Supplementary Online Appendix:
A Theory Model of Digital Currency with Asymmetric Privacy

March 2025

Abstract

This appendix includes more detailed proofs of the statements in the main paper "Theory Model of Digital Currency with Asymmetric Privacy". It also provides proofs of uniqueness statements and a generalization of key insights regarding mixed strategies and a wider set of tax policies.

Keywords: Central bank digital currency design, data privacy, learning, real effects of privacy preferences, verification costs, technological tools for privacy.

JEL Codes: C70, D18, D83, E42, E58, G21, G23, L86

O.1 Generalization of aspects of the setting

As in the main paper, the firm has N target consumers, and each consumer n is characterized by their valuation of the product, $v_n \in \{0,1\}$, and their privacy-sensitive traits, $T_n \in \{A, B\}$. It holds that $\Pr(T_n = A) = q_A$, $\Pr(T_n = B) = 1 - q_A$, $\Pr(v_n = 1|T_n = A) = z_A$ and $\Pr(v_n = 1|T_n = B) = z_B < z_A$. Consumer valuations are conditionally independent and the unconditional probability $\Pr(v_n = 1) = q_A z_A + (1 - q_A) z_B \equiv \bar{z}$.

When considering the equilibrium in the product market, the analysis in this Appendix also considers the possibility that consumers may adopt mixed strategies. For this, it is useful to define the consumers' actions, strategies and beliefs separately and extend the definition of the privacy loss to include the set of equilibrium beliefs.

Let $b_{\{v_n,T_n\}}$ denote the actual purchase decision of a consumer defined as

$$b_{\{v_n,T_n\}} = \begin{cases} 1 \text{ if consumer } n \text{ of type } \{v_n, T_n\} \text{ buys} \\ 0 \text{ if consumer } n \text{ of type } \{v_n, T_n\} \text{ does not buy} \end{cases}. \tag{1}$$

Additionally, let $\sigma_{\{v_n,T_n\}}$ denote the possibly mixed strategy of a consumer. There are four consumer types $\{v_n, T_n\} = \{0,1\} \times \{A, B\}$, and each type follows and must be believed to follow the same (possibly mixed) strategy, $\sigma_{\{v_n,T_n\}}$, on the equilibrium path. Denoting the belief that consumers of type

$\{v_n, T_n\}$ buy the product with $\tilde{\sigma}_{\{v_n,T_n\}}$, such that the belief set is $\mathcal{B} = \left\{\tilde{\sigma}_{\{0,A\}}, \tilde{\sigma}_{\{0,B\}}, \tilde{\sigma}_{\{1,A\}}, \tilde{\sigma}_{\{1,B\}}\right\}$. This belief set includes 16 ex-ante possibilities for pure strategies and a wider set of mixed strategies.

Following the analysis in Section 3.2 of the main paper, the consumer's indirect utility is

$$V\left(v_n, T_n, b_{\{v_n,T_n\}}; \mathcal{B}\right) = \begin{cases} v_n - p - \frac{\epsilon}{2}\mathbb{E}\left[\mathcal{L}\left(\Omega, \mathcal{B}\right)|v_n, T_n, b_{\{v_n,T_n\}} = 1\right] & \text{if } b_{\{v_n,T_n\}} = 1 \\ -\frac{\epsilon}{2}\mathbb{E}\left[\mathcal{L}\left(\Omega, \mathcal{B}\right)|v_n, T_n, b_{\{v_n,T_n\}} = 0\right] & \text{if } b_{\{v_n,T_n\}} = 0 \end{cases}, \quad (2)$$

where p is the price charged by the firm, $\epsilon \geq 0$ is a parameter capturing the importance of privacy concern, and $\mathcal{L}\left(\Omega, \mathcal{B}\right)$ reflects learning about the consumer's privacy-sensitive traits.

The latter in turn is determined by the overall information set Ω regarding the level of detail about consumer n's purchases recorded on the digital payment ledger, and beliefs, $\mathcal{B}$. Learning about the consumer's privacy-sensitive traits is given by

$$\mathcal{L}\left(\Omega, \mathcal{B}\right) = \frac{\Pr\left[T_n|\Omega;\mathcal{B}\right]}{\Pr\left[T_n\right]} - \frac{\Pr[\tilde{T}_n|\Omega;\mathcal{B}]}{\Pr[\tilde{T}_n]}. \quad (3)$$

Note that is assumed in this Appendix that both consumer types have the same sensitivity to privacy concerns, i.e., they are equally likely to be targeted by the thieves described in the main setting. This is merely to simplify the exposition as the effect of differences in privacy concerns is analyzed in the main paper and the key elements of the proof do not rely on this difference.

