act in health care), otherwise a hold-up problem would exist.

[2] Implicit is here the assumption that the reputational damage to losing access to a subset of data is sufficient to force the entity into bankrupty.

that is, observes all information. The second model introduces a third party infrastructure ("Fedwire") that perfectly observes all transaction data. This entity, which we denote by $F$, is run by the government and maximizes social welfare when choosing its level of protection. We call this the model with double covers and an optimally protected single-entity cover.

In our analysis, we focus on symmetric equilibria.

## 3.1 Double Covers with Information Segmentation

Assume there are exactly three entities $\mathcal{N} = \{A, B, C\}$ that observe information, and that each transaction is observed by exactly two entities, the sender and the receiver of a payment transaction. The results are generalised to any finite number of entities in the Appendix. Assume that A,B, and C have equal market share when it comes to transactions, that is, we assume symmetry $|I_A| = |I_B| = |I_C|$. The data structure is as depicted in Figure 1.

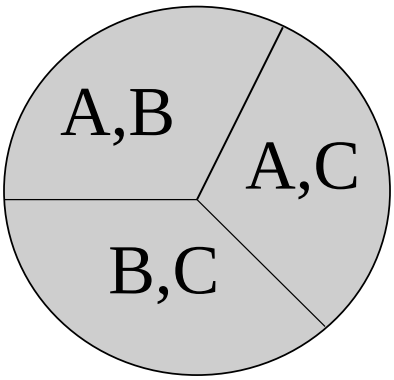



Figure 1: Each transaction in $I$ is observed by exactly two entities, the sender and the receiver.

### 3.1.1 Analysis of the private optimum

We focus on Bank A. Given our symmetric structure the same calculations can be applied to banks B and C. There are three scenarios under which the data of entity A is lost: A and B are attacked, A and C are attacked or all three are attacked. Hence, the probability of a data loss for bank A is given as the probability that either A and B are attacked or A and C are attacked, where the event that all banks are attacked is included in the event that only two banks are attacked. Thus, A's probability of a data loss equals

$$\alpha(c_A)\alpha(c_B) + \alpha(c_A)\alpha(c_C) - \alpha(c_A)\alpha(c_B)\alpha(c_C). \tag{3}$$

Here, one can see very nicely the spill-over effect of investment in data security: A's probability of a data loss very much depends on B's and C's investment in data security and vice versa since they mutually serve as backups. This is somewhat related to public goods provision by private parties.

The expected profits of entity A given expenditure $c_A$ is

$$\pi_A(c_A) = (1 - \alpha(c_A)\alpha(c_B) - \alpha(c_A)\alpha(c_C) + \alpha(c_A)\alpha(c_B)\alpha(c_C))\ R(|I_A|) - c_A f(|I_A|). \tag{4}$$

We abstract from limited liability. The first-order condition for an interior level of data security that maximizes profits of entity A is

$$\frac{\partial}{\partial c_A}\pi_A(c_A) = -\alpha'(c_A)(\alpha(c_B) + \alpha(c_C) - \alpha(c_B)\alpha(c_C))R(|I_A|) - f(|I_A|) = 0. \tag{5}$$

An interior private optimum for $A$ requires

$$-\alpha'(c_A^*)(\alpha(c_B) + \alpha(c_C) - \alpha(c_B)\alpha(c_C))R(|I_A|) = f(|I_A|) \tag{6}$$

By $|I_A| = |I_B| = |I_C|$, any private equilibrium $(c_A^*, c_B^*, c_C^*)$ must satisfy

$$\begin{aligned} &\alpha'(c_A^*)\left(\alpha(c_B^*) + \alpha(c_C^*) - \alpha(c_B^*)\alpha(c_C^*)\right) \\ &= \alpha'(c_B^*)\left(\alpha(c_A^*) + \alpha(c_C^*) - \alpha(c_A^*)\alpha(c_C^*)\right) \\ &= \alpha'(c_C^*)\left(\alpha(c_A^*) + \alpha(c_B^*) - \alpha(c_A^*)\alpha(c_B^*)\right) \end{aligned} \tag{7}$$

meaning that the FOC's of all entities are symmetric.

We have the following result.

**Proposition 3.1** (Double Covers - Private Equilibrium)**.** *Assume Assumptions 1-3 hold, and $\alpha(c)$ is strictly convex. Let $|I_A| = |I_B| = |I_C|$.*

*(i) There exists a unique symmetric private equilibrium $c_A^* = c_B^* = c_C^*$. The equilibrium expenditure level $c_A^*$ is interior, and characterized as the solution to*

$$-\alpha'(c_A^*)[2\alpha(c_A^*) - \alpha(c_A^*)^2] = \frac{f(|I_i|)}{R(|I_i|)}. \tag{8}$$

*If assumption 2.1(ii) does not hold, then $-\alpha'(0) < \frac{f(|I_A|)}{R(|I_A|)}$, and "no investment" arises as the unique private symmetric equilibrium, i.e., $c_i^* = 0$ for all $i$.*

*(ii) If $h(x) = \alpha(c)/\alpha'(x)$ is weakly decreasing, there exist no asymmetric interior*

*equilibria, and the symmetric interior equilibrium characterized as the solution to (8) is the only interior equilibrium.*

*(iii) If the attack probability satisfies* $-\alpha'(0) > f/R$*, and*

$$-\alpha'(0)\alpha(c)(2-\alpha(c)) < \frac{f}{R} \tag{9}$$

*where* $c$ *is the solution to* $-\alpha'(c) = \frac{f}{R}$*, there exists an asymmetric corner equilibrium* $(0, c, c)$*. In that equilibrium, one entity does not invest and the other entities invest symmetrically,* $c > 0$*, providing cover for the shirking institution.*

Proof (ii)
Consider the function

$$f(x,y,z) = -\alpha'(x)(\alpha(y)+\alpha(z)-\alpha(y)\alpha(z)) = -\alpha'(x)\left(\alpha(y)(1-\alpha(z))+\alpha(z)\right) \tag{10}$$

that describes the FOC's for entities A,B,C. Note that this function is symmetric in its last two arguments $f(x,y,z) = f(x,z,y)$, but is generically asymmetric in the first and second, respectively, the first and third argument, $f(x,y,z) \neq f(y,x,z)$ and $f(x,y,z) \neq f(z,y,x)$.

Assume there exists an asymmetric, interior equilibrium. That is, there exists $x \geq y \geq z \geq 0$ (wlog) with

$$f(x,y,z) = f(y,x,z) = f(z,y,x) = \frac{f(|I_i|)}{R(|I_i|)}. \tag{11}$$

This equation, in fact, contains three separate constraints. Let us consider the first constraint first. It holds $f(x,y,z) = f(y,x,z)$ if and only if

$$-\alpha'(x)\left(\alpha(y)(1-\alpha(z))+\alpha(z)\right) = -\alpha'(y)\left(\alpha(x)(1-\alpha(z))+\alpha(z)\right) \tag{12}$$

This equation is equivalent to

$$(1-\alpha(z))(\alpha'(y)\alpha(x)-\alpha'(x)\alpha(y)) + \alpha(z)(\alpha'(y)-\alpha'(x)) = 0 \tag{13}$$

It holds $(1-\alpha(z)), \alpha(z) \in [0,1]$, and $(\alpha'(y)-\alpha'(x)) \leq 0$ by $y \leq x$ and because $\alpha(\cdot)$ is convex. Moreover, $\alpha'(y)\alpha(x) - \alpha'(x)\alpha(y) \leq 0$ if

$$\frac{\alpha(x)}{\alpha'(x)} \leq \frac{\alpha(y)}{\alpha'(y)} \tag{14}$$

If the function $h(x) \equiv \frac{\alpha(x)}{\alpha'(x)}$ is weakly decreasing, then (14) holds by $x \geq y$. But then (13) has only the trivial solution $x = y$. By the same argument, $f(x, y, z) = f(z, y, x)$ if and only if

$$(1 - \alpha(y))(\alpha'(x)\alpha(z) - \alpha'(z)\alpha(x)) + \alpha(y)(\alpha'(x) - \alpha'(z)) = 0 \tag{15}$$

where $(\alpha'(x) - \alpha'(z)) \geq 0$ by $x \geq z$ and $\alpha'(x)\alpha(z) - \alpha'(z)\alpha(x) \geq 0$ iff $\frac{\alpha(z)}{\alpha'(z)} \geq \frac{\alpha(x)}{\alpha'(x)}$ which holds again if $h(x)$ is weakly decreasing. Thus, (15) has only the trivial solution $x = z$. (iii) Asymmetric corner equilibria: Consider the candidate equilibrium $c_A^* = 0$ and $c_B, c_C > 0$ interior. Given $c_A^* = 0$, B and C optimally set an interior level of data investment if their first order conditions hold. Because $\alpha(c_A^*) = \alpha(0) = 1$, B's profit function changes to

$$\Pi_B(c_B) = (1 - \alpha(c_B))R - c_B f \tag{16}$$

Thus, B's FOC equals

$$-\alpha'(c_B^*) = \frac{f}{R} \tag{17}$$

Likewise, for C

$$-\alpha'(c_C^*) = \frac{f}{R} \tag{18}$$

thus, $c_B^* = c_C^* = c^*$. If $-\alpha'(0) > f/R$, then the interior $c^*$ exists, see proof above. If $-\alpha'(0) \leq f/R$, $c^* = 0$.

From here on, assume $-\alpha'(0) > f/R$. Given these interior investments in data security, A's investment of zero, $c_A^* = 0$ is optimal only if

$$-\alpha'(c_A)\alpha(c)(2 - \alpha(c)) < \frac{f}{R}, \text{ for all } c_A > 0 \tag{19}$$

Because $\alpha(\cdot)$ is decreasing and convex, a sufficient condition for (19) is

$$-\alpha'(0)\alpha(c)(2 - \alpha(c)) < \frac{f}{R} \tag{20}$$

Because $-\alpha'(0) > f/R$, condition (20) can fail. Because $\alpha(c) \in (0, 1)$ and $(2 - \alpha(c)) \in (1, 2)$, condition (20) might hold. Thus, the asymmetric corner equilibrium $(0, c, c)$ can but does not have to exist.

### 3.1.2 Analysis of the social optimum

Now consider the social planner problem. The planner takes into account that the expenditure on data protection by any entity impacts the likelihood that another entity will suffer an unrecoverable data loss. In particular, the planner jointly chooses $c_A, c_B$, and $c_C$ to maximize the sum of bank profits.[3] The planner maximizes

$$\pi_P(c_A, c_B, c_C) = \pi_A + \pi_B + \pi_C \tag{21}$$

The first-order condition for an interior maximizer with respect to $c_A$ is

$$\begin{aligned}\frac{\partial}{\partial c_A}\pi_P(c_A, c_B, c_C) &= \frac{\partial}{\partial c_A}\pi_A(c_A, c_B, c_C) + \frac{\partial}{\partial c_A}\pi_B(c_A, c_B, c_C) + \frac{\partial}{\partial c_A}\pi_C(c_A, c_B, c_C) \\ &= -\alpha'(c_A)R(|I_A|)(2\alpha(c_B) + 2\alpha(c_C) - 3\alpha(c_B)\alpha(c_C)) - f(|I_A|) = 0\end{aligned} \tag{22}$$

where we have used the symmetry $|I_A| = |I_B| = |I_C|$. We obtain similar expressions for the first-order equations $\frac{\partial}{\partial c_B}\pi_P(c_A, c_B, c_C) = 0$ and $\frac{\partial}{\partial c_C}\pi_P(c_A, c_B, c_C) = 0$. Denote a solution of the system of first-order equations (ie a social optimum) by $(\hat{c}_A, \hat{c}_B, \hat{c}_C)$.

To characterize the social solution, note that the first-order conditions for the social optimum imply

$$\begin{aligned}&-\alpha'(c_A)(2\alpha(c_B) + 2\alpha(c_C) - 3\alpha(c_B)\alpha(c_C)) \\ &= -\alpha'(c_B)(2\alpha(c_A) + 2\alpha(c_C) - 3\alpha(c_A)\alpha(c_C)) \\ &= -\alpha'(c_C)(2\alpha(c_A) + 2\alpha(c_C) - 3\alpha(c_A)\alpha(c_C))\end{aligned} \tag{23}$$

We then have the following result.

**Proposition 3.2** (Double Covers: Social Optimum)**.** *Assume assumptions 2.1 holds, and assume $\alpha(c)$ is strictly convex. There exist a symmetric social optimum $\hat{c}_A = \hat{c}_B = \hat{c}_C$. This social optimum is interior, and characterized as the expenditure level that solves*

$$-\alpha'(\hat{c}_A)(4\alpha(\hat{c}_A) - 3\alpha(\hat{c}_A)^2) = \frac{f(|I_A|)}{R(|I_A|)}. \tag{24}$$

*If the function $-g(c) \equiv -\alpha'(c)\alpha(c)(4 - 3\alpha(c))$ crosses $f/R$ only once, the symmetric social optimum is unique. If assumption 2.1(i) and (iii) hold but not (ii), that is,*

[3] This calculation assumes that all consumer costs to data loss are reflected in bank profits. This would be true, for example, if banks were required to pay restitution to consumers equal to their damages.

$(-\alpha'(0)) < f/R$, *then the symmetric social optimum is zero investment* $\hat{c}_i = 0$, *and the social planner equilibrium is unique.*

A sufficient condition for $-g(c)$ crossing $f/R$ only once is when $g(c)$ is strictly increasing. In the example of section 5, the function $g(c)$ with $\alpha(c) = exp(-\beta c)$ is not strictly increasing. But one can can show single-crossing.

An interesting observation is, that if the social planner lets one entity invest much in data security, $c_C$ large, his investments via the remaining two institutions become substitutes. A larger investment $c_A$ would be compensated for by a reduction of $c_B$.

$$\frac{\partial}{\partial c_B}\frac{\partial}{\partial c_A}\pi_P(c_A, c_B, c_C) = -\alpha'(c_A)R(|I_A|)\alpha'(c_B)\left(2 - 3\alpha(c_C)\right) < 0 \tag{25}$$

for $\alpha(c_C) < 2/3$, i.e., for $c_C$ large. To see this substitutability, the social planner only requires investment via two institutions to attain a full cover of $I$ which appears to make the third institution redundant. This suggests that setting $c_B = 0$, and $c_A = c_C > 0$ might be socially optimal, giving rise to the possibility of an asymmetric social planner equilibrium. Indeed, the planner's marginal profit due to increasing $c_B$ becomes negative when both $c_A$ and $c_C$ are large:

$$\lim_{c_A, c_C \to \infty} \frac{\partial}{\partial c_B}\pi_P(c_A, c_B, c_C) = -f(|I_A|) < 0 \tag{26}$$

It however turns out that, depending on the attack function $\alpha(c)$ such an aymmetric equilibrium might not exist because $A$'s and $C$'s required investments would need to be too large to compensate for the lack of B's investment.[4]

We can now compare the solutions associated with the private equilibrium and the social optimum.

**Proposition 3.3** (Double Covers: Social versus Private Optimum)**.** *Assume assumptions A1-A3 hold, and assume* $\alpha(c)$ *is strictly convex. In the symmetric private equilibrium, there is strict under investment in data security relative to the symmetric social optimum;* $c_i^* < \hat{c}_i$, *for all* $i \in \{A, B, C\}$.

[4]To check for this asymmetric equilibrium with $c_B = 0$ and $c = c_C = c_A > 0$, the first order condition of the social planner becomes, $\frac{\partial}{\partial c_A}\pi_P(c, 0, c) = -\alpha'(c)R(|I_A|)(2 - \alpha(c)) - f(|I_A|) = 0$. The optimality of $c_B = 0$ requires $\frac{\partial}{\partial c_B}\pi_P(c, 0, c) = -\alpha'(0)(2\alpha(c_A) + 2\alpha(c_C) - 3\alpha(c_A)\alpha(c_C)) < \frac{f(|I_A|)}{R(|I_A|)}$ whereas optimality of $c_A = c_C = c > 0$ requires $-\alpha'(c)(2 - \alpha(c)) = \frac{f(|I_A|)}{R(|I_A|)}$. Jointly, the condition $-\alpha'(0)\alpha(c)(4 - 3\alpha(c)) < -\alpha'(c)(2 - \alpha(c))$ needs to be met for an asymmetric equilibrium to exist. The latter inequality can however fail because $4 - 3\alpha(c) > 2 - \alpha(c)$ by $\alpha(c) < 1$. In our example of section 5, $\alpha'(0)\alpha(c) = \alpha'(c)$ which rules out the possibility of an symmetric equilibrium with $c_B = 0$ and $c_A = c_C > 0$.