The analysis in this Appendix also imposes lesser restrictions to the tax function $\tau\left(.\right)$ and financing contracts $\phi\left(.\right)$. Namely, it is assumed that the tax function $\tau\left(.\right)$ is strictly increasing and it is conjectured that the financing contract with external financiers, $\phi\left(.\right)$, is weakly increasing. This implies that the firm's total obligations, $\varphi_s \equiv p\tau_s + \phi\left(pS - p\tau_s\right)$ are strictly increasing in s. This formulation allows the tax policy to have different rates for different levels of reported sales. The only constraint imposed is that the total obligations function does not have too large upward jumps/is not too convex, i.e., $\frac{\varphi_{s+1}-\varphi_s}{\varphi_s-\varphi_{s-1}} \leq \frac{(1-H_{s-1})h_s}{(1-H_s)h_{s-1}}$ for any s. It will be show that $\frac{(1-H_{s-1})h_s}{(1-H_s)h_{s-1}} > 1$, and therefore this condition holds for any total obligations that are linear or weakly concave in s, including proportional taxes and typical financing contracts like debt or equity considered in the main paper.[1]

The appendix will start by highlighting some general statistical observations that apply in this setting and then proceed to analyze the PBE in the product market and the Mechanism Design problem.

[1] Weak concavity requires that $\varphi_{s+1} + \varphi_{s-1} - 2\varphi_s \leq 0 \Leftrightarrow \frac{\varphi_{s+1}-\varphi_s}{\varphi_s-\varphi_{s-1}} \leq 1$.

O.2 Useful statistical properties

O.2.1 Proof that the quantity sold is Binomial

The total quantity sold $S = \sum_{n=1}^{N} b_{\{v_n,T_n\}}$, and, as it will be shown in Part O.3, all possible Perfect Bayesian Equilibria, have the feature that either all consumers whose preference for the good is $v_n = 1$ buy the product, or a fraction of these consumers with $v_n = 1$ buy the product.

Consider the pure strategies first. It holds that $S = \sum_{n=1}^{N} v_n$. Because consumers' preferences are assumed to be conditionally independent, $\Pr(v_n, v_k|T_n, T_k) = \Pr(v_n|T_n)\Pr(v_k|T_k)$, it also follows that the unconditional preferences for the good are also independent across consumers, i.e., $\Pr(v_n, v_k) = \Pr(v_n)\Pr(v_k)$. To prove this, we can use the the law of total probability to derive

$$\begin{aligned}
\Pr(v_n, v_k) &= \sum_{T_n=\{A,B\}} \sum_{T_k=\{A,B\}} \Pr(T_n, T_k)\Pr(v_n, v_k|T_n, T_k) = \\
&= \sum_{T_n=\{A,B\}} \sum_{T_k=\{A,B\}} \Pr(T_n)\Pr(T_k)\Pr(v_n|T_n)\Pr(v_k|T_k) \\
&= \sum_{T_n=\{A,B\}} \Pr(T_n)\Pr(v_n|T_n) \sum_{T_k=\{A,B\}} \Pr(T_k)\Pr(v_k|T_k) = \Pr(v_n)\Pr(v_k) .
\end{aligned}$$

As unconditionally $\Pr(v_n = 1) = q_A z_A + (1 - q_A) z_B \equiv \bar{z}$, it follows from well known statistical properties that $S \sim \textit{Binomial}(N, \bar{z})$.

This independence extends to mixed strategies as the probability that a particular consumer with $v_n = 1$ buys the product is independent of other parameters of the model and thus $\Pr\left(b_{\{v_n,T_n\}} = 1\right) = \tilde{\sigma}\Pr(v_n = 1) = \tilde{\sigma}\bar{z}$, where $\tilde{\sigma}$ is the probability that a particular consumer buys the product, and thus $S \sim \textit{Binomial}(N, \tilde{\sigma}\bar{z})$.