## 3.2 Fedwire: Double covers and an optimally protected single-entity cover

In the section above, we have seen that all entities underinvest in data security relative to the social optimum since they fail to internalize the impact of their investment on the other institutions' profits. Regulating investment in data security is tricky because the firms could simply understate the value of their data to the regulator. Therefore, we take a different approach. We are instead interested in whether the provision of a government layer of security improves overall data security. Or, can we increase overall data security in an incentive-compatible way by changing the information environment? Will Fedwire's inception improve overall data security given the reaction of all other private entities?

For that purpose, assume that each transaction is observed by the payor and the payee and that every transaction is also observed by a third party (eg Fedwire) $F$.

We consider a two-stage game: the third party (Fedwire) sets its security first and perfectly observably to all entities. Then the banks follow by simultaneously choosing their security levels in stage two. We consider symmetric subgame perfect equilibria where given the choice of Fedwire in stage 1, the entities choose their privately optimal level of data security in stage 2. Anticipating the private choices that follow in subgame $c_F$, Fedwire then optimizes welfare in stage 1.

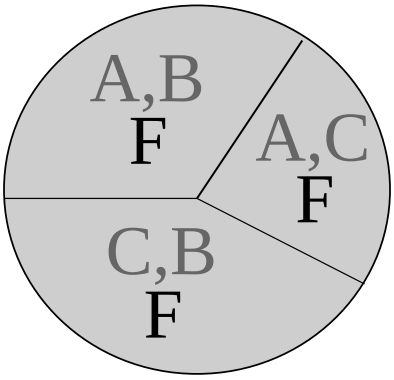



Figure 2: Each transaction is observed by two entities and the Fed.

### 3.2.1 Private security investment with Fedwire (Stage 2)

We begin by solving for the equilibrium of the subgame that is played by entities A,B and C taking as given the security choice by Fedwire, $c_F$.

Profits of entity A change to

$$\pi_A(c_A) = (1-\alpha(c_A)\alpha(c_F)(\alpha(c_B)+\alpha(c_C)-\alpha(c_B)\alpha(c_C)))\ R(|I_A|)-c_A\ f(|I_A|) \quad (27)$$

because Fedwire now additional provides one full cover. Importantly, Fedwire can also be attacked. It's probability of attack equals $\alpha(c_F)$. As an important feature of this modified information system, we allow Fedwire to walk away when it anticipates bad behavior that follows by private entities in stage 2: By setting $c_F = 0$, we nest the previous informan environment where Fedwire is absent. This is because $\alpha(0) = 1$. The first-order condition becomes

$$\frac{\partial}{\partial c_A}\pi_A(c_A) = -\alpha'(c_A)\alpha(c_F)(\alpha(c_B) + \alpha(c_C) - \alpha(c_B)\alpha(c_C))\ R(|I_A|) - \ f(|I_A|) = 0 \quad (28)$$

The FOCs for B and C are symmetric.

By the symmetry $|I_A| = |I_B| = |I_C|$, and using the same argument as the previous section, for every $c_F$ there exists a unique symmetric equilibrium of the subgame following $c_F$, $c_A^{*,F} = c_B^{*,F} = c_C^{*,F}$ on $[0, \infty)$ where all entities invest the same amount in data security. The symmetric equilibrium can be located at the boundary $\{0, \infty\}$.

**Proposition 3.4** (Private Optimum with Fedwire (stage 2)). *Assume $\alpha(c)$ is stricty convex and assumption 2.1 holds. For every choice of Fedwire's data security $c_F \geq 0$, there exist a unique private symmetric equilibrium $c_A^{*,F} = c_B^{*,F} = c_C^{*,F}$ in $[0, \infty)$.*
*(i) The unique symmetric private equilibrium following $c_F$ is interior and finite if*

1. $-\alpha'(0) > \frac{1}{\alpha(c_F)}\frac{f(|I_i|)}{R(|I_i|)}$ *and*
2. $-\lim_{c\to\infty}\alpha'(c)(2\alpha(c) - \alpha^2(c)) < \frac{1}{\alpha(c_F)}\frac{f(|I_i|)}{R(|I_i|)}$ *hold.*

*In that case, the unique symmetric private equilibrium $c_A^{*,F}$ in the subgame $c_F$ is characterized as the solution to*

$$-\alpha'(c_A^{*,F})[2\alpha(c_A^{*,F}) - \alpha(c_A^{*,F})^2] = \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)} \quad (29)$$

*(ii) If for given $c_F$ it holds $-\alpha'(0) \leq \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$, then the unique symmetric private equilibrium following $c_F$ is the "noinvestment" equilibrium where no bank invests,*

$c^* = 0$.
*(iii) By assumption 2.1 and given $c_F$, the unique symmetric private equilibrium cannot be at $c^* = \infty$.*

From equation (29) it is apparent that whenever the symmetric equilibrium is interior it varies substantially in Fedwire's choice of data security $c_F$. Via its choice $c_F$, Fedwire can therefore steer the symmetric equilibrium $c^*$ that follows in the subgame.

**Lemma 3.1.** *Assume $\alpha(c)$ is stricty convex and assumption 2.1 holds. Assume the subgame $c_F$ gives rise to the interior symmetric equilibrium $c_A^{*,F} = c_B^{*,F} = c_C^{*,F}$. Then the change of the interior symmetric equilibrium due to a marginal change in the subgame $c_F$ is given as*

$$\frac{\partial c_A}{\partial c_F} = \frac{\frac{\alpha'(c_F)}{\alpha^2(c_F)}}{\alpha''(c_A)\alpha(c_A)[2-\alpha(c_A)] + 2[\alpha'(c_A)]^2(1-\alpha(c_A))]} \frac{f(|I_A|)}{R(|I_A|)} < 0, \text{ for all } c_f \in [0,\infty) \tag{30}$$

Lemma 3.1 shows that the private institutions free-ride on Fedwire's investment in data security, reducing their private investment as Fedwire scales up the security of the third layer.

To see the result, consider the function

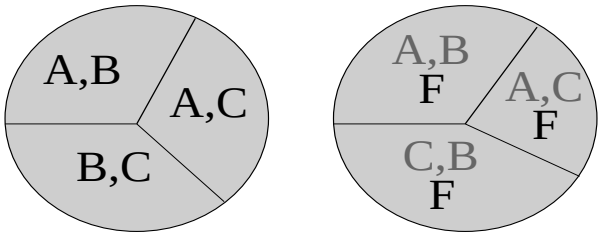
$$F(c_A, c_F) = \frac{1}{\alpha(c_F)} \frac{f(|I_A|)}{R(|I_A|)} + \alpha'(c_A)[2\alpha(c_A) - \alpha(c_A)^2] \tag{31}$$

Consider condition (29) for an interior private equilibrum in the Fedwire case. For every subgame $c_F$, the zeros to the implicit function $F(c_A(c_F), c_F) = 0$ describe the symmetric equilibrium. Via the implicit function theorem, the change of the symmetric equilibrium due to a change in the subgame $c_F$ is given as $\frac{\partial c_A}{\partial c_F} = -\frac{\frac{\partial F}{\partial c_F}}{\frac{\partial F}{\partial c_A}}$ yielding the result above.

Lemma 3.1 implies an important proposition.

**Proposition 3.5** (Double Covers versus Fedwire: Free-riding on the Fed)**.** *When adding Fedwire as an additional cover, in the unique symmetric private equilibrium all banks shirk by reducing their investment in data security, $c_i^* \geq c_i^{*,F}$ for all $i \in \{A, B, C\}$, whatever the choice of $c_F$. Further, $c_i^* > c_i^{*,F}$ if the unique symmetric private equilibrium with Double Covers is interior $c_i^* > 0$ .*

The proposition follows from the lemma because the privately optimal investment in data security without Fedwire corresponds to the privately optimal




(a) Double Covers (b) with Fedwire

investment in data security with Fedwire, but where Fedwire decides not to invest, $c_A^{*,priv,Fed}(0) = c_A^{*,priv}$. This is by design of our environment. Lemma 3.1 shows that $c_A^{*,priv,Fed}(c_F) \leq c_A^{*,priv,Fed}(0)$. When additionally considering the insights of Proposition 3.3, we get the following ordering of optimal investments:

$$c_A^{*,priv,Fed}(c_F) \leq c_A^{*,priv,Fed}(0) = c_A^{*,priv} < c_A^{*,soc}, \quad \text{for any } c_F > 0 \tag{32}$$

The privately optimal investment in the Fedwire case is not only below the privately optimal investment without Fedwire but, in particular, below the socially optimal investment in the Double Covers case without Fedwire.

### 3.2.2 The optimal security choice of Fedwire (Stage 1)

Next we solve the stage 1 game, where Fedwire seeks to maximise social welfare by optimally choosing $c_F$, taking as given the privately optimal security choices that follow by the banks in stage 2. Fedwire chooses $c_F$ to maximize joint profits accounting for its own data security costs:

$$\begin{aligned}&\pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F)\\ &= \pi_A(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) + \pi_B(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) + \pi_C(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) - c_F\ f(|I|)\end{aligned} \tag{33}$$

In this section, we analyze to what extent Fedwire can impact the selection of the private equilibrium that follows in the subgame. Fist, let us consider corner equilibria:

Reconsider asummption 2.1. Consider the case where assumption 2.1(ii) is violated. That is, $-\alpha'(0) < \frac{f(|I_i|)}{R(|I_i|)}$. That means, a small investment in data security reduces the attack probability only slowly.

**Theorem 3.1** (Impossibility Theorem)**.** *Let assumption 2.1(i) and (iii) hold. If $-\alpha'(0) < \frac{f(|I_A|)}{R(|I_A|)}$, then "no investment" is the unique symmetric private equilibrium in both settings with and without Fedwire. Put differently, no Fedwire choice $c_F \in$*

$[0, \infty]$ *can deter the unique symmetric " no investment" equilibrium at* $c^* = 0$.

This Theorem is the first indicator that adding Fedwire as a third cover is not always a powerful tool to enhance overall investment in data security. The condition $-\alpha'(0) < \frac{f(|I_A|)}{R(|I_A|)}$ means that a small investment in data security close to zero does not reduce that attack probability fast.

Theorem 3.1 (ii) says that if "no-investment" is the unique symmetric equilibrium in the setting without Fedwire, then "no-investment" remains the unique symmetric equilibrium in the setting with Fedwire, whatever investment choice $c_F$. As a consequence, the presence of Fedwire can only improve the efficiency of the outcome. The result depends on the assumption that $\alpha(0) = 1$ and $\lim_{c\to\infty} \alpha(c) = 0$. If instead the cost function satisfied $\alpha(0) \neq 1$, then the presence of Fedwire could potentially make outcomes worse than in the setting where Fedwire is not present.

**Theorem 3.2** (Socially optimal Fedwire provision)**.** *Assume the attack probability* $\alpha(c)$ *is convex and assumption 2.1(i) and (iii) hold.*
*(i) Assume* $-\alpha'(0) < \frac{f(|I_A|)}{R(|I_A|)}$ *so that* $c_i^* = 0$ *is the unique symmetric private equilibrium following all* $c_F \geq 0$.
*(ia) If* $(-\alpha'(0)) \in (0, \frac{f(|I|)}{3R(|I_A|)}]$ *it is socially optimal to not provide Fedwire,* $c_F^* = 0$.
*(ib) If* $(-\alpha'(0)) \in (\frac{f(|I|)}{3R(|I_A|)}, \frac{f(|I_A|)}{R(|I_A|)}]$, *implementing Fedwire creates value* $c_F^* > 0$.
*(ii) Assume* $-\alpha'(0) > \frac{f(|I_A|)}{R(|I_A|)}$ *so that absent Fedwire the banks play an interior symmetric private equilibrium* $c_i^* > 0$. *Then,*

$$\frac{\alpha'(0)}{\alpha'(c_i^*)/\alpha(c_i^*)} - \frac{1}{3} > 0. \tag{34}$$

*is a necessary condition for Fedwire to optimally set* $c_F^* > 0$.

Important for understanding the Theorem is that Fedwire's optimal choice $c_F^* = 0$ means the setting endogenously reduces to the case of Double Covers analyzed in section 3.1. It means, the conditions of the information system and its costs are such that Fedwire optimally walks away and does not provide the third cover, implying the private entities are on their own when it comes to protecting their data.

The intuition behind the Proposition is as follows. The private entities and Fedwire adjust their optimal behavior depending on how fast the attack probability declines in investment in data security. On (i), if the attack probability $\alpha(c)$ declines slowly for small levels of investment in data security all private

entities decide to optimally not invest, independently of what Fedwire does. Fedwire faces the same attack probability $\alpha(c)$ as the private entities. If the attack probability declines particularly slow in the investment in data security, (ia), then also Fedwire abstains from investment since the monetary costs of investing do not justify the benefits. Recall that when Fedwire abstains, the setting is equivalent to the Double Covers setting studied in section 3.1.

If the attack probability declines slightly faster in investment, the private entities still do not invest but Fedwire does. In that case, the monetary costs of investing exceed the benefits of providing the third cover, and thus more security to all entities. Since the private entities do not invest they cannot react to Fedwires' investment by shirking. On (ii), if the attack probability declines even faster the private entities do invest. As the appendix in the proof shows, Fedwire's marginal change in profit due to a marginal increase in data security investment consists of three terms

$$\begin{aligned}&\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_F)\\&= 3R(|I_A|)\Big[\frac{f(|I|)}{R(|I_A|)}\left(\frac{\alpha'(c_F)/\alpha(c_F)}{\alpha'(c_A)/\alpha(c_A)}-\frac{1}{3}\right)+\frac{\partial c_A}{\partial c_F}\alpha(c_F)\,(-\alpha'(c_A))2\alpha(c_A)(1-\alpha(c_A))\Big]\end{aligned} \tag{35}$$

The first term in (45) involving the expression $\frac{\alpha'(c_F)/\alpha(c_F)}{\alpha'(c_A)/\alpha(c_A)}$ captures the increase in expected profits to all three firms as Fedwire increases security by providing the third layer. This term is always positive. The second term involving $-\frac{1}{3}$ is negative and captures the increase in monetary costs as investment in data security goes up. The third term involving the expression $\frac{\partial c_A}{\partial c_F}$ is negative and captures that all private entites reduce their investment in data security due to Fedwire's increase in investment (free-riding), see Lemma 3.1. Fedwire's investment in data security is optimal only if the monetary costs and the extent of free-riding is not too intense relative to the benefit of increased security and resulting higher profits. A necessary condition for that to hold is inequality (34) which implies that the first and second term in the marginal profit function of Fedwire are positive, that is, $\frac{\alpha'(c_F)/\alpha(c_F)}{\alpha'(c_A)/\alpha(c_A)}-\frac{1}{3}>0$ for $c_F$ close to zero. As we show in the proof, the inequality holds if $c_i^*$ is sufficiently small. Yet, this difference between the first and second term still needs to be traded off against the third, negative term.

Since the Fed's goal is to maximize welfare and choosing $c_F = 0$ is an option, the follow corollary follows immediately.

**Corollary 3.1.** *In cases where Fedwire chooses $c_F^* > 0$ their presence in the system is welfare improving relative to the Double Cover case where Fedwire is absent.*

# 4 Welfare compared across Information Systems I

What remains to be seen is whether Fedwire can achieve the social optimum through its own choice of data security investment. In this section, we investigate whether welfare in the constrained optimally protected Fedwire information system can reach or even exceed welfare obtained in the solution to the planners problem without Fedwire. The two underlying information systems differ since in the Fedwire case each transaction is observed by three parties, if Fedwire indeed invests, relative to the Double Cover case where every transaction is observed by two parties. We only consider symmetric equilibria as before. Welfare in the Fedwire case exceeds welfare at the socially optimal investment in the Double Cover case (without Fedwire) if and only if

$$3\,\Pi_A(c_A^{*,soc}, c_B^{*,soc}, c_C^{*,soc}) \leq 3\,\Pi_A(c_F^*, c_A^{*,F}, c_B^{*,F}, c_C^{*,F}) - c_F^* f(|I|) \tag{36}$$

Recall, every planner equilibrium is symmetric via $c_A^{*,soc} = c_C^{*,soc}, c_B^{*,soc} = 0$, whereas we impose symmetry for the private Fedwire equilibrium, $c_A^{*,F} = c_B^{*,F} = c_C^{*,F}$. If $(-\alpha'(0)) > f/R$, both equilibria are interior. Plugging into (**??**), (4), (27) and (33) we can rewrite this inequality as

$$\underbrace{(3 - 4\alpha(c_A) + \alpha(c_A)^2)R - 2c_A f}_{=\Pi_P^{DC,Soc}(c_i^{*,soc})} \tag{37}$$

$$\leq \underbrace{3\left[(1 - 2\alpha^2(c_A^F)\alpha(c_F) + \alpha^3(c_A^F)\alpha(c_F))R(|I_A|) - c_A^F f(|I_A|)\right] - c_F\, f(|I|)}_{=\Pi_P^{Fed}(c_F^*, c_i^{*,F})} \tag{38}$$

We obtain

**Theorem 4.1** (Socially optimal Double Cover versus Fedwire)**.** *Assume the attack probability $\alpha(c)$ is convex and assumption 2.1(i) and (iii) hold.*
*(i) If $(-\alpha'(0)) \in (0, \frac{f(|I|)}{3R(|I_A|)}]$ welfare in the case with Fedwire and welfare in the social optimum with Double Covers are both zero, and thus equal, $\Pi_P^{Fed} = 0 = \Pi_P^{DC,Soc}$.*
*(ii) If $(-\alpha'(0)) \in (\frac{f(|I|)}{3R(|I_A|)}, \frac{f(|I_A|)}{R(|I_A|)}]$, then*

$$\Pi_P^{Fed} > \Pi_P^{DC,Soc} = 0 \tag{39}$$

*(iii) Assume* $-\alpha'(0) > \frac{f(|I_A|)}{R(|I_A|)}$*, then either can dominate the other.*

In the case (i), the attack probability declines so slowly with the investment in data security that no party in either scenario—neither private entities, Fedwire, nor the social planner in the Double Cover case— invests in data security. Thus, welfare is zero in both information systems and therefore equal.

In the case of (ii) the attack probability declines still slowly with a marginal investment in data security. Therefore, the social planner in the Double Cover case still does not invest, and welfare in that system is optimally zero. For the Fedwire case, the private institutions optimally do not invest, but Fedwire invests. Therefore, welfare in the optimally protected Fedwire case exceeds welfare in the socially optimally protected Double Cover case. This might be surprising at first. Note, however, that the Double Cover case and the Fedwire case differ substantially since Fedwire provides an entire cover via its single investment, whereas the social planner in the Double Cover case symmetrically invests in three partially overlapping but incomplete[5] information sets at the same time.

In the case (iii), the attack probability declines rapidly such that the social planner in the Double Cover case sets an interior investment in data security, $c_i^{*,soc} > 0$. Likewise, the private instutions in the Fedwire case invest $c_i^{*,Fed} > 0$, and Fedwire may or may not invest.

# 5 Example

Consider the attack probability function $\alpha(c) = e^{-\beta c}$. This function is positive, decreasing, convex, with $\alpha(0) = 1$, $\alpha(c) \to 0$ as $c \to \infty$, and $\alpha(c) \in [0, 1]$ for all $c \geq 0$. It holds $-\alpha'(0) = \beta$ so that for different $\beta \in (0, \infty)$ we can scale the speed at which the attack probability falls in the data security investment. We set $R = 1,\ f = 0.5$.

## 5.1 Private and Social planner equilibrium Double Covers

The unique symmetric private equilibrium $c_A^*$ in the Double Covers case is given by

- If $(-\alpha'(0)) = \beta > f/R$, $c_A^*$ is given as the solution to (8), that is,

[5]Here incomplete means that no entity observes all transactions at the same time whereas Fedwire observes everything.

$$\beta e^{-2\beta c_A^*}[2 - e^{-\beta c_A^*}] = \frac{f(|I_i|)}{R(|I_i|)}. \tag{40}$$

- If $(-\alpha'(0)) = \beta \leq f/R$, $c_A^* = 0$.

The equilibrium condition for the social planner becomes

- Double Covers (No Fedwire): If $(-\alpha'(0)) = \beta > f/R$, socially optimal investment $c_A^*$ solves

$$\beta\, e^{-2\beta c_A}(4 - 3e^{-\beta c_A}) = \frac{f(|I_A|)}{R(|I_A|)} \tag{41}$$

The social planner equilibrium is unique in this example because the function $-g(c) = -\alpha'(c)\alpha(c)(4 - 3\alpha(c))$ crosses the value $f/R$ only once, see Proposition 3.2.[6]

If $(-\alpha'(0)) = \beta < f/R$, the social planner sets $c_A^* = 0$.

## 5.2 Fedwire equilibrium

### 5.2.1 Case of interior private optimum

- Given Fedwire's investment $c_F$ satisfies, $-\alpha'(0) = \beta > \frac{1}{\alpha(c_F)} \frac{f(|I_i|)}{R(|I_i|)}$, the privately optimal investment $c_A^F$ is interior by Proposition 3.4, and given as the solution to

$$\beta\, e^{-2\beta c_A^F}(2 - e^{-\beta c_A^F})e^{-\beta c_F} = f(|I_A|)/R(|I_A|) \tag{42}$$

- Since at the given $c_F$ the private optimum is interior $c_A^* > 0$, the equilibrium change in the privately optimal investment $c_A^F$ due to a marginal change in $c_F$ is given by Lemma 3.1 as

$$\frac{\partial c_A^F}{\partial c_F} = \frac{-e^{\beta\, c_F}}{\beta\, e^{-2\beta\, c_A^F}(4 - 3e^{-\beta\, c_A^F})} \frac{f}{R} \tag{43}$$

[6] To see this, note that $g(c) = -\beta e^{-2\beta c}(4 - 3e^{-\beta c})$. Thus $g'(c) = \beta^2 e^{-2\beta c}(8 - 9e^{-\beta c})$. The factor $\beta^2 e^{-2\beta c}$ is always positive. The bracket is positive if and only if $c > \frac{1}{\beta} \ln\left(\frac{9}{8}\right)$. Thus, $-g(c)$ decreases if and only if $c > \frac{1}{\beta} \ln\left(\frac{9}{8}\right)$. Because $-g(0) = \alpha'(0) > f/R$ by assumption, and because $-\lim_{c\to\infty} g(c) = 0 < f/R$, the function $-g(c)$ starts at a value above $f/R$ at zero, increases strictly away from that value until it reaches its maximum at $c = \frac{1}{\beta} \ln\left(\frac{9}{8}\right)$, then decreases strictly for all $c > \frac{1}{\beta} \ln\left(\frac{9}{8}\right)$, eventually crossing $f/R$ once, and approaching zero as $c$ gets large.

- Because at the given $c_F$ the private optimum is interior $c_A^* > 0$, the first order condition for the optimal Fedwire choice $c_F^*$ as a function of $c_A^*$ is given by (174) and becomes

$$\begin{aligned}
&\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_F) \\
&= 3R(|I_A|)\frac{f(|I|)}{R(|I_A|)}\Big[\frac{2}{3} + 2\frac{-e^{\beta\, c_F}e^{-\beta\, c_F}}{(4-3e^{-\beta\, c_A^F})}\,(\frac{e^{-2\beta\, c_A^F}}{e^{-2\beta\, c_A^F}})(1-e^{-\beta\, c_A^F})\Big] \qquad (44)\\
&= 6f(|I|)\,\Big[\frac{1}{3} - \frac{(1-e^{-\beta\, c_A^F})}{(4-3e^{-\beta\, c_A^F})}\Big] \qquad (45)
\end{aligned}$$

since $\alpha'(c)/\alpha(c) = -\beta$, $\frac{\alpha'(c_F)/\alpha(c_F)}{\alpha'(c_A)/\alpha(c_A)} = 1$. Note that this derivative is independent of $c_F$.

### 5.2.2 Case of private corner equilibrium

- If Fedwire's investment $c_F$ satisfies $-\alpha'(0) = \beta < \frac{1}{\alpha(c_F)}\frac{f(|I_i|)}{R(|I_i|)}$, the privately optimal investment is at zero $c_A^F = 0$ by Proposition 3.4. This holds in particular, if $-\alpha'(0) = \beta < \frac{f(|I_i|)}{R(|I_i|)}$.

- If for given $c_F$ the private optimum is at zero $c_A^* = 0$, the equilibrium change in the privately optimal investment $c_A^F$ due to a marginal change in $c_F$ is also zero since all banks shirk and cannot invest less than zero.

$$\frac{\partial c_A^F}{\partial c_F} = 0 \qquad (46)$$

- Because the private optimum is at $c_A^* = 0$, the first order condition for the optimal Fedwire choice $c_F^*$ as a function of $c_A^*$ is given by (168) and becomes

$$\begin{aligned}
&\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) \\
&= -3\alpha^2(c_A)\alpha'(c_F)\; R(|I_A|)\Big(2-\alpha(c_A)\Big) - f(|I|) \qquad (47)\\
&= -3\alpha'(c_F)\; R(|I_A|) - f(|I|) \qquad (48)
\end{aligned}$$

since $\frac{\partial c_A^F}{\partial c_F} = 0$, and $\alpha(0) = 1$. Note that this derivative now depends on $c_F$.

## 5.3 Solving the example for different attack probabilities beta

We now solve explicitly for the equilibria depending on the given attack probability function $\alpha(c) = e^{-\beta c}$, parametrized by beta.

**Corollary 5.1** (Fedwire equilibria of the example)**.** *Consider the attack probability function $\alpha(c) = e^{-\beta c}$.*
*(i) If $\beta \in \left(0, \frac{f(|I_i|)}{3R(|I_i|)}\right]$, the private symmetric equilibrium equals $c_A^* = 0$ and Fedwire optimally sets $c_F^* = 0$.*
*(ii) If $\beta > \frac{f(|I_i|)}{3R(|I_i|)}$, the private symmetric equilibrium equals $c_A^* = 0$ and Fedwire optimally sets $c_F^* = \left(-\frac{1}{\beta}\right) \ln\left(\frac{f}{3R\beta}\right) > 0$.*

We include the solution to the example, i.e., the proof of the Corollary in the main text for expositional purpose.

**Case 1:** $-\alpha'(0) = \beta \in (0, \frac{f(|I_i|)}{R(|I_i|)}]$.

In this case it follows that $\beta \leq \frac{1}{\alpha(c_F)} \frac{f(|I_i|)}{R(|I_i|)})$ for all $c_F \geq 0$.

- Then by the instructions above, $c_A^* = 0$, and $\frac{\partial c_A^F}{\partial c_F} = 0$.
- Therefore, $\frac{\partial}{\partial c_F} \pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) = 3\beta e^{-\beta c_F}\ R(|I_A|) - f(|I|)$.

  It holds $\frac{\partial}{\partial c_F} \pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) > 0$ if and only if $c_F < \left(-\frac{1}{\beta}\right) \ln\left(\frac{f}{3R\beta}\right)$. If $\beta \in (0, \frac{f}{3R})$, then $\ln\left(\frac{f}{3R\beta}\right) > 0$. Thus, there exists no positive $c_F$ with $c_F < \left(-\frac{1}{\beta}\right) \ln\left(\frac{f}{3R\beta}\right)$, implying $\frac{\partial}{\partial c_F} \pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) < 0$ for all $c_F \geq 0$. Thus, $c_F^* = 0$. If $\beta \in (\frac{f}{3R}, \frac{f}{R})$, then $\ln\left(\frac{f}{3R\beta}\right) < 0$, and $c_F^* = \left(-\frac{1}{\beta}\right) \ln\left(\frac{f}{3R\beta}\right) > 0$.
- To verify that we have indeed found an equilibrium, see that for the case $\beta \in (0, \frac{f}{3R})$ with $c_F^* = 0$, respectively for the $\beta \in (\frac{f}{3R}, \frac{f}{R})$ with $c_F^* = \left(-\frac{1}{\beta}\right) \ln\left(\frac{f}{3R\beta}\right)$ it holds $\beta < \frac{1}{\alpha(c_F*)} \frac{f(|I_i|)}{R(|I_i|)})$, and thus $c_A^* = 0$ is optimal in either case. We conclude, if $\beta \in (0, \frac{f}{3R})$, the equilibrium equals $(c_A^*, c_F^*) = (0, 0)$ whereas in the case $\beta \in (\frac{f}{3R}, \frac{f}{R})$ the equilibrium equals $(c_A^*, c_F^*) = (0, \left(-\frac{1}{\beta}\right) \ln\left(\frac{f}{3R\beta}\right))$.

**Case 2:** $-\alpha'(0) = \beta > \frac{f(|I_i|)}{R(|I_i|)}$.

In this case we can follow that there exists a cut-off $\bar{c}_F$ such that

$$\beta = \frac{1}{\alpha(\bar{c}_F)} \frac{f(|I_i|)}{R(|I_i|)}) \tag{49}$$

Therefore, $\beta < \frac{1}{\alpha(c_F)} \frac{f(|I_i|)}{R(|I_i|)})$ for $c_F > \bar{c}_F$ and $\beta > \frac{1}{\alpha(c_F)} \frac{f(|I_i|)}{R(|I_i|)})$ if $c_F < \bar{c}_F$. Plugging in the exponential function for $\alpha(c)$, it holds

$$\bar{c}_F = \frac{1}{\beta} \ln \left( \frac{\beta R}{f} \right) \tag{50}$$

**Case 2a:** Assume $c_F \geq \bar{c}_F$, and thus $\beta \leq \frac{1}{\alpha(c_F)} \frac{f(|I_i|)}{R(|I_i|)})$.

- Then, $c_A^* = 0$ and $\frac{\partial c_A^F}{\partial c_F} = 0$.
- Therefore, as above, $\frac{\partial}{\partial c_F} \pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) = 3\beta e^{-\beta c_F} \; R(|I_A|) - f(|I|)$.

- It holds $\frac{\partial}{\partial c_F} \pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F) > 0$ if and only if $c_F < \left(-\frac{1}{\beta}\right) \ln \left(\frac{f}{3R\beta}\right)$.

  Because $\beta > f/R$, it follows $\ln \left(\frac{f}{3R\beta}\right) < \ln \left(\frac{1}{3}\right) < 0$, and $c_F^* = \left(-\frac{1}{\beta}\right) \ln \left(\frac{f}{3R\beta}\right) > 0$.

- To verify whether we have indeed found an equilibrium, we need to verify that $c_F^* = \left(-\frac{1}{\beta}\right) \ln \left(\frac{f}{3R\beta}\right) \geq \bar{c}_F$. If that is the case, then indeed, $c_A^* = 0$ is optimal and $(c_A^*, c_F^*) = (0, \left(-\frac{1}{\beta}\right) \ln \left(\frac{f}{3R\beta}\right))$ is an equilibrium for $\beta > f/R$.

  It holds $c_F^* \geq \bar{c}_F$ if and only if

$$\left(-\frac{1}{\beta}\right) \ln \left(\frac{f}{3R\beta}\right) \geq \frac{1}{\beta} \ln \left(\frac{\beta R}{f}\right) \tag{51}$$

  which is equivalent to $\ln(3\beta R) \geq \ln(\beta R)$. But this is always true because the logarithm is monotone increasing. Thus, $(c_A^*, c_F^*) = (0, \left(-\frac{1}{\beta}\right) \ln \left(\frac{f}{3R\beta}\right))$ is an equilibrium for $\beta > f/R$.

**Case 2b (interior case):** Fix any $c_F < \bar{c}_F$, and thus $\beta > \frac{1}{\alpha(c_F)} \frac{f(|I_i|)}{R(|I_i|)})$.

- Then $c_A^* > 0$ and is given as the solution to

$$\beta \, e^{-2\beta c_A^F} (2 - e^{-\beta c_A^F}) e^{-\beta c_F} = f(|I_A|)/R(|I_A|) \tag{52}$$

  Note, the solution $c_A^* > 0$ depends on the choice of $c_F$.

- Moreover, as Fedwire increases its investment the private entities shirk, $\frac{\partial c_A^F}{\partial c_F} < 0$ where

$$\frac{\partial c_A^F}{\partial c_F} = \frac{-e^{\beta\, c_F}}{\beta\, e^{-2\beta\, c_A^F}(4 - 3e^{-\beta\, c_A^F})} \frac{f}{R} < 0 \tag{53}$$

- Fedwire's FOC changes to

$$\begin{aligned}
&\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_F) \\
&= 3R(|I_A|)\frac{f(|I|)}{R(|I_A|)}\Big[\frac{2}{3} + 2\frac{-e^{\beta\, c_F}e^{-\beta\, c_F}}{(4 - 3e^{-\beta\, c_A^F})}\,(\frac{e^{-2\beta\, c_A^F}}{e^{-2\beta\, c_A^F}})(1 - e^{-\beta\, c_A^F})\Big] \qquad (54)\\
&= 6f(|I|)\,\Big[\frac{1}{3} - \frac{(1 - e^{-\beta\, c_A^F})}{(4 - 3e^{-\beta\, c_A^F})}\Big] \qquad (55)
\end{aligned}$$

  This equation only depends on $c_A$ and is strictly positive for any $c_A \geq 0$, i.e. cannot become zero or negative. To see this, it holds

$$\frac{1}{3} \geq \frac{(1 - e^{-\beta\, c_A^F})}{(4 - 3e^{-\beta\, c_A^F})} \tag{56}$$

  if and only if

$$4 - 3e^{-\beta\, c_A^F} \geq 3 - 3e^{-\beta\, c_A^F} \tag{57}$$

  iff $1 > 0$.