O.2.2 Proof that the Hazard function of the Binomial Distribution is increasing

Claim O.2.1. *Suppose that $S \sim \textit{Binomial}(N, z)$. It holds that*

$$\frac{h_S}{1 - H_S} > \frac{h_{S-1}}{1 - H_{S-1}}. \tag{4}$$

Proof. Inequality (4) can be rewritten as follows:

$$\frac{h_S}{1 - \sum\limits_{s=0}^{S} h_s} > \frac{h_{S-1}}{1 - \sum\limits_{s=0}^{S-1} h_s},$$

$$h_S \sum_{s=S}^{N} h_s > h_{S-1} \sum_{s=S+1}^{N} h_s = h_{S-1} \sum_{s=S}^{N-1} h_{s+1},$$

$$h_N h_S + \sum_{s=S}^{N-1} \left(h_s h_S - h_{s+1} h_{S-1}\right) > 0.$$

As $h_N h_S > 0$ for any S, we just need to show that $h_s h_S \geq h_{s+1} h_{S-1}$ for any $s \geq S$. We find that

$$\begin{aligned} \frac{h_s h_S}{h_{s+1} h_{S-1}} &= \frac{\frac{N!}{s!(N-s)!} z^s (1-z)^{N-s} \frac{N!}{S!(N-S)!} z^S (1-z)^{N-S}}{\frac{N!}{(s+1)!(N-s-1)!} z^{s+1} (1-z)^{N-s-1} \frac{N!}{(S-1)!(N-S+1)!} z^{S-1} (1-z)^{S-V+1}} \\ &= \frac{(s+1)(N-S+1)}{(N-s)S}, \end{aligned}$$

which is clearly increasing in s, and bigger than zero when $s = S$ as

$$\frac{(S+1)(N-S+1)}{(N-S)S} > 1 \iff N+1 > 0.$$

□

O.3 Proofs of existence and uniqueness of Perfect Bayesian Equilibria in the product market, including mixed strategies

In any Perfect Bayesian Equilibrium, it must be the case that the strategies pursued by players are consistent with equilibrium strategies and beliefs about the strategies they may pursue, and beliefs are updated according to the Bayes' rule on the equilibrium path. This implies that the belief about the strategy pursued equals the actual purchasing decisions under any set of beliefs, i.e., $\tilde{\sigma}_{\{v_n,T_n\}} = \Pr\left(b_{\{v_n,T_n\}} = 1 | T_n, v_n; \mathcal{B}\right)$. This proof considers all possible belief structures, and identifes the set of belief structures that are consistent with PBE.

There is always a trivial PBE where $\sigma_{\{v_n,T_n\}} = \tilde{\sigma}_{\{v_n,T_n\}} = 0$ for all types, and the firm sets a very high price, guaranteeing that no consumer has an incentive to buy the product. However, because other parts of the model involve the firm needing to pay the investment cost and taxes if it is active, the only relevant and interesting PBE candidates are the ones where the firm makes a positive profit, i.e., it only considers PBE candidates where the price set by the firm, $p > 0$, and $\sigma_{\{v_n,T_n\}} = \tilde{\sigma}_{\{v_n,T_n\}} > 0$ at least for one type. This condition will be imposed from here onwards.

Defining

$$\Delta \mathcal{L}_{\{v_n,T_n\}} \equiv \mathbb{E}\left[\mathcal{L}(\Omega;\mathcal{B}) | T_n, v_n, b_{\{v_n,T_n\}} = 1\right] - \mathbb{E}\left[\mathcal{L}(\Omega;\mathcal{B}) | T_n, v_n, b_{\{v_n,T_n\}} = 0\right], \quad (5)$$

it follows from (2) that the consumer's optimal strategy is

$$\sigma_{\{v_n,T_n\}} = \begin{cases} 1 \text{ if } p < v_n - \frac{\epsilon}{2}\Delta\mathcal{L}_{\{v_n,T_n\}} \\ (0,1] \text{ if } p = v_n - \frac{\epsilon}{2}\Delta\mathcal{L}_{\{v_n,T_n\}} \\ 0 \text{ if } p > v_n - \frac{\epsilon}{2}\Delta\mathcal{L}_{\{v_n,T_n\}} \end{cases}. \tag{6}$$

For the sake of the argument, let us focus on the setting where the payment system is such that all individual purchases are recorded and observable by third parties, i.e., $\Omega = \left\{b_{\{v_n,T_n\}}\right\}^N = \{0,1\}^N$. The setting where no information is available is akin to the special case where privacy concerns are moot, i.e., $\epsilon = 0$. Furthermore, while the PBE under asymmetric privacy is different, all the proofs identifying plausible belief structures are similar.

By Bayes' rule, the prior distribution of T_n being known, and the law of total expectations,

$$\frac{\Pr(T_n|\Omega;\mathcal{B})}{\Pr(T_n)} = \frac{\Pr(\Omega|T_n;\mathcal{B})}{\Pr(\Omega;\mathcal{B})} = \frac{(1-z_{T_n})\Pr(\Omega|v_n=0,T_n;\mathcal{B}) + z_{T_n}\Pr(\Omega|v_n=1,T_n;\mathcal{B})}{\sum_{v_n=\{0,1\},T_n=\{A,B\}}\Pr(v_n|T_n)\Pr(T_n)\Pr(\Omega|v_n,T_n;\mathcal{B})},$$

where $z_{T_n} = \Pr(v_n = 1|T_n)$.

Denote $\Omega_{-n} = \{0,1\}^{N-1}$ the information that is observable on the payment ledger about all other consumers except n, such that we can express $\Omega = \left\{\Omega_{-n}, b_{\{v_n,T_n\}}\right\}$. Furthermore, as individual preferences and purchasing decisions are independent conditional on the type (and must be believed to be independent along any PBE), it holds that $\Pr(\Omega|T_n,v_n;\mathcal{B}) = \Pr(\Omega_{-n}|\mathcal{B})\Pr\left(b_{\{v_n,T_n\}}|T_n,v_n;\mathcal{B}\right)$. As the consumer of type $\{T_n, v_n\}$ is believed to buy the product with probability $\tilde{\sigma}_{\{T_n,v_n\}}$, it follows that

$$\frac{\Pr(T_n|\Omega;\mathcal{B})}{\Pr(T_n)} = \frac{\Pr\left(b_{\{v_n,T_n\}}|T_n;\mathcal{B}\right)}{\Pr\left(b_{\{v_n,T_n\}};\mathcal{B}\right)} = \begin{cases} \frac{(1-z_{T_n})\tilde{\sigma}_{\{0,T_n\}}+z_{T_n}\tilde{\sigma}_{\{1,T_n\}}}{\tilde{Z}} \text{ if } b_{\{v_n,T_n\}} = 1 \\ \frac{(1-z_{T_n})\left(1-\tilde{\sigma}_{\{0,T_n\}}\right)+z_{T_n}\left(1-\tilde{\sigma}_{\{1,T_n\}}\right)}{1-\tilde{Z}} \text{ if } b_{\{v_n,T_n\}} = 0 \end{cases},$$

where

$$\tilde{Z} \equiv (1-z_A)\,q_A\tilde{\sigma}_{\{0,A\}} + (1-z_B)(1-q_A)\,\tilde{\sigma}_{\{0,B\}} + z_A q_A\tilde{\sigma}_{\{1,A\}} + z_B(1-q_A)\,\tilde{\sigma}_{\{1,B\}}. \tag{7}$$

Using this and (3) in (5) and simplifying

$$\Delta\mathcal{L}_{\{v_n,A\}} = \frac{z_A\left(\tilde{\sigma}_{\{1,A\}} - \tilde{\sigma}_{\{0,A\}}\right) - z_B\left(\tilde{\sigma}_{\{1,B\}} - \tilde{\sigma}_{\{0,B\}}\right) + \left(\tilde{\sigma}_{\{0,A\}} - \tilde{\sigma}_{\{0,B\}}\right)}{\tilde{Z}\left(1-\tilde{Z}\right)} = -\Delta\mathcal{L}_{\{v_n,B\}}. \tag{8}$$

We can see from (8) that $\Delta\mathcal{L}_{\{1,T_n\}} = \Delta\mathcal{L}_{\{0,T_n\}}$ as the privacy depends on the core parameters of the model and beliefs, and not on v_n directly. This enables us to shorten the notation and define $\Delta\mathcal{L} \equiv \Delta\mathcal{L}_{\{1,A\}} = \Delta\mathcal{L}_{\{0,A\}}$, such that $\Delta\mathcal{L}_{\{1,B\}} = \Delta\mathcal{L}_{\{0,B\}} = -\Delta\mathcal{L}$. Using this, we can express (6) for different consumer types as