- To calculate the equilibrium, we plug the private solution $c_A^* > 0$ from (52) into (55), and verify that $\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_F) > 0$. But this means that $c_F < \bar{c}_F$ is not optimal. We need to marginally increase $c_F$. As $c_F$ increases towards $\bar{c}_F$, this will cause $c_A^*$ to decline by $\frac{\partial c_A^F}{\partial c_F} < 0$. Eventually $c_A^*$ hits zero as $c_F = \bar{c}_F$. The decline in $c_A^*$ will not impact the sign of $\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_F) > 0$, thus $c_F = \bar{c}_F$ is optimal. But $c_F = \bar{c}_F$ implies $c_A^* = 0$. Thus, we are back to the case 2a.

Overall, we have shown that there exists no equilibrium with $c_F < \bar{c}_F$ when $\beta > f/R$. We have also shown that for any attack probability $\alpha(c) = exp(-\beta c)$, $\beta > 0$ there exists no Fedwire equilibrium where the private entities invest. There exists no interior private equilibrium with Fedwire because Fedwire always finds it beneficial to protect, $\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_F) > 0$, independently of what the private entities do. The private entities respond by shirking down to zero, see Figure 4. . This is related to the particular shape of our attack probability function. Note, however, that in the case $\beta > f/R$ the private entities do invest, $c_A^* > 0$, if Fedwire is absent (Double Covers case), see Figure 4.

## 5.4 Simulation and discussion

In Figure 4, the optimal investment in data security is depicted across varying individual attack probabilities $\alpha(c) = e^{-\beta c}$. As $\beta$ increases along the x-axis, the rate at which the attack probability diminishes accelerates for marginal investments in data security. This means that as $\beta$ attains larger values, investing in data security yields increasingly high "security returns".

Generically, private institutions that operate without the support of Fedwire (Double Covers) invest less compared to the socially optimal benchmark. Furthermore, and as anticipated, the private institutions that operate next to Fedwire invest less, effectively zero, relative to the case where Fedwire is absent. Recall that the setting with private institutions but without Fedwire can be interpreted as the setting with private institutions and Fedwire but where Fedwire commits to not invest, thus, abstaining from providing the third cover. Consequently, Fedwire's strategic decision to provide the third cover, triggers a cascade effect leading all private institutions to curtail their investments to zero.

Furthermore, the graph illustrates an intriguing observation: the social planner may allocate a greater investment in data security compared to Fedwire when the parameter $\beta$ is approximately $f/R = 0.5$. However, for $\beta \geq f/R$, Fedwire's investment surpasses that of the social planner. This phenomenon may initially seem counterintuitive; however, it is important to recall that in the symmetric optimum, the social planner distributes data security investments across all three institutions to provide two covers, incurring the cost function for security investment threefold. In contrast, Fedwire provides an entire cover for all data via one single investment, thus incurring the cost only once.

It is worth noting, as demonstrated earlier in the analysis of the Double Covers case, that the social planner in this scenario optimally chooses to provide both covers. Hence, it is not socially optimal to set the investment of one institution to zero and optimize welfare through the remaining two institutions, thereby providing only one cover akin to Fedwire.

The relative investments of Fedwire versus the social planner hinges on the attack probability, parameterized by $\beta$, in relation to the cost function of data security, denoted by $-c\,f$. Depending on this relationship, either Fedwire or the social planner may exhibit a greater willingness to invest.

Indeed, a larger investment by Fedwire relative to the social planner is further justified by the fact that the entire system with Fedwire relies solely on a

single cover—the Fedwire cover. This is due to the collective decision of all private institutions to abstain from protection, thus leaving Fedwire to compensate for the absence of two additional covers by fortifying the single cover extensively. In contrast, the social planner, when investing in security via all three institutions, provides two covers.

To enhance comparability between Fedwire's investment and the social planner's investment, Figure 5 plots the total investments per provided cover and Figure 6 plots the total investment per institution. These are reasonable performance comparisons because Fedwire invests only once, providing one cover whereas the social planner invests via three institutions to provide two covers. For Fedwire, the individual investment, total investment and investment per cover, thus, coincides. But the total cost attributed to the social planner equal $3 \times c_A$, where $c_A$ represents the individual investment whereas the planner's adjustment for investment per cover equals $(3/2) \times c_A$.

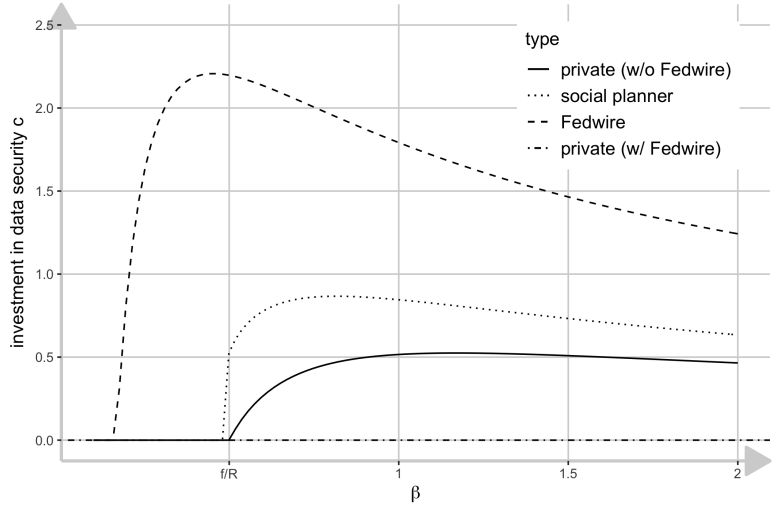



Figure 4: Optimal individual investments in data security by private entities (banks), the social planner, private entities as Fedwire coexists and Fedwire. Along the x-axis, we increase $\beta$ of the attack probability $\alpha(c) = e^{-\beta c}$.

At $f/R = 0.5$, a significant shift in the behavior of all institutions is evident in the plot. This transition arises due to the fact that for smaller values of $\beta$, both private and socially optimal investments equal zero. This occurs because a smaller $\beta$ implies that the attack probability diminishes too slow relative to the per-unit costs $f$ associated with data investment and the revenue $R$ generated when data is secure.

Conversely, for $\beta$ values above $f/R$, optimal investments in security become strictly positive. As $\beta$ surpasses the threshold of $f/R$, the cost-benefit trade-off

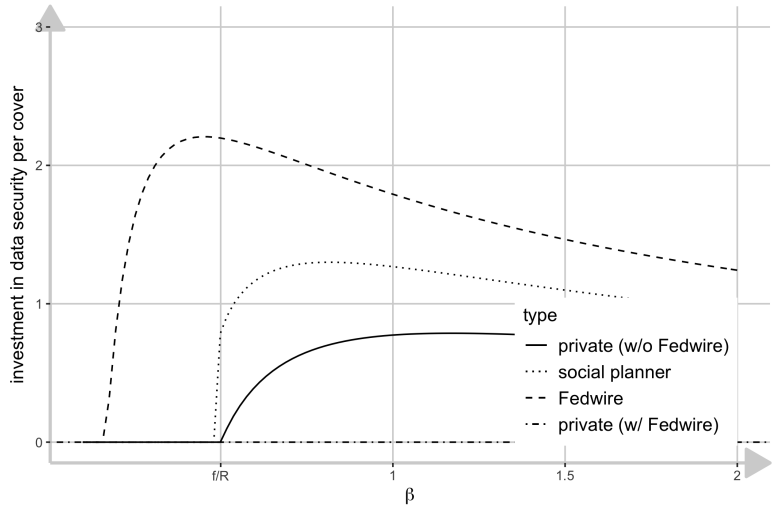



Figure 5: Equilibrium investment per cover. The private institutions, respectively the social planner invests symmetrically via 3 institutions to provide two covers. Fedwire invests once to provide one cover.

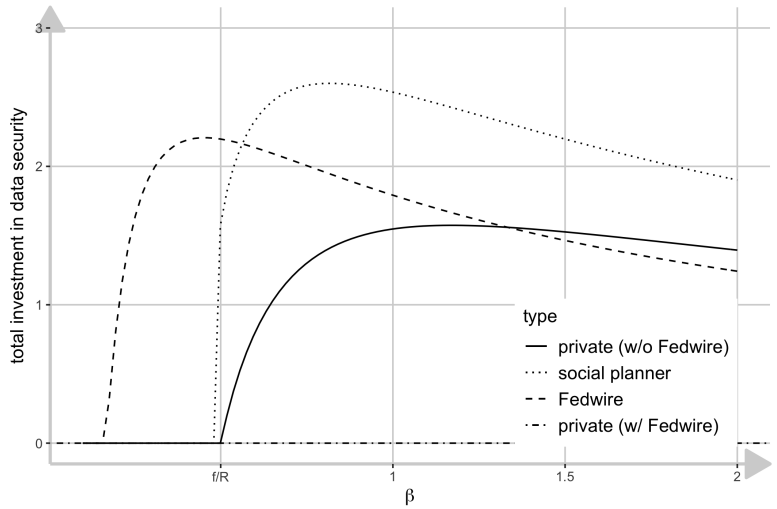



Figure 6: Total Investment: The three private institutions jointly invest $3c_A$. Likewise, the social planner invests via three institutions $3c_A$. Fedwire makes only one large investment $c_F$.

faced by all institutions undergoes alteration. Specifically, investment in data security becomes increasingly effective in reducing individual attack probabilities, while the cost function for data security remains unchanged. Consequently, as $\beta$ increasingly exceeds $f/R$, all institutions systematically reduce their investments.

Figure 7 illustrates the endogenous levels of data security resulting from op-

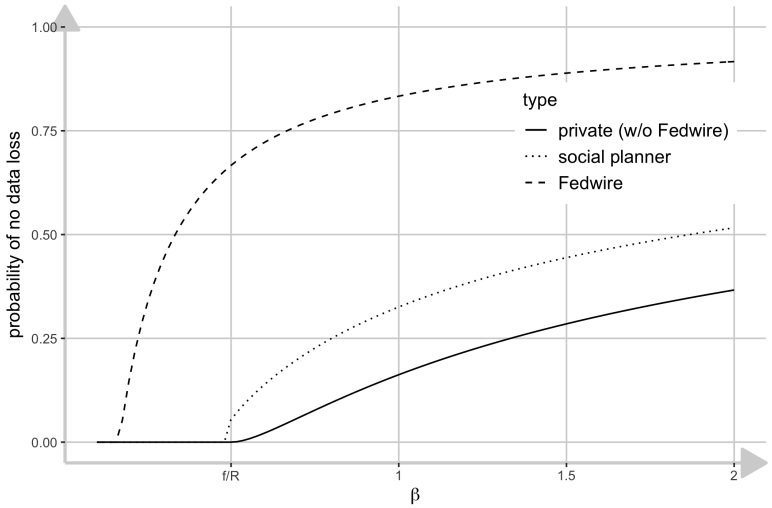



Figure 7: The probability of no data loss.

timal investment strategies. In the scenario involving only private institutions, all entities collectively provide two covers, resulting in a level of security quantified by $(1 - \alpha(c)\alpha(c)(2 - \alpha(c)))$. Similarly, the social planner adheres to the same security function but evaluates it at a higher investment level $c$, thereby enhancing overall security. As Fedwire enters the economy, the overall security function changes to $(1-\alpha(c)\alpha(c_F)(2\alpha(c)-\alpha(c)^2))$, where $c_F$ represents Fedwire's investment, and $c$ denotes investment via the remaining institutions. However, due to the collective shirking of all institutions upon Fedwire's entry, resulting in their zero investment, the security function for Fedwire adapts endogenously to $(1 - \alpha(c_F))$ since $\alpha(0) = 1$.

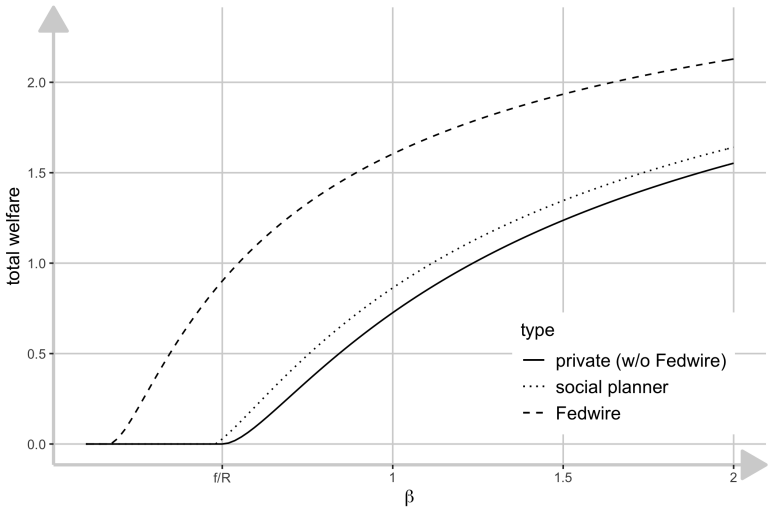



Figure 8: Total welfare in different information systems

Welfare is depicted in Figure 8. Evidently, welfare achieves higher levels when the planner invests in security compared to private institutions. When comparing welfare with Fedwire relative to the social planner one needs to be cautious because the welfare functions are different. As mentioned above, it is essential to recognize that the planner invests in security through all three institutions, incurring the cost function threefold. Through its investment strategy, the planner establishes two covers of security. Conversely, Fedwire invests solely once, incurring the cost function once, but provides only one cover. This discrepancy stems from the fact that all private entities shirk, thereby abstaining from providing the two additional covers that could be provided. Therefore, while comparing welfare between Fedwire and the social planner, it is vital to acknowledge the differing investment and security coverage constraints inherent to their respective strategies.

# 6 General Case for N banks: Double Covers

In this section we develop a general model for the Double Covers and Fedwire case with $N$ banks.

Generically, we define the Double Covers case as a symmetric information environment, where each transaction in the full data set $I = \mathbb{U}_{i=1}^{N} I_i$ is observed by exactly two entites $i, j$ and all entities in $\{1, \dots N\}$ observes the same amount of data $|I_i|$. As before, we exclude transactions within one bank. Each entity's transacts with every other bank. But transactions across two banks are not observed by the remaining banks. Therefore, each transaction in $i'$ information set $I_i$ is observed by exactly one other entity $j \in \{1, \dots N\}/\{i\}$. Therefore, each bank can entirely recover its data via the remaining entities, that is, there are two covers of $I$.

How can we generalize the attack probability for the Double Covers case with $N$ banks?

**Lemma 6.1.** *Let entities $j = i_1, \dots i_n \in \mathcal{N}$, $n \geq 1$ form a cover of information set $I_i$, $I_i \subseteq \bigcup_{j=i_1}^{i_n} I_j$. Assume that no transaction in $I_i$ is observed by more than one entity $j = i_1, \dots i_n$ so that every entity $j = i_1, \dots i_n$ is necessary to form a cover of $I_i$, $I_i \not\subset \bigcup_{j \in \{i_1, \dots, i_n\}/i_k} I_j, i_k \in \{i_1, \dots, i_n\}$. Then the probability of a successful attack on this cover of $I_i$ equals*

$$\sum_{j=1}^{n} \alpha(c_{i_j}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_m})) \tag{58}$$

*where we define* $\prod_{n=1}^{0} = 1$

**Corollary 6.1** (Attack probability for N banks)**.** *In the Double Covers case with* $N$ *entities, the chance that entity* $i_N$*'s data is compromised equals*

$$\alpha(c_{i_N}) \times \sum_{j=1}^{N-1} \alpha(c_{i_j}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_m})) \tag{59}$$

In the Double Covers case, each entity $i_N$'s probability of data loss equals the probability that $i_N$ is successfully attacked and its cover is successfully attacked. The entities $i_1, \ldots, i_{N-1}$ jointly form a cover of $I_N$. Lemma 6.1 states the probability that $i$'s cover is successfully attacked, that is, the probability that at least one entity $i_1, \ldots, i_{N-1}$ is attacked, $N-1 = n$. Therefore, formula (58) states the probability that $i_N$'s data is compromised, equalling the chance that $i_N$ and at least one other instutution is attacked.