$$\sigma_{\{v_n,T_n\}} = \begin{cases} 1 \text{ if } \left\{p < v_n - \frac{\epsilon}{2}\Delta\mathcal{L} \wedge T_n = A\right\} \vee \left\{p < v_n + \frac{\epsilon}{2}\Delta\mathcal{L} \wedge T_n = B\right\} \\ (0,1] \text{ if } \left\{p = v_n - \frac{\epsilon}{2}\Delta\mathcal{L} \wedge T_n = A\right\} \vee \left\{p = v_n + \frac{\epsilon}{2}\Delta\mathcal{L} \wedge T_n = B\right\} \\ 0 \text{ if } \left\{p > v_n - \frac{\epsilon}{2}\Delta\mathcal{L} \wedge T_n = A\right\} \vee \left\{p > v_n + \frac{\epsilon}{2}\Delta\mathcal{L} \wedge T_n = B\right\} \end{cases} \tag{9}$$

Using these results together with the PBE requirement of consistency between strategies and beliefs, we can narrow the set of belief structures that are consistent with PBE, i.e., satisfy $\sigma_{\{v_n,T_n\}} = \tilde{\sigma}_{\{v_n,T_n\}}$.

Lemma O.3.1. *There are no Perfect Bayesian Equilibria where $\Delta\mathcal{L} < 0$.*

Proof. Suppose that there is a PBE where $\Delta\mathcal{L} < 0$. As we are seeking PBE where $p > 0$, by (9) it must hold that type $\{0, B\}$ never buys, i.e., $\sigma_{\{0,B\}} = 0$. As beliefs must be consistent with optimal strategies, it must also hold that $\tilde{\sigma}_{\{0,B\}} = 0$. From (9) it also follows that type $\{1, A\}$ must be most willing to buy, and whether type $\{1, B\}$ or $\{0, A\}$ is more willing to buy depends on $|\Delta\mathcal{L}|$. We have the following possibilities:

1) Consider that the firm has set $p \leq \min\left[-\frac{\epsilon}{2}\Delta\mathcal{L}, 1 + \frac{\epsilon}{2}\Delta\mathcal{L}\right]$ to ensure that both of these types buy, or $p \leq \max\left[-\frac{\epsilon}{2}\Delta\mathcal{L}, 1 + \frac{\epsilon}{2}\Delta\mathcal{L}\right]$ so that only one of these types buys. In either case, it must hold that type $\{v_n, T_n\} = \{1, A\}$ buys for sure and must be believed to do so on-path, i.e., $\sigma_{\{1,A\}} = \tilde{\sigma}_{\{1,A\}} = 1$. Using $\tilde{\sigma}_{\{0,B\}} = 0$ and $\tilde{\sigma}_{\{1,A\}} = 1$ in (8) we obtain that $\Delta\mathcal{L} \propto z_A - z_B + z_B\left(1 - \tilde{\sigma}_{\{1,B\}}\right) + (1 - z_A)\,\tilde{\sigma}_{\{0,A\}}$, which is strictly positive as $z_A > z_B$, and $\tilde{\sigma}_{\{1,B\}}, \tilde{\sigma}_{\{0,A\}} \in [0, 1]$. This contradicts $\Delta\mathcal{L} < 0$ and the belief structures that take the form $\mathcal{B} = \left\{\tilde{\sigma}_{\{0,A\}}, \tilde{\sigma}_{\{0,B\}}, \tilde{\sigma}_{\{1,A\}}, \tilde{\sigma}_{\{1,B\}}\right\} = \left\{\tilde{\sigma}_{\{0,A\}}, 0, 1, \tilde{\sigma}_{\{1,B\}}\right\}$ cannot be consistent.

2) Consider that the firm has set $\max\left[-\frac{\epsilon}{2}\Delta\mathcal{L}, 1 + \frac{\epsilon}{2}\Delta\mathcal{L}\right] < p \leq 1 + \frac{\epsilon}{2}\Delta\mathcal{L}$. From (9) it is then clear that $\sigma_{\{v_n,T_n\}} = 0$ for types $\{v_n, T_n\} = \{0, A\}, \{0, B\}, \{1, B\}$, and by consistency of beliefs and strategies, it must also hold that $\tilde{\sigma}_{\{0,A\}}, \tilde{\sigma}_{\{0,B\}}, \tilde{\sigma}_{\{1,B\}} = 0$. Using this in (8) we obtain that $\Delta\mathcal{L} \propto z_A\tilde{\sigma}_{\{1,A\}} > 0$, which again contradicts $\Delta\mathcal{L} < 0$ and a belief structure where only type $\{1, A\}$ buys the product with positive probability cannot be consistent.

3) Finally, if the firm has set $p > 1 + \frac{\epsilon}{2}\Delta\mathcal{L}$, no consumer buys and $\Delta\mathcal{L} = 0$, which again leads to a contradiction. $\square$

Lemma O.3.1 shows that belief structures that may be consistent with PBE cannot have the property that types with $T_n = A$ suffer a lesser privacy loss if they buy. This is intuitive as these consumers are more likely to value the product highly, i.e., $z_A > z_B$. Hence it must be the case in any PBE that $\Delta\mathcal{L} \geq 0$, and this is taken as given in what follows.

Lemma O.3.2. *There are no Perfect Bayesian Equilibria where $\Delta\mathcal{L} \geq \frac{1}{\epsilon}$.*

Proof. Suppose that there is a PBE where $\Delta\mathcal{L} \geq \frac{1}{\epsilon}$ and $p > 0$. As we are seeking PBE where $p > 0$, by (9) it must hold that type $\{0, A\}$ never buys and must be believed to never buy, i.e., $\sigma_{\{0,A\}} = \tilde{\sigma}_{\{0,A\}} = 0$. Furthermore, when $\Delta\mathcal{L} > \frac{1}{\epsilon}$ it holds that $\min\left[\frac{\epsilon}{2}\Delta\mathcal{L}, 1 - \frac{\epsilon}{2}\Delta\mathcal{L}\right] = 1 - \frac{\epsilon}{2}\Delta\mathcal{L}$. We have the following possibilities to consider:

1) Consider that the firm has set $p \leq 1 - \frac{\epsilon}{2}\Delta\mathcal{L}$. From (9) it then follows that type $\{1, A\}$ is willing to buy the product with a positive probability, while types $\{0, B\}$ and $\{1, B\}$ buy the product with probability 1. As beliefs must be consistent with strategies, it must hold that $\tilde{\sigma}_{\{0,B\}} = \tilde{\sigma}_{\{1,B\}} = 1$. However, by (8), it must then also be the case that $\Delta\mathcal{L} \propto z_A\tilde{\sigma}_{\{1,A\}} - 1 < 0$, which contradicts $\Delta\mathcal{L} > \frac{1}{\epsilon}$.

2) Consider that the firm has set $1 - \frac{\epsilon}{2}\Delta\mathcal{L} < p \leq \frac{\epsilon}{2}\Delta\mathcal{L}$. From (9) it then follows that type $\{v_n, T_n\} = \{1, A\}$ never buys the product, i.e., $\sigma_{\{1,A\}} = \tilde{\sigma}_{\{1,A\}} = 0$, type $\{0, B\}$ is willing to buy it at a positive probability, and type $\{1, B\}$ must buy the product with probability 1, i.e., $\sigma_{\{1,B\}} = \tilde{\sigma}_{\{1,B\}} = 1$. However by (8) this implies that $\Delta\mathcal{L} \propto -z_B - (1 - z_B)\,\tilde{\sigma}_{\{0,B\}} < 0$, which again contradicts $\Delta\mathcal{L} > \frac{1}{\epsilon}$.

3) Setting $p > \frac{\epsilon}{2}\Delta\mathcal{L}$ cannot also be consistent. The only type who could buy at $p > \frac{\epsilon}{2}\Delta\mathcal{L}$ is type $\{v_n, T_n\} = \{1, B\}$, i.e., it must be the case that $\tilde{\sigma}_{\{0,A\}}, \tilde{\sigma}_{\{0,B\}}, \tilde{\sigma}_{\{1,A\}} = 0$, which implies that $\Delta\mathcal{L} \propto -z_B\tilde{\sigma}_{\{1,B\}} \leq 0$ and contradicts $\Delta\mathcal{L} \geq \frac{1}{\epsilon}$. □

Lemmas O.3.1 and O.3.2 eliminate a wide set of belief structures as implausible and highlight that any plausible PBE must have $0 \leq \Delta\mathcal{L} \leq \frac{1}{\epsilon}$. By (9), this clearly establishes constraints that a plausible belief structure must follow. Namely, type $\{v_n, T_n\} = \{0, A\}$ never buys and must be believed to follow this strategy, i.e., $\tilde{\sigma}_{\{0,A\}} = 0$, type $\{0, B\}$ cannot be more likely to buy than type $\{1, A\}$, and the corresponding beliefs must have $0 \leq \tilde{\sigma}_{\{0,B\}} \leq \tilde{\sigma}_{\{1,A\}}$. Finally, it also holds that type $\{1, B\}$ must be the type who is most likely to buy the product in any plausible PBE.