This general formula is elaborate and is derived via induction in the appendix. To gain some intuition for the formula, we include here the cases for $N = 4, 5$ banks.

**Case: N=4**

Consider the symmetric entities $\{A, B, C, D\}$, $I = I_A \cup I_B \cup I_C \cup I_D$. What is the probability that A's data is compromised? It equals the probability that A is successfully attacked and either B,C or D is attacked, or two out of the three or all three. Therefore, A's data is compromised with probability $\alpha(c_A)\Big[\alpha(c_B) + (1 - \alpha(c_B))(\alpha(c_C) + (1 - \alpha(c_C))\alpha(c_D))\Big]$.

**Case: N=5**

A's probability of data loss equals the probability that A is successfully attacked and either B,C,D or E is attacked, or two out of the four or three out of the four or all four entities are attacked, $\alpha(c_A)\Big[\alpha(c_B)+(1-\alpha(c_B))(\alpha(c_C)+(1-\alpha(c_C))[\alpha(c_D)+(1 - \alpha(c_D))\alpha(c_E))\Big]$.

## 6.1 Private Equilibrium

With $N$ entities in total, entity $i_N$'s profit function is given by

$$\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}}) = \left(1-\alpha(c_{i_N})\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m}))\right)R_{i_N} - c_{i_N}f(I_{i_N}) \tag{60}$$

Entity $i_N$'s marginal profit equals

$$\frac{\partial}{\partial c_{i_N}}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}}) = -\alpha'(c_{i_N})\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m}))\,R_{i_N} - f(I_{i_N}) \tag{61}$$

Clearly, the profit function is concave, meaning a unique maximum exists,

$$\frac{\partial^2}{\partial c_{i_N}^2}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}}) = -\alpha''(c_{i_N})\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m}))\,R_{i_N} < 0 \tag{62}$$

The first order condition for an interior private equilibrium equals

$$-\alpha'(c_{i_N})\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m})) = \frac{f(I_{i_N})}{R_{i_N}} \tag{63}$$

The first order condition for an interior symmetric private equilibrium equals

$$-\alpha'(c_{i_N})\alpha(c_{i_N})\times\sum_{j=0}^{N-2}(1-\alpha(c_{i_N}))^j = \frac{f(I_{i_N})}{R_{i_N}} \tag{64}$$

The latter can be rewritten via the geometric row[7] as

$$-\alpha'(c_{i_N})\times\left(1-(1-\alpha(c_{i_N}))^{N-1}\right) = \frac{f(I_{i_N})}{R_{i_N}}. \tag{66}$$

**Proposition 6.1** (Private Equilibrium: Double Covers with $N$ entities)**.** *Assume assumption 2.1 holds. Then there exists a unique, interior symmetric private equilib-*

[7]
$$\sum_{j=1}^{N-1}(1-\alpha(c_{i_N}))^{j-1} = \sum_{j=0}^{N-2}(1-\alpha(c_{i_N}))^j = \frac{1-(1-\alpha(c_{i_N}))^{N-1}}{\alpha(c_{i_N})} \tag{65}$$

*rium which is characterized as the solution to*

$$-\alpha'(c_{i_N}) \times \left(1-(1-\alpha(c_{i_N}))^{N-1}\right) = \frac{f(I_{i_N})}{R_{i_N}}. \tag{67}$$

*If $-\alpha'(0) \leq f/R$, there exists no interior symmetric equilibrium, and the symmetric equilibrium is located at $c = 0$ instead.*

*Proof.* [Proposition 6.1] The proof uses an induction argument. The Double Covers cases for $i = 1$ and $i = 2$ are special. Therefore, we show that the formula holds for all $n = 1, 2, 3$, and then proceed with $n \to n+1$ for $n \geq 3$.

n=1: The case $n = 1$ is special. It means there are $n + 1 = 2$ banks in the economy. The banks transact with one another, meaning they have the exact same information sets $I_1 = I_2 = I$, observing all transactions in the economy. Bank 1 alone forms a cover of bank 2 and vice versa, bank 2 alone forms a cover of bank 1. But then the probability that bank 1's cover is hacked just equals the probability that bank 2 is hacked, $\alpha(c_2)$, and vice versa.

n=2: In the case $n = 2$, there are 3 banks in the economy, our benchmark. Two entities $i_1$ and $i_2$ form a cover of the third entitie's information, $I_3$, and none of the entities form a cover of $I_3$ on their own, $I_3 \not\subset I_{i_1},\ I_3 \not\subset I_{i_2}$. If one of the two entities or both are attacked, they no longer form a cover of $I_i$. Therefore, the probability that the cover of $I_3$ is successfully attacked equals the probability that either $i_1$ or $i_2$ or both are attacked. Since we want to prove formula (58) and give some intuition for the general formula, the attack probability on the cover equals the probability that $i_1$ is successfully attacked plus the probability that $i_1$ is not attacked but information $I_3 \setminus \{I_{i_1}\}$ is attacked. The probability that information $I_i \setminus \{I_{i_1}\}$ is attacked equals the probability that $i_2$ is attacked. That is, the cover of $I_3$ is attacked with probability $\alpha(c_{i_1}) + (1-\alpha(c_{i_1}))\alpha(c_{i_2})$, and the formula holds for $N = 2$.

n=3: Assume the three entities $i_1, i_2, i_3$ form a cover of $I_4$. The probability that the cover of $I_4$ is successfully attacked equals the probability that $i_1$ is successfully attacked plus the probability that $i_1$ is not attacked but information $I_4 \setminus \{I_{i_1}\}$ is successfully attacked. Entities $i_2, i_3$ form a cover of $I_4 \setminus \{I_{i_1}\}$. The probability that their cover is attacked equals (case n=2) $\alpha(c_{i_2})+(1-\alpha(c_{i_2}))\alpha(c_{i_3})$. The overall probability of an attack on the cover thus equals $\alpha(c_{i_1}) + (1-\alpha(c_{i_1}))(\alpha(c_{i_2}) + (1-\alpha(c_{i_2}))\alpha(c_{i_3}))$.

$n \to n+1$: Assume the formula holds for $n$ entities, forming a cover of en-

tity $i_{(n+1)}$'s information $I_{n+1}$. We want to show that the formular must therefore also hold for $n+1$ entities forming a cover of entity $i_{(n+2)}$'s information $I_{n+2}$. Assume the $n+1$ entities $i_1, i_2, \ldots, i_n, i_{n+1}$ form a cover of $I_{n+2}$. The probability that this cover of $I_{n+2}$ is successfully attacked equals the probability that $i_{n+1}$ is successfully attacked plus the probability that $i_{n+1}$ is not attacked but information $I_{n+2} \setminus \{I_{i_{n+1}}\}$ is successfully attacked. But we know that the $n$ entities $i_1, i_2, \ldots, i_n$ form a cover of $I_{n+2} \setminus \{I_{i_{n+1}}\}$, and formula (68) holds for information covers with $n$ entities. Thus, the probability that information $I_{n+2} \setminus \{I_{i_{n+1}}\}$ is attacked equals (case $n$)

$$\sum_{j=1}^{n} \alpha(c_{i_j}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_m})) = \sum_{j=1}^{n} \alpha(c_{i_{n-j+1}}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_{n-m+1}})) \tag{68}$$

where we have exchanged the ordering of the summation for convenience. Consequentially, the overall probability that the cover of $I_{n+2}$ is attacked equals

$$\alpha(c_{i_{n+1}}) + (1 - \alpha(c_{i_{n+1}})) \times \sum_{j=1}^{n} \alpha(c_{i_{n-j+1}}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_{n-m+1}})) \tag{69}$$

$$= \sum_{j=1}^{n+1} \alpha(c_{i_{(n+1)-j+1}}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_{(n+1)-m+1}})) \tag{70}$$

$$= \sum_{j=1}^{n+1} \alpha(c_{i_j}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_m})) \tag{71}$$

□

## 6.2 Social Planner equilibrium

The social planner maximizes

$$\pi_P(c_{i_1}, c_{i_2}, \ldots c_{i_N}) = \sum_{k=1}^{N} \pi_{i_k}(c_{i_1}, c_{i_2}, \ldots c_{i_N}) \tag{72}$$

$$= \sum_{k=1}^{N} \left( 1 - \alpha(c_{i_k}) \times \sum_{\substack{j=1, \\ j \neq k}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1, \\ m \neq k}}^{j-1} (1 - \alpha(c_{i_m})) \right) R_{i_k} - c_{i_k} f(I_{i_k}) \tag{73}$$

The first-order condition for the planner with regard to an interior maximizer $c_{i_{\hat{k}}}$, $\hat{k} \in \{1, \dots N\}$ is

$$\frac{\partial}{\partial c_{i_{\hat{k}}}} \pi_P(c_{i_1}, c_{i_2}, \dots c_{i_N}) \tag{74}$$

$$= \sum_{k=1}^{N} \frac{\partial}{\partial c_{i_{\hat{k}}}} \pi_{i_k}(c_{i_1}, c_{i_2}, \dots c_{i_N})$$

$$= \sum_{k=1}^{N} \frac{\partial}{\partial c_{i_{\hat{k}}}} \left[ \left( 1 - \alpha(c_{i_k}) \times \sum_{\substack{j=1,\\ j\neq k}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq k}}^{j-1} (1 - \alpha(c_{i_m})) \right) R_{i_k} - c_{i_k} f(I_{i_k}) \right]$$

$$= (-\alpha'(c_{i_{\hat{k}}})) \Big[ R_{i_{\hat{k}}} \underbrace{\sum_{\substack{j=1,\\ j\neq \hat{k}}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq \hat{k}}}^{j-1} (1 - \alpha(c_{i_m}))}_{\equiv A} + \underbrace{\sum_{\substack{k=1,\\ k\neq \hat{k}}}^{N} \alpha(c_{i_k})\, R_{i_k} \prod_{\substack{m=1,\\ m\neq k}}^{\hat{k}-1} (1 - \alpha(c_{i_m}))}_{\equiv B} \tag{75}$$

$$\underbrace{- \sum_{\substack{k=1,\\ k\neq \hat{k}}}^{N} \alpha(c_{i_k}) R_{i_k} \sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq k,\\ m\neq \hat{k}}}^{j-1} (1 - \alpha(c_{i_m}))}_{\equiv C} \Big] - f(I_{i_{\hat{k}}}) \tag{76}$$

Due to its complexity, we split the anlysis of the derivative in three parts. Term A corresponds to the derivative of profit for $k = \hat{k}$, term B corresponds for the derivative of profit when $k \neq \hat{k}$ and $j = \hat{k}$, term C corresponds to the derivative of profit when $k \neq \hat{k}$ and $m = \hat{k}$. In the symmetric case $c_{i_1} = \dots, c_{i_N} = c_{i_k}$. It therefore holds

$$A = \sum_{\substack{j=1,\\ j\neq \hat{k}}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq \hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) \tag{77}$$

$$= \sum_{j=1}^{\hat{k}-1} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq \hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) + \sum_{j=\hat{k}+1}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq \hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) \tag{78}$$

$$= \alpha(c_{i_k}) \sum_{j=1}^{\hat{k}-1} (1 - \alpha(c_{i_k}))^{j-1} + \alpha(c_{i_k}) \sum_{j=\hat{k}+1}^{N} (1 - \alpha(c_{i_k}))^{j-2} \tag{79}$$

because by $j > \hat{k}$, the product in the second term has only $j - 2$ factors whereas the product in the first terms has $j - 1$ factors by $j \leq \hat{k} - 1$. Also, we have set

$\sum_{j=1}^{z} = 0, z < 1$ and $\sum_{j=N+1}^{N} = 0$. It further holds

$$\sum_{j=1}^{\hat{k}-1}(1-\alpha(c_{i_k}))^{j-1} = \sum_{j=0}^{\hat{k}-2}(1-\alpha(c_{i_k}))^{j} = \frac{1-(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})} \tag{80}$$

$$\sum_{j=\hat{k}+1}^{N}(1-\alpha(c_{i_k}))^{j-2} = \sum_{j=\hat{k}-1}^{N-2}(1-\alpha(c_{i_k}))^{j} \tag{81}$$

$$= \sum_{j=0}^{N-2}(1-\alpha(c_{i_k}))^{j} - \sum_{j=0}^{\hat{k}-2}(1-\alpha(c_{i_k}))^{j} \tag{82}$$

$$= \frac{1-(1-\alpha(c_{i_k}))^{N-1}}{\alpha(c_{i_k})} - \frac{1-(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})} \tag{83}$$

Jointly,

$$A = \alpha(c_{i_k})\left(\frac{1-(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})} + \frac{1-(1-\alpha(c_{i_k}))^{N-1}}{\alpha(c_{i_k})} - \frac{1-(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})}\right) \tag{84}$$

$$= \alpha(c_{i_k})\left(\frac{1-(1-\alpha(c_{i_k}))^{N-1}}{\alpha(c_{i_k})}\right) \tag{85}$$

$$= 1-(1-\alpha(c_{i_k}))^{N-1} \tag{86}$$

Note, generically, the double covers case considers $N \geq 3$. For the next term, in the symmetric case $c_{i_1} = \ldots, c_{i_N} = c_{i_k}$ it holds

$$B = \sum_{\substack{k=1,\\ k\neq\hat{k}}}^{N} \alpha(c_{i_k})\; R_{i_k} \prod_{\substack{m=1,\\ m\neq k}}^{\hat{k}-1}(1-\alpha(c_{i_m})) \tag{87}$$

$$= \sum_{k=1}^{\hat{k}-1} \alpha(c_{i_k})\; R_{i_k} \prod_{\substack{m=1,\\ m\neq k}}^{\hat{k}-1}(1-\alpha(c_{i_m})) + \sum_{k=\hat{k}+1}^{N} \alpha(c_{i_k})\; R_{i_k} \prod_{\substack{m=1,\\ m\neq k}}^{\hat{k}-1}(1-\alpha(c_{i_m})) \tag{88}$$

$$= \sum_{k=1}^{\hat{k}-1} \alpha(c_{i_k})\; R_{i_k}\,(1-\alpha(c_{i_k}))^{\hat{k}-2} + \sum_{k=\hat{k}+1}^{N} \alpha(c_{i_k})\; R_{i_k}\,(1-\alpha(c_{i_k}))^{\hat{k}-1} \tag{89}$$

$$= \alpha(c_{i_k})\,(1-\alpha(c_{i_k}))^{\hat{k}-2}\; R_{i_k}\left((\hat{k}-1) + (N-\hat{k})\,(1-\alpha(c_{i_k}))\right) \tag{90}$$

where the products simplify because in the first term by $k \leq \hat{k} - 1$ the product has only $\hat{k} - 2$ factors whereas in the second term the product has $\hat{k} - 1$ factors by $k > \hat{k}$, moreover in the symmetric equilibrium all $c'$s are the same.

Last,

$$C = \sum_{\substack{k=1,\\ k\neq\hat{k}}}^{N} \alpha(c_{i_k}) R_{i_k} \sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq k,\\ m\neq\hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) \tag{91}$$

$$= \sum_{k=1}^{\hat{k}-1} \alpha(c_{i_k}) R_{i_k} \sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq k,\\ m\neq\hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) + \sum_{k=\hat{k}+1}^{N} \alpha(c_{i_k}) R_{i_k} \sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{N} \alpha(c_{i_j}) \prod_{\substack{m=1,\\ m\neq k,\\ m\neq\hat{k}}}^{j-1} (1 - \alpha(c_{i_m}))$$

$$= \sum_{k=1}^{\hat{k}-1} \alpha(c_{i_k})^2 R_{i_k} \sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{N} \prod_{\substack{m=1,\\ m\neq k,\\ m\neq\hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) \tag{92}$$

$$+ \sum_{k=\hat{k}+1}^{N} \alpha(c_{i_k})^2 R_{i_k} \left( \sum_{j=\hat{k}+1}^{k-1} \prod_{\substack{m=1,\\ m\neq k,\\ m\neq\hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) + \sum_{j=k+1}^{N} \prod_{\substack{m=1,\\ m\neq k,\\ m\neq\hat{k}}}^{j-1} (1 - \alpha(c_{i_m})) \right) \tag{93}$$

$$= \sum_{k=1}^{\hat{k}-1} \alpha(c_{i_k})^2 R_{i_k} \sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{N} (1 - \alpha(c_{i_j}))^{j-3} \tag{94}$$

$$+ \sum_{k=\hat{k}+1}^{N} \alpha(c_{i_k})^2 R_{i_k} \left( \sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{k-1} (1 - \alpha(c_{i_k}))^{j-2} + \sum_{\substack{j=k+1,\\ j\neq k}}^{N} (1 - \alpha(c_{i_k}))^{j-3} \right) \tag{95}$$

$$\tag{96}$$

where the number of factors in the products differ across terms depending on whether the $k$ and $\hat{k}$ are included in the product or not. The first product has $j-3$ factors because $k < \hat{k} \leq j-1$, the second product has $j-2$ factors because $j - 1 \geq \hat{k}$ but $j < k$, thus $j - 1 < k$. The third product has $j - 3$ factors because $j > k$, thus $j - 1 \geq k$ and $j > \hat{k}$. We further simplify these terms using again

the geometric row,

$$\sum_{k=1}^{\hat{k}-1} \sum_{\substack{j=\hat{k}+1, \\ j\neq k}}^{N} (1-\alpha(c_{i_j}))^{j-3} = (\hat{k}-1) \sum_{j=\hat{k}+1}^{N} (1-\alpha(c_{i_j}))^{j-3} \tag{97}$$

$$= (\hat{k}-1) \sum_{j=\hat{k}-2}^{N-3} (1-\alpha(c_{i_j}))^{j} \tag{98}$$

$$= (\hat{k}-1) \left( \sum_{j=0}^{N-3} (1-\alpha(c_{i_j}))^{j} + \sum_{j=0}^{\hat{k}-3} (1-\alpha(c_{i_j}))^{j} \right) \tag{99}$$

$$= (\hat{k}-1) \left( \frac{1-(1-\alpha(c_{i_k}))^{N-2}}{\alpha(c_{i_k})} - \frac{1-(1-\alpha(c_{i_k}))^{\hat{k}-2}}{\alpha(c_{i_k})} \right) \tag{100}$$

$$= (\hat{k}-1) \left( \frac{(1-\alpha(c_{i_k}))^{\hat{k}-2} - (1-\alpha(c_{i_k}))^{N-2}}{\alpha(c_{i_k})} \right) \tag{101}$$

$$= (\hat{k}-1) \frac{(1-\alpha(c_{i_k}))^{\hat{k}-2}}{\alpha(c_{i_k})} \left( 1-(1-\alpha(c_{i_k}))^{N-2-(\hat{k}-2)} \right) \tag{102}$$

$$= (\hat{k}-1) \frac{(1-\alpha(c_{i_k}))^{\hat{k}-2}}{\alpha(c_{i_k})} \left( 1-(1-\alpha(c_{i_k}))^{N-\hat{k}} \right) \tag{103}$$

$$\tag{104}$$

where the constraint $j \neq k$ drops since it always holds. For the second term of

C,

$$\sum_{k=\hat{k}+1}^{N}\left(\sum_{j=\hat{k}+1}^{k-1}(1-\alpha(c_{i_k}))^{j-2}+\sum_{\substack{j=k+1,\\ j\neq k}}^{N}(1-\alpha(c_{i_k}))^{j-3}\right) \tag{105}$$

$$=\sum_{k=\hat{k}+2}^{N}\sum_{\substack{j=\hat{k}+1,\\ j\neq k}}^{k-1}(1-\alpha(c_{i_k}))^{j-2}+\sum_{k=\hat{k}+1}^{N}\sum_{j=k-2}^{N-3}(1-\alpha(c_{i_k}))^{j} \tag{106}$$

$$=\sum_{k=\hat{k}+2}^{N}\sum_{j=\hat{k}-1}^{k-3}(1-\alpha(c_{i_k}))^{j}+\sum_{k=\hat{k}+1}^{N}\sum_{j=k-2}^{N-3}(1-\alpha(c_{i_k}))^{j} \tag{107}$$

$$=\sum_{k=\hat{k}+2}^{N}\frac{(1-\alpha(c_{i_k}))^{\hat{k}-1}-(1-\alpha(c_{i_k}))^{k-2}}{\alpha(c_{i_k})}+\sum_{k=\hat{k}+1}^{N}\frac{(1-\alpha(c_{i_k}))^{k-2}-(1-\alpha(c_{i_k}))^{N-2}}{\alpha(c_{i_k})} \tag{108}$$

$$=(N-(\hat{k}+1))\frac{(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})}-\sum_{k=\hat{k}}^{N-2}\frac{(1-\alpha(c_{i_k}))^{k}}{\alpha(c_{i_k})} \tag{109}$$

$$+\sum_{k=\hat{k}-1}^{N-2}\frac{(1-\alpha(c_{i_k}))^{k}}{\alpha(c_{i_k})}-(N-\hat{k})\frac{(1-\alpha(c_{i_k}))^{N-2}}{\alpha(c_{i_k})} \tag{110}$$

$$=(N-(\hat{k}+1))\frac{(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})}-\left(\frac{(1-\alpha(c_{i_k}))^{\hat{k}}}{\alpha(c_{i_k})^2}-\frac{(1-\alpha(c_{i_k}))^{N-1}}{\alpha(c_{i_k})^2}\right) \tag{111}$$

$$+\frac{(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})^2}-\frac{(1-\alpha(c_{i_k}))^{N-1}}{\alpha(c_{i_k})^2}-(N-\hat{k})\frac{(1-\alpha(c_{i_k}))^{N-2}}{\alpha(c_{i_k})} \tag{112}$$

$$\tag{113}$$

where at the first equality we have dropped the summand $k=\hat{k}+1$ since that

sum equals zero. Overall,

$$\frac{\partial}{\partial c_{i_{\hat{k}}}}\pi_P(c_{i_1}, c_{i_2}, \dots c_{i_N}) \tag{114}$$

$$= (-\alpha'(c_{i_{\hat{k}}}))\Big[R_{i_{\hat{k}}}\left(1-(1-\alpha(c_{i_k}))^{N-1}\right) \tag{115}$$

$$+\alpha(c_{i_k})\left(1-\alpha(c_{i_k})\right)^{\hat{k}-2} R_{i_k}\left((\hat{k}-1)+(N-\hat{k})\left(1-\alpha(c_{i_k})\right)\right) \tag{116}$$

$$+\alpha(c_{i_k})^2 R_{i_k}\ (\hat{k}-1)\frac{(1-\alpha(c_{i_k}))^{\hat{k}-2}}{\alpha(c_{i_k})}\left(1-(1-\alpha(c_{i_k}))^{N-\hat{k}}\right) \tag{117}$$

$$+\alpha(c_{i_k})^2 R_{i_k}\left((N-(\hat{k}+1))\frac{(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})}-\left(\frac{(1-\alpha(c_{i_k}))^{\hat{k}}}{\alpha(c_{i_k})^2}-\frac{(1-\alpha(c_{i_k}))^{N-1}}{\alpha(c_{i_k})^2}\right)\right) \tag{118}$$

$$+\alpha(c_{i_k})^2 R_{i_k}\left(\frac{(1-\alpha(c_{i_k}))^{\hat{k}-1}}{\alpha(c_{i_k})^2}-\frac{(1-\alpha(c_{i_k}))^{N-1}}{\alpha(c_{i_k})^2}-(N-\hat{k})\frac{(1-\alpha(c_{i_k}))^{N-2}}{\alpha(c_{i_k})}\right)\Big]\ -f(I_{i_{\hat{k}}}) \tag{119}$$

$$= (-\alpha'(c_{i_{\hat{k}}}))\Big[R_{i_{\hat{k}}}\left(1-(1-\alpha(c_{i_k}))^{N-1}\right) \tag{120}$$

$$+\alpha(c_{i_k})\left(1-\alpha(c_{i_k})\right)^{\hat{k}-2} R_{i_k}\left((\hat{k}-1)+(N-\hat{k})\left(1-\alpha(c_{i_k})\right)\right) \tag{121}$$

$$+\alpha(c_{i_k}) R_{i_k}\ (\hat{k}-1)(1-\alpha(c_{i_k}))^{\hat{k}-2}\left(1-(1-\alpha(c_{i_k}))^{N-\hat{k}}\right) \tag{122}$$

$$+R_{i_k}\left((N-(\hat{k}+1))\alpha(c_{i_k})(1-\alpha(c_{i_k}))^{\hat{k}-1}-\left((1-\alpha(c_{i_k}))^{\hat{k}}-(1-\alpha(c_{i_k}))^{N-1}\right)\right) \tag{123}$$

$$+R_{i_k}\left((1-\alpha(c_{i_k}))^{\hat{k}-1}-(1-\alpha(c_{i_k}))^{N-1}-(N-\hat{k})\alpha(c_{i_k})(1-\alpha(c_{i_k}))^{N-2}\right)\Big]\ -f(I_{i_{\hat{k}}}) \tag{124}$$

$$\tag{125}$$

## 6.3 Fedwire: Private Equilibrium stage 2

As before, Fedwire moves first in $t = 1$, setting $c_F$, whereas private entities move in $t = 2$ after observing $c_F$. With Fedwire and $N$ private entities in total, entity $i_N$'s profit function given $c_F$ equals

$$\Pi_{i_N}(c_{i_N}|c_{i_1}, \dots, c_{i_{N-1}}) = \left(1-\alpha(c_{i_N})\alpha(c_F)\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m}))\right)R_{i_N} - c_{i_N}f(I_{i_N}) \tag{126}$$

Entity $i_N$'s marginal profit equals

$$\frac{\partial}{\partial c_{i_N}}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}}) = -\alpha'(c_{i_N})\alpha(c_F)\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m}))\,R_{i_N}-f(I_{i_N}) \tag{127}$$

Clearly, the profit function is concave,

$$\frac{\partial^2}{\partial c_{i_N}^2}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}}) = -\alpha''(c_{i_N})\alpha(c_F)\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m}))\,R_{i_N} < 0 \tag{128}$$

The first order condition for an interior private Fedwire equilibrium equals

$$-\alpha'(c_{i_N})\times\sum_{j=1}^{N-1}\alpha(c_{i_j})\prod_{m=1}^{j-1}(1-\alpha(c_{i_m})) = \frac{1}{\alpha(c_F)}\frac{f(I_{i_N})}{R_{i_N}} \tag{129}$$

The first order condition for an interior symmetric private equilibrium equals

$$-\alpha'(c_{i_N})\alpha(c_{i_N})\times\sum_{j=0}^{N-2}(1-\alpha(c_{i_N}))^j = \frac{1}{\alpha(c_F)}\frac{f(I_{i_N})}{R_{i_N}} \tag{130}$$

The latter can be rewritten via the geometric row as

$$-\alpha'(c_{i_N})\times\left(1-(1-\alpha(c_{i_N}))^{N-1}\right) = \frac{1}{\alpha(c_F)}\frac{f(I_{i_N})}{R_{i_N}}. \tag{131}$$

**Proposition 6.2** (Private Fedwire Equilibrium $N$ entities)**.** *Assume assumption 2.1 holds. Then there exists a unique, interior symmetric private equilibrium which is characterized as the solution to*

$$-\alpha'(c_{i_N})\times\left(1-(1-\alpha(c_{i_N}))^{N-1}\right) = \frac{1}{\alpha(c_F)}\frac{f(I_{i_N})}{R_{i_N}}. \tag{132}$$

*If $-\alpha'(0) \leq f/R$, there exists no interior symmetric equilibrium, and the symmetric equilibrium is located at $c = 0$ instead.*

## 6.4 Fedwire equilibrium stage 1

Fedwire moves first in $t = 1$, taking as given the collective behavior of the private entities that follow in $t = 2$.

Fedwire maximizes

$$\pi_P(c_F|c_{i_1}^F(c_F), c_{i_2}^F(c_F), \ldots, c_{i_N}^F(c_F))$$

$$= \sum_{k=1}^{N} \pi_{i_k}(c_{i_1}^F, c_{i_2}^F, \ldots, c_{i_N}^F, c_F) - c_F \ f(|I|) \tag{133}$$

$$= \sum_{k=1}^{N} \left[ \left( 1 - \alpha(c_{i_k})\alpha(c_F) \times \sum_{j \in \{1,2,\ldots,N\}/k} \alpha(c_{i_j}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_m})) \right) R_{i_k} - c_{i_k} f(I_{i_k}) \right] \tag{134}$$

$$- c_F \ f(|I|) \tag{135}$$

$$\tag{136}$$

$$\Pi_{i_N}(c_{i_N}|c_{i_1}, \ldots, c_{i_{N-1}}) = \left( 1 - \alpha(c_{i_N})\alpha(c_F) \times \sum_{j=1}^{N-1} \alpha(c_{i_j}) \prod_{m=1}^{j-1} (1 - \alpha(c_{i_m})) \right) R_{i_N} - c_{i_N} f(I_{i_N}) \tag{137}$$

# 7 Conclusion

Existing payment and banking networks were established before the information age. Their adaptation or restructuring in terms of the extent of information centralization and complementarity of entities is costly and requires a thorough analysis of possible subsequent equilibrium effects. The analysis in this paper contributes to that debate by providing and economic model of data security that features redundancies (backups) and data segmentation.

We observe that data redundancy generically causes free-riding and does not necessarily increase security when all parties internalize the quantity of backups. Information segmentation when keeping the backup quantity constant can but does not have to improve security.

We can contrast these results to a distributed ledger system. In the system we consider, all participants participate in the transaction validation process (mining). Consequently there are as many copies of the data as there are participants. In a DLT system recovery is easy so long as any one participant is functioning. However individual incentives to protect data fall as the system size grows.

# References


Mohammed A AlZain, Ben Soh, and Eric Pardede. A new approach using redundancy technique to improve security in cloud computing. In *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pages 230–235. IEEE, 2012.

George-Marios Angeletos and Alessandro Pavan. Efficient use of information and social value of information. *Econometrica*, 75(4):1103–1142, 2007.

Juliane Begenau, Maryam Farboodi, and Laura Veldkamp. Big data in finance and the growth of large firms. *Journal of Monetary Economics*, 97:71–87, 2018.

Bruno Biais, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta. The blockchain folk theorem. *The Review of Financial Studies*, 32(5):1662–1715, 2019.

Eric Budish. The economic limits of bitcoin and the blockchain. Technical report, National Bureau of Economic Research, 2018.

Zahra Ebrahimi, Bryan Routledge, and Ariel Zetlin-Jones. Getting blockchain incentives right. Technical report.

Maryam Farboodi and Laura Veldkamp. Long-run growth of financial data technology. *American Economic Review*, 110(8):2485–2523, 2020.

Maryam Farboodi and Laura Veldkamp. A model of the data economy. Technical report, National Bureau of Economic Research, 2021.

Maryam Farboodi, Roxana Mihet, Thomas Philippon, and Laura Veldkamp. Big data and firm dynamics. In *AEA papers and proceedings*, volume 109, pages 38–42, 2019.

Maryam Farboodi, Dhruv Singal, Laura Veldkamp, and Venky Venkateswaran. Valuing financial data. Technical report, National Bureau of Economic Research, 2022.

Gerald A Feltham. The value of information. *The accounting review*, 43(4):684–696, 1968.

Navid Ghaffarzadegan. How a system backfires: Dynamics of redundancy problems in security. *Risk Analysis: An International Journal*, 28(6):1669–1687, 2008.

Jack Hirshleifer. The private and social value of information and the reward to inventive activity. In *Uncertainty in economics*, pages 541–556. Elsevier, 1978.

Gur Huberman, Jacob D Leshno, and Ciamac Moallemi. Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *The Review of Economic Studies*, 88(6):3011–3040, 2021.

Dayu Jia, Junchang Xin, Zhiqiong Wang, Wei Guo, and Guoren Wang. Elasticchain: Support very large blockchain by reducing data redundancy. In *Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data*, pages 440–454. Springer, 2018.

Bev Littlewood and Lorenzo Strigini. Redundancy and diversity in security. In *European symposium on research in computer security*, pages 423–438. Springer, 2004.

Stephen Morris and Hyun Song Shin. Social value of public information. *american economic review*, 92(5):1521–1534, 2002.

Linda Schilling. Risks involved with cbdcs: on cash, privacy, and information centralization. *Privacy, and Information Centralization (November 1, 2019)*, 2019.

# 8 Appendix

## 8.1 Double Covers

*Proof.* [Proposition 3.1] From (5), the first order condition when searching for a symmetric equilibrium, $c_A^* = c_B^* = c_C^*$, is given as (8).

First note that Assumption 1 and Assumption 2 imply that $-\alpha'(0) = -\alpha'(0)(4\alpha(0) - 3\alpha^2(0)) = -\alpha'(0)(2\alpha(0) - \alpha^2(0)) > \frac{f(|I_i|)}{R(|I_i|)}$. Hence by Assumptions 1,2 and 3, and by continuity of the function $-\alpha'(c)[2\alpha(c) - \alpha(c)^2]$ in $c$, there is at least one interior candidate for a symmetric private equilibrium, i.e., a solution to (8). Moreover, the function $g(c) = \alpha'(c)[2\alpha(c) - \alpha(c)^2]$ is strictly increasing in $c$ because $\alpha(c)$ is strictly convex: The second derivative of the private profit function is negative (the profit function is strictly concave)

$$\frac{\partial^2}{\partial c_A^2}\pi_A(c_A) = -\alpha''(c_A)(\alpha(c_B) + \alpha(c_C) - \alpha(c_B)\alpha(c_C))R(|I_A|) < 0 \tag{138}$$

because $\alpha(c)$ is strictly convex. Therefore, the function $-g(c)$ crosses the value $f(|I_A|)/R(|I_A|)$ exactly once, ruling out multiple symmetric equilibria.

The solution to (8) yields $\frac{\partial}{\partial c_A}\pi_A(c_A) = 0$, for $c_A = c_B = c_C$. To show that this solution to (8) is indeed an equilibrium, we further need to show that

$$\frac{\partial}{\partial c_A}\pi_A(c_A, c_B) < 0, \text{ for } c_A > c_B = c_C, \tag{139}$$

$$\frac{\partial}{\partial c_A}\pi_A(c_A c_B) > 0, \text{ for } c_A < c_B = c_C \tag{140}$$

Assume $c_A > c_B = c_C$, and assume that $C$ and $B$ play the solution to (8). Because $\alpha$ is convex, we can follow $\alpha'(c_A) > \alpha'(c_B)$. Hence,

$$\frac{\partial}{\partial c_A}\pi_A(c_A, c_B) = -\alpha'(c_A)\alpha(c_B)(2-\alpha(c_B))R - f < -\alpha'(c_B)\alpha(c_B)(2-\alpha(c_B))R - f = 0 \tag{141}$$

Vice versa, for $c_A < c_B = c_C$, it follows $\alpha'(c_A) < \alpha'(c_B)$ and thus

$$\frac{\partial}{\partial c_A}\pi_A(c_A, c_B) = -\alpha'(c_A)\alpha(c_B)(2-\alpha(c_B))R - f > -\alpha'(c_B)\alpha(c_B)(2-\alpha(c_B))R - f = 0 \tag{142}$$

which proves that the symmetric solution to (8) is the unique symmetric interior equilibrium.

A1-A3 ensure the existence of an interior equilibrium whereas strict convexity of $\alpha(c)$ gives uniqueness of a symmetric equilibrium in $[0, \infty)$.

A1) If $-g(c) \leq f(|I_A|)/R(|I_A|)$ for all $c \in [0, \infty)$, then $c_i^* = 0$ for all $i = A, B, C$ is the unique symmetric equilibrium: Given $c_B = c_C = 0$, and since $\alpha(0) = 1$ A's marginal profit function becomes

$$\frac{\partial}{\partial c_A}\pi_A(c_A, 0) = -\alpha'(c_A)R - f \tag{143}$$

Then $c_A = 0 = c_B$ is an equilibrium if $-\alpha'(c_A)R - f < 0$ for all $c_A \geq 0$. Because $-\alpha'(c_A)$ is a decreasing function, a sufficient condition for the symmetric zero investment equilibrium, $c_i^* = 0$, is $-\alpha'(0)R - f < 0$. Assumption 1 and 2 jointly exclude this corner result.

A2) If $-g(c) \geq \frac{f(|I_i|)}{R(|I_i|)}$ for all $c \in [0, \infty)$, then $c_i^* = \infty$ for all $i = A, B, C$ is the unique symmetric equilibrium. A sufficient and necessary condition for $c_i^* = \infty$ is given by $-\lim_{c\to\infty} g(c) \geq \frac{f(|I_i|)}{R(|I_i|)}$. This corner is excluded by Assumption 3.

□

*Proof.* [Proposition 3.2] We follow the same reasoning as in the private case. An interior symmetric social equilibrium has to satisfy (24).

First note that Assumption 3 ensures that $-\lim_{c\to\infty}\alpha'(c)(4\alpha(c)-3\alpha^2(c)) < -\lim_{c\to\infty}\alpha'(c)(4\alpha(c)-2\alpha^2(c)) < \frac{f(|I_i|)}{R(|I_i|)}$. By Assumption 1 and 2, $-\alpha'(0) = -\alpha'(0)(4\alpha(0)-3\alpha^2(0)) > \frac{f(|I_i|)}{R(|I_i|)}$. Hence Assumptions 1, 2 and 3 jointly with continuity of the function $g(c) = \alpha'(c)(4\alpha(c)-3\alpha(c)^2)$ guarantee that at least one candidate for a symmetric social equilibrium exists. Moreover, if the function $g(c) = \alpha'(c)(4\alpha(c)-3\alpha(c)^2)$ crosses zero only once, then because $g(c)$ is continuous the symmetric social equilibrium is unique. A sufficient condition for this to hold is when $g(c)$ is strictly increasing. Therefore, the function $-g(c)$ crosses the value $f(|I_A|)/R(|I_A|)$ exactly once, ruling out multiple symmetric equilibria. To show that the solution to (24) is indeed an equilibrium, we need to show that when B and C both play the solution to (24), then

$$\frac{\partial}{\partial c_A}\pi_P(c_A,c_B) < 0, \text{ for } c_A > c_B = c_C, \tag{144}$$

$$\frac{\partial}{\partial c_A}\pi_P(c_A,c_B) > 0, \text{ for } c_A < c_B = c_C \tag{145}$$

But this follows, as in the privately optimal case, from the convexity of $\alpha(\cdot)$.

If $(-\alpha'(0)) < f/R$, then the function $-g(c)$ does not cross the value $f/R$. Hence, the social profit function is monotonically decreasing in $c$, and the unique symmetric social optimum is zero investment $\hat{c}_i = 0$.

□

*Proof.* [Proposition 3.2] We follow the same reasoning as in the private case. An interior symmetric social equilibrium has to satisfy (24).

First note that Assumption 3 ensures that $-\lim_{c\to\infty}\alpha'(c)(4\alpha(c)-3\alpha^2(c)) < -\lim_{c\to\infty}\alpha'(c)(4\alpha(c)-2\alpha^2(c)) < \frac{f(|I_i|)}{R(|I_i|)}$. By Assumption 1 and 2, $-\alpha'(0) = -\alpha'(0)(4\alpha(0)-3\alpha^2(0)) > \frac{f(|I_i|)}{R(|I_i|)}$. Hence Assumptions 1, 2 and 3 jointly with continuity of the function $g(c) = \alpha'(c)(4\alpha(c)-3\alpha(c)^2)$ guarantee that at least one candidate for a symmetric social equilibrium exists. Moreover, the function $g(c) = \alpha'(c)(4\alpha(c)-3\alpha(c)^2)$ is strictly increasing because $\alpha(c)$ is strictly convex. Therefore, the function $-g(c)$ crosses the value $f(|I_A|)/R(|I_A|)$ exactly once, ruling out multiple symmetric equilibria. To show that the solution to (24) is indeed an equilibrium, we need to show that when B and C both play

the solution to (24), then

$$\frac{\partial}{\partial c_A}\pi_P(c_A, c_B) < 0, \text{ for } c_A > c_B = c_C, \tag{146}$$

$$\frac{\partial}{\partial c_A}\pi_P(c_A, c_B) > 0, \text{ for } c_A < c_B = c_C \tag{147}$$

But this follows, as in the privately optimal case, from the convexity of $\alpha(\cdot)$.

If $(-\alpha'(0)) < f/R$, then the function $-g(c)$ does not cross the value $f/R$. Hence, the social profit function is monotonically decreasing in $c$, and the unique symmetric social optimum is zero investment $\hat{c}_i = 0$.

□

*Proof.* [Proposition 3.3] Fix some tuple of data investment choices $(c_A, c_B, c_C)$ . Note that $\alpha' < 0$ and $\alpha(c) \in [0, 1]$ for every $c$. Therefore, the last two terms of the planner's marginal profit in (74) are positive. Hence, in every investment choice point $(c_A, c_B, c_C)$ and for every entity $i \in \{A, B, C\}$, the planner's marginal profit exceeds the private marginal profit of that entity,

$$\frac{\partial}{\partial c_i}\pi_P(c_A, c_B, c_C) > \frac{\partial}{\partial c_i}\pi_i(c_A, c_B, c_C). \tag{148}$$

For comparing interior equilibria, we set the investment choices $(c_A, c_B, c_C)$ equal to the symmetric social equilibrium $\hat{c}_i$. When evaluating each entity i's private profit function at the social optimum, the derivative must be negative, and therefore, undercut the value the derivative of the private profit function takes in the symmetric private solution,

$$\frac{\partial}{\partial c_i}\pi_i(\hat{c}_i) < \frac{\partial}{\partial c_i}\pi_P(\hat{c}_i) = 0 = \frac{\partial}{\partial c_i}\pi_i(c_i^*) \tag{149}$$

As the last step, recall that for an interior equilibrium, we require strict convexity of $\alpha(c)$ which implies that all profit functions $\pi_i$ are strictly concave in $c_i$:

$$\frac{\partial^2}{\partial c_i^2}\pi_i(c_i) = -\alpha''(c_i)\left(\sum_{j\in\{A,B,C\}\setminus\{i\}}\alpha(c_j) - \prod_{j\in\{A,B,C\}\setminus\{i\}}\alpha(c_j)\right) R(|I_i|) < 0 \tag{150}$$

But strict concavity of the profit function then implies $c_A^* < \hat{c}_A$. Likewise for C and B. □

## 8.2 Fedwire

*Proof.* [Proposition 3.4] First, see that in the subgame $c_F$, A's profit function is strictly concave in $c_A$

$$\frac{\partial^2}{\partial c_A^2}\pi_A(c_A) = -\alpha''(c_A)\alpha(c_F)(\alpha(c_B)+\alpha(c_C)-\alpha(c_B)\alpha(c_C))\ R(|I_A|) < 0 \tag{151}$$

by convexity of $\alpha(c)$. Therefore, the maximizer $c_A$ is unique. In the symmetric equilibrium $c_A^{*,F} = c_B^{*,F} = c_C^{*,F}$, the first order derivative becomes

$$\frac{\partial}{\partial c_A}\pi_A(c_A) = -\alpha'(c_A)\alpha(c_F)(2\alpha(c_A)-\alpha(c_A)^2)\ R(|I_A|) - \ f(|I_A| \tag{152}$$

Recall that the function $g(c) = \alpha'(c)(2\alpha(c)-\alpha^2(c))$ is strictly increasing and continuous. This implies that the symmetric private equilibrium is unique in every subgame $c_F$. Further, the function $-g(c)$ takes its maximum in zero and its minimum at infinity.

(ii) If $c_F$ is such that $-\alpha'(0)[2\alpha(0)-\alpha(0)^2] = -\alpha'(0) \leq \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$, then for all $c \in [0,\infty]$: $-\alpha'(c)[2\alpha(c)-\alpha(c)^2] \leq \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$, meaning the symmetric equilibrium is given as $c_i^* = 0$.

(iii) If for given $c_F$, it holds $-\lim_{c\to\infty}\alpha'(c)[2\alpha(c)-\alpha(c)^2] \geq \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$, then likewise, the symmetric equilibrium is given by $c_i^* = \infty$. We however exclude this possibility via assumption 2.1.

(i) An interior symmetric equilibrium requires that $c_A$ solves

$$-\alpha'(c_A)\alpha(c_F)(2\alpha(c_A)-\alpha(c_A)^2) = \frac{f(|I_A|)}{R(|I_A|)} \tag{153}$$

The symmetric equilibrium is interior if $c_F$ is such that $-\alpha'(0)[2\alpha(0)-\alpha(0)^2] = -\alpha'(0) > \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$ *and* $-\lim_{c\to\infty}\alpha'(c)[2\alpha(c)-\alpha(c)^2] = 0 < \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$ hold. The latter is always true by assumption 2.1.

Moreover the solution to (153) is indeed an equilibrium by the same reasoning as in the case without the Fed. □

*Proof.* [Proposition 3.1]

Because $\alpha(c)$ is strictly decreasing, the function $\frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$ is strictly increasing, and continuous in $c_F$ for $c_F \geq 0$. Further, it holds

$$\frac{f(|I_A|)}{R(|I_A|)} = \lim_{c_F\to 0}\ \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)} \leq \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)} \leq \lim_{c_F\to\infty}\ \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)} = \infty, \tag{154}$$

or, $\frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)} \in \left[\frac{f(|I_A|)}{R(|I_A|)}, \infty\right)$. Recall the definition $g(c) \equiv \alpha'(c)[2\alpha(c) - \alpha(c)^2]$ from above, and that $-g$ is continuous, positive, and strictly decreasing, taking its maximum in zero.

If $-\alpha'(0)[2\alpha(0) - \alpha(0)^2] = -\alpha'(0) < \frac{f(|I_A|)}{R(|I_A|)}$, then by (154) there exists no $c_F$ with $-\alpha'(0)[2\alpha(0) - \alpha(0)^2] > \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)}$. Hence, no Fedwire choice $c_F \in [0, \infty]$ can prevent the symmetric "no investment" equilibrium $c^* = 0$.

Recall that by Proposition 3.1, the condition $-\alpha'(0) = -\alpha'(0)[2\alpha(0) - \alpha(0)^2] < \frac{f(|I_A|)}{R(|I_A|)}$ implies that the unique symmetric private equilibrium in the Double cover case is the no-investment equilibrium $c^* = 0$. □

## 8.3 Proof main Theorems

*Proof.* [Theorem 4.1] Consider the Fedwire objective function (33). When calculating the first-order derivative with respect to $c_F$, we need to take into account that a change in the subgame $c_F$ causes a change of behavior by A,B,C. In addition, we use the symmetry $|I_A| = |I_B| = |I_C|$ to calculate

$$\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F)$$

$$= -\alpha'(c_F)\Big[\alpha(c_A)(\alpha(c_B) + \alpha(c_C) - \alpha(c_B)\alpha(c_C)))\ R(|I_A|) \tag{155}$$

$$+ \alpha(c_B)(\alpha(c_A) + \alpha(c_C) - \alpha(c_A)\alpha(c_C)))\ R(|I_B|) \tag{156}$$

$$+ \alpha(c_C)(\alpha(c_A) + \alpha(c_B) - \alpha(c_A)\alpha(c_B)))\ R(|I_C|)\Big] - f(|I|) \tag{157}$$

$$- \alpha'(c_A)\frac{\partial c_A}{\partial c_F}\alpha(c_F)(\alpha(c_B) + \alpha(c_C) - \alpha(c_B)\alpha(c_C)))\ R(|I_A|) - \frac{\partial c_A}{\partial c_F}f(|I_A|) \tag{158}$$

$$- \alpha'(c_B)\frac{\partial c_B}{\partial c_F}\alpha(c_F)(\alpha(c_A) + \alpha(c_C) - \alpha(c_A)\alpha(c_C)))\ R(|I_B|) - \frac{\partial c_B}{\partial c_F}f(|I_B|) \tag{159}$$

$$- \alpha'(c_C)\frac{\partial c_C}{\partial c_F}\alpha(c_F)(\alpha(c_A) + \alpha(c_B) - \alpha(c_A)\alpha(c_B)))\ R(|I_C|) - \frac{\partial c_C}{\partial c_F}f(|I_C|) \tag{160}$$

$$- \alpha(c_A)\alpha(c_F)(\alpha'(c_B)\frac{\partial c_B}{\partial c_F} + \alpha'(c_C)\frac{\partial c_C}{\partial c_F} - (\alpha(c_C)\alpha'(c_B)\frac{\partial c_B}{\partial c_F} + \alpha'(c_C)\alpha(c_B)\frac{\partial c_C}{\partial c_F}))\ R(|I_A|) \tag{161}$$

$$- \alpha(c_B)\alpha(c_F)(\alpha'(c_A)\frac{\partial c_A}{\partial c_F} + \alpha'(c_C)\frac{\partial c_C}{\partial c_F} - (\alpha(c_C)\alpha'(c_A)\frac{\partial c_A}{\partial c_F} + \alpha'(c_C)\alpha(c_A)\frac{\partial c_C}{\partial c_F}))\ R(|I_B|) \tag{162}$$

$$- \alpha(c_C)\alpha(c_F)(\alpha'(c_A)\frac{\partial c_A}{\partial c_F} + \alpha'(c_B)\frac{\partial c_B}{\partial c_F} - (\alpha(c_B)\alpha'(c_A)\frac{\partial c_A}{\partial c_F} + \alpha'(c_B)\alpha(c_A)\frac{\partial c_B}{\partial c_F}))\ R(|I_C|) \tag{163}$$

In the symmetric equilibrium, $c_A = c_B = c_C$ and $\frac{\partial c_A}{\partial c_F} = \frac{\partial c_B}{\partial c_F} = \frac{\partial c_C}{\partial c_F}$. Therefore,

we can simplify

$$\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_B^{*,F}, c_C^{*,F}, c_F)$$

$$= -3\alpha'(c_F)\ R(|I_A|)\Big(2\alpha^2(c_A) - \alpha^3(c_A)\Big) - f(|I|) \tag{164}$$

$$- 3\alpha'(c_A)\alpha(c_A)\alpha(c_F)\frac{\partial c_A}{\partial c_F}(2-\alpha(c_A))\ R(|I_A|) - 3\frac{\partial c_A}{\partial c_F}f(|I_A|) \tag{165}$$

$$- 6\alpha'(c_A)\alpha(c_A)\alpha(c_F)\frac{\partial c_A}{\partial c_F}(1-\alpha(c_A))\ R(|I_A|) \tag{166}$$

$$= -3\alpha^2(c_A)\alpha'(c_F)\ R(|I_A|)\Big(2-\alpha(c_A)\Big) - f(|I|) - 3\frac{\partial c_A}{\partial c_F}f(|I_A|) \tag{167}$$

$$- 3\alpha(c_A)\alpha'(c_A)\frac{\partial c_A}{\partial c_F}\alpha(c_F)\ R(|I_A|)\ (4-3\alpha(c_A)) \tag{168}$$

**Case 1:** Assume $-\alpha'(0) < \frac{f(|I_A|)}{R(|I_A|)}$. This implies that the attack probability is rather inelastic, declining slowly for a small investment in data security. In this case, Theorem 3.1 (ii) implies that the unique symmetric private equilibrium in the case without Fedwire equals the no investment corner equilibrium $c_i^* = 0$. Moreover, adding Fedwire does not change the symmetric equilibrium, and banks continue to play $c_A^* = 0$ for every $c_F \geq 0$. That is, the marginal change in the symmetric equilibrium due to a change in the subgame is zero, $\frac{\partial c_A}{\partial c_F} = 0$.

We would like to find out whether adding Fedwire, by setting $c_F > 0$, nevertheless creates value. For that purpose, we evaluate the change in welfare due to a change in $c_F$ in the symmetric equilibrium $c_i^* = 0$ for all $i \in \{A, B, C\}$ and $c_F = 0$. Recall that the choice $c_F = 0$ indicates absence of Fedwire. With (168) and $\alpha(0) = 1$,

$$\frac{\partial}{\partial c_F}\pi_P(0,0,0,0) = 3R(|I_A|)\Big((-\alpha'(0)) - \frac{f(|I|)}{3R(|I_A|)}\Big) \tag{169}$$

There are two cases:
1a) If $(-\alpha'(0)) \in (0, \frac{f(|I|)}{3R(|I_A|)}]$, then $\frac{\partial}{\partial c_F}\pi_P(0,0,0,0) \leq 0$. Thus, Fedwire's socially optimal investment in data security is $c_F^* = 0$. Fedwire should abstain from providing an additional cover. In $(-\alpha'(0)) = \frac{f(|I|)}{3R(|I_A|)}$ the benefits of providing Fedwire equal the costs. In that case, we break ties by letting Fedwire abstain.
1b) If $(-\alpha'(0)) \in (\frac{f(|I|)}{3R(|I_A|)}, \frac{f(|I_A|)}{R(|I_A|)}]$, then $\frac{\partial}{\partial c_F}\pi_P(0,0,0,0) > 0$. Thus, the security benefits of providing Fedwire outweight the costs, $c_F^* > 0$.

**Case 2:** Assume $-\alpha'(0) > \frac{f(|I_A|)}{R(|I_A|)}$ so that absent Fedwire the banks play the

interior symmetric private equilibrium $c_i^* > 0$, $i = A, B, C$. Akin to the case above, we need to evaluate the change in welfare due to a change in $c_F$ in the symmetric equilibrium $c_i^* > 0$ for all $i \in \{A, B, C\}$ and $c_F = 0$. At an interior equilibrium, we can use the FOC (29) evaluated in $c_F = 0$ to further simplify (168) to

$$\frac{\partial}{\partial c_F}\pi_P(c_A^{*,F}, c_F)$$

$$= 3R(|I_A|)\Big( -\alpha'(c_F)\,\alpha^2(c_A)\Big(2-\alpha(c_A)\Big) - \frac{f(|I|)}{3R(|I_A|)} \tag{170}$$

$$- \frac{\partial c_A}{\partial c_F}\left[\frac{f}{R} + \alpha(c_A)\alpha'(c_A)\alpha(c_F)(4-3\alpha(c_A))\right] \tag{171}$$

$$= 3R(|I_A|)\Big( -\alpha'(c_F)\,\alpha^2(c_A)\Big(2-\alpha(c_A)\Big) - \frac{f(|I|)}{3R(|I_A|)} \tag{172}$$

$$- 2\frac{\partial c_A}{\partial c_F}\alpha(c_F)\,\alpha'(c_A)\alpha(c_A)(1-\alpha(c_A))\Big) \tag{173}$$

$$= 3R(|I_A|)\Big[\frac{f(|I|)}{R(|I_A|)}\left(\frac{\alpha'(c_F)/\alpha(c_F)}{\alpha'(c_A)/\alpha(c_A)} - \frac{1}{3}\right) + 2\frac{\partial c_A}{\partial c_F}\alpha(c_F)\,(-\alpha'(c_A))\alpha(c_A)(1-\alpha(c_A))\Big] \tag{174}$$

where at the second equality sign we have rewritten the third term in (168), replacing $f/R$, via the FOC (29). At the third equality sign we have rewritten the first term in (168), replacing $\alpha(c_A)(2-\alpha(c_A))$ via the FOC (29).

First, see that the second term in the edgy bracket is always negative because $\frac{\partial c_A}{\partial c_F} < 0$. This term indicates that all firms shirk as Fedwire increases its investment in data security, leading to a reduction in expected profits and thus Fedwire's objective. The first term can have either sign. In the first term, the $-1/3$ represents that Fedwire's investment in data security is costly. On the other hand, the term $\frac{\alpha'(c_F)/\alpha(c_F)}{\alpha'(c_A)/\alpha(c_A)}$ represents that Fedwire's investment increases security to all institutions. The latter effect is the only positive effect of Fedwire's investment.

The first term to be positive is a necessary condition for Fedwire's investment to be optimal. To determine when the first term is positive, plug in $c_F = 0$, and use $\alpha(0) = 1$. We see that the first term is positive if

$$\frac{\alpha'(0)}{\alpha'(c_A)/\alpha(c_A)} - \frac{1}{3} > 0. \tag{175}$$

That is, (175) is a necessary condition for $c_F^* > 0$.

Because $c_i^* > 0$ is the unique interior symmetric equilibrium, we know

$-\alpha'(0) > \frac{f(|I_A|)}{R(|I_A|)}$, and via the FOC, $-\alpha'(c_A^*)\alpha(c_A^*)(2-\alpha(c_A^*)) = \frac{f(|I_A|)}{R(|I_A|)}$. Plugging this in yields

$$\frac{\alpha'(0)}{\alpha'(c_A)/\alpha(c_A)} = \frac{-\alpha'(0)}{-\alpha'(c_A)/\alpha(c_A)} > -\frac{\frac{f(|I_A|)}{R(|I_A|)}}{\alpha'(c_A)/\alpha(c_A)} = \alpha(c_A^*)^2(2-\alpha(c_A^*)) \quad (176)$$

That is, for $\alpha(c_A^*)^2(2-\alpha(c_A^*)) > \frac{1}{3}$, the first term in the bracket is positive, and this holds if $\alpha(c_A^*) \in (0,1)$ is sufficiently close to one, that is, for $c_A^*$ small and close to zero. Overall, the first term needs to be traded off against the second term.

□

### 8.3.1 Proof Theorem 2

*Proof.* [Theorem 4.1]

**Case (i)** Consider $(-\alpha'(0)) < (0, \frac{f(|I|)}{3R(|I_A|)})$. Then by Theorem 4.1, $c_A^F = 0$, $c_F = 0$ and hence, $\Pi_P^{Fed} = 0$. On the other hand, by Proposition 3.2, also $c_i^{*,soc} = 0$, and thus $\Pi_P^{DC} = 0$. Thus, welfare in the Fedwire case and the social optimum with Double Covers coincide.

**Case (ii)** In the case $(-\alpha'(0)) \in (\frac{f(|I|)}{3R(|I_A|)}, \frac{f(|I|)}{R(|I_A|)})$, we know from Theorem 4.1 that the private entities still do not invest $c_i^{*,F} = 0$ but Fedwire does $c_F^* > 0$. Therefore, with $\alpha(0) = 1$,

$$\Pi_P^{Fed} = 3\left[(1-2\alpha^2(c_A^F)\alpha(c_F) + \alpha^3(c_A^F)\alpha(c_F))R(|I_A|) - c_A^F f(|I_A|)\right] - c_F\, f(|I|) \quad (177)$$

$$= 3\left[(1-2\alpha(c_F) + \alpha(c_F))R(|I_A|)\right] - c_F\, f(|I|) \quad (178)$$

$$= 3(1-\alpha(c_F))R(|I_A|) - c_F\, f(|I|) > 0 \quad (179)$$

On the other hand, by Proposition 3.2, the social planner in the Double Cover case still does not invest, $c_i^{*,soc} = 0$, implying $\Pi_P^{DC} = 0$. Thus welfare in the Fedwire case exceeds welfare in the social optimum with Double Covers.

**Case (iii)** Assume assumption 2.1(ii) additionally holds, $(-\alpha'(0)) > \frac{f(|I|)}{R(|I_A|)}$. Then by Theorem 4.1 in the Fedwire case, the private instutions play the symmetric private interior equilibrium $c_i^{*,F} > 0$. This interior equilibrium is charac-

terized as the solution to (29), repeated here as

$$-\alpha'(c_A^{*,F})\alpha(c_A^{*,F})[2-\alpha(c_A^{*,F})] = \frac{1}{\alpha(c_F)}\frac{f(|I_A|)}{R(|I_A|)} \tag{180}$$

Fedwire, in return, may or may not invest $c_F^* \geq 0$ depending on the sign in (174). For the Double Cover case, by Proposition 3.2 the social planner optimally sets an interior investment in security $c_i^{*,soc} > 0$. The interior socially optimal investment is characterized as the solution to equation (24),

$$-\alpha'(\hat{c}_A)(2-\alpha(\hat{c}_A)) = \frac{f(|I_A|)}{R(|I_A|)}. \tag{181}$$

A closed form solution to inequality (37) is not possible to compute and we resort to numerical solutions.

□

## 8.4 Generalization with N entities

### 8.4.1 Private Equilibrium

*Proof.* [Proposition 6.1] To show existence of an interior symmetric private equilibrium, see that for $c_{i_N} \to 0$, by $\alpha(0) = 1$, the left hand side of (64) goes to $-\alpha'(0)$. For $c_{i_N} \to \infty$, the left hand side goes to zero by $\alpha(c) \to 0$ and since $\alpha(c)$ is decreasing and convex. If $-\alpha'(0) > f/R$, the left hand side of (64) as a function of $c$ crosses $f/R$ at least once, guaranteeing existence of a candidate for an interior symmetric private equilibrium $c = c_{i_1} = \cdots = c_{i_N}$ at which the FOC holds.

The candidate is indeed an equilibrium: Assume that $c_{i_N} < c = c_{i_1} = \cdots = c_{i_{N-1}}$. Then, by convexity of $\alpha(c)$,

$$\begin{aligned}\frac{\partial}{\partial c_{i_N}}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}}=c) &= -\alpha'(c_{i_N}) \times \sum_{j=1}^{N-1}\alpha(c)\prod_{m=1}^{j-1}(1-\alpha(c))\,R_{i_N} - f(I_{i_N}) \\ &> -\alpha'(c) \times \sum_{j=1}^{N-1}\alpha(c)\prod_{m=1}^{j-1}(1-\alpha(c))\,R_{i_N} - f(I_{i_N}) = 0\end{aligned} \tag{182}$$

Thus, $c_{i_N} < c$ is not optimal. By the same argument, $c_{i_N} > c$ is not optimal because $\frac{\partial}{\partial c_{i_N}}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}}=c) < 0$, showing that $c = c_{i_1} = \cdots = c_{i_N}$ is an equilibrium.

To show uniqueness, we require single-crossing. Consider the function $g(c) = \alpha'(c) \times \left[1 - (1 - \alpha(c))^{N-1}\right]$. This function is strictly increasing because $\left[1 - (1 - \alpha(c))^{N-1}\right] > 0$, and thus, $g'(c) = \alpha''(c)\left[1 - (1 - \alpha(c))^{N-1}\right] + (N-1)\,\alpha'(c)^2\,(1-\alpha(c))^{N-2} > 0$, by convexity of $\alpha(c)$. Therefore, the function $-g(c)$ crosses $f/R$ only once, if at all. Therefore, if $-\alpha'(0) > f/R$, there exists a unique symmetric private equilibrium which is interior, characterized by (66). Assumption 2.1 covers $-\alpha'(0) \leq f/R$. If $-\alpha'(0) \leq f/R$, then there exists no crossing of $f/R$, the interior symmetric equilibrium does not exist, and the symmetric equilibrium is at $c = 0$ instead.

□

### 8.4.2 Private Fedwire Equilibrium: stage 2

*Proof.* [Proposition 6.2]

To show existence of an interior symmetric private Fedwire equilibrium, see that for $c_{i_N} \to 0$, by $\alpha(0) = 1$, the left hand side of (64) goes to $-\alpha'(0)$. For $c_{i_N} \to \infty$, the left hand side goes to zero by $\alpha(c) \to 0$ and since $\alpha(c)$ is decreasing and convex. If $-\alpha'(0) > f/R$, the left hand side of (64) as a function of $c$ crosses $f/R$ at least once, guaranteeing existence of a candidate for an interior symmetric private equilibrium $c = c_{i_1} = \cdots = c_{i_N}$ at which the FOC holds.

The candidate is indeed an equilibrium: Assume that $c_{i_N} < c = c_{i_1} = \cdots = c_{i_{N-1}}$. Then, by convexity of $\alpha(c)$,

$$\begin{aligned}\frac{\partial}{\partial c_{i_N}}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}} = c) &= -\alpha'(c_{i_N}) \times \sum_{j=1}^{N-1}\alpha(c)\prod_{m=1}^{j-1}(1-\alpha(c))\,R_{i_N} - f(I_{i_N}) \\ &> -\alpha'(c) \times \sum_{j=1}^{N-1}\alpha(c)\prod_{m=1}^{j-1}(1-\alpha(c))\,R_{i_N} - f(I_{i_N}) = 0\end{aligned} \tag{183}$$

Thus, $c_{i_N} < c$ is not optimal. By the same argument, $c_{i_N} > c$ is not optimal because $\frac{\partial}{\partial c_{i_N}}\Pi_{i_N}(c_{i_N}|c_{i_1},\ldots,c_{i_{N-1}} = c) < 0$, showing that $c = c_{i_1} = \cdots = c_{i_N}$ is an equilibrium.

To show uniqueness, we require single-crossing. Consider the function $g(c) = \alpha'(c) \times \left[1 - (1 - \alpha(c))^{N-1}\right]$. This function is strictly increasing because $\left[1 - (1 - \alpha(c))^{N-1}\right] > 0$, and thus, $g'(c) = \alpha''(c)\left[1 - (1 - \alpha(c))^{N-1}\right] + (N-1)\,\alpha'(c)^2\,(1-\alpha(c))^{N-2} > 0$, by convexity of $\alpha(c)$. Therefore, the function $-g(c)$ crosses $f/R$ only once, if at all. Therefore, if $-\alpha'(0) > f/R$, there exists a unique symmetric private equilibrium which is interior, characterized by (66). Assumption 2.1 covers $-\alpha'(0) \leq f/R$.

If $-\alpha'(0) \leq f/R$, then there exists no crossing of $f/R$, the interior symmetric equilibrium does not exist, and the symmetric equilibrium is at $c = 0$ instead.

□