We can then identify a set of plausible PBE as follows.

Proposition O.3.3. *Provided that $\epsilon \leq \frac{\bar{z}(1-\bar{z})}{z_A - z_B}$, there exists a PBE in pure strategies where $\sigma_{\{1,A\}} = \sigma_{\{1,B\}} = 1$, $\sigma_{\{0,A\}} = \sigma_{\{0,B\}} = 0$, $p = 1 - \frac{\epsilon}{2}\frac{z_A - z_B}{\bar{z}(1-\bar{z})}$, where $\bar{z} = Pr(v_n = 1)$ equals the expected demand by one consumer in equilibrium. Furthermore, this equilibrium is a unique equilibrium in pure strategies, and there is no PBE in pure strategies when $\epsilon > \frac{\bar{z}(1-\bar{z})}{z_A - z_B}$.*

Proof. As shown, a PBE could only exist when $0 \leq \Delta\mathcal{L} \leq \frac{1}{\epsilon}$. By (9) it follows that there are only three potentially plausible belief structures remaining to be considered: these are $\mathcal{B} = \left\{\tilde{\sigma}_{\{0,A\}}, \tilde{\sigma}_{\{0,B\}}, \tilde{\sigma}_{\{1,A\}}, \tilde{\sigma}_{\{1,B\}}\right\} = \{\{0,0,0,1\}, \{0,0,1,1\}, \{0,1,1,1\}\}$. Using these in (8), it follows that the first and the last belief structure cannot be consistent with $0 \leq \Delta\mathcal{L} \leq \frac{1}{\epsilon}$ as $\Delta\mathcal{L}_{\{0,0,0,1\}} \propto -z_B < 0$ and $\Delta\mathcal{L}_{\{0,1,1,1\}} \propto -(1-z_A) < 0$. Hence, the only plausible belief structure is $\mathcal{B} = \{0,0,1,1\}$, which by (8) and (7) gives $\Delta\mathcal{L}_{\{0,0,1,1\}} = \frac{z_A - z_B}{\bar{z}(1-\bar{z})}$. Clearly, $\frac{z_A - z_B}{\bar{z}(1-\bar{z})} > 0$. However, we also need $\Delta\mathcal{L} \leq \frac{1}{\epsilon}$, which implies that this equilibrium only exists if $\epsilon \leq \frac{\bar{z}(1-\bar{z})}{z_A - z_B}$. Furthermore, $0 \leq \Delta\mathcal{L} \leq \frac{1}{\epsilon}$ also implies that the firm must set the price $p \in \left(\frac{\epsilon}{2}\frac{z_A - z_B}{\bar{z}(1-\bar{z})}, 1 - \frac{\epsilon}{2}\frac{z_A - z_B}{\bar{z}(1-\bar{z})}\right]$ to induce only types $\{1,A\}$ and $\{1,B\}$ to buy. As replacing beliefs with actual demand in (7) gives the expected demand by a random consumer, the firm's expected profit under these strategies is $Np\bar{z}$, and the firm sets $p = 1 - \frac{\epsilon}{2}\frac{z_A - z_B}{\bar{z}(1-\bar{z})}$. As $\epsilon \leq \frac{\bar{z}(1-\bar{z})}{z_A - z_B}$, it holds that $p > \frac{1}{2} > 0$. □

Proposition O.3.3 shows that if the privacy concerns are not too pressing, there is an equilibrium where the firm offers enough of a discount to induce all consumers who value the product at $v_n = 1$ to buy the product. However, this comes at the cost of having to offer the product at a lower price.

While there is no PBE in pure strategies when ϵ is high, there always exist mixed strategy equilibria. In particular, there are always mixed strategy equilibria that fully conceal the consumer types.

Proposition O.3.4. *For any ϵ, there exist PBE in mixed strategies where type $\{1,B\}$ buys the product with probability $\sigma_{\{1,B\}} = \breve{\sigma} \in (0,1]$, type $\{1,A\}$ buys the product with probability $\sigma_{\{1,A\}} = \frac{z_B}{z_A}\breve{\sigma}$, and types $\{0,A\}$ and $\{0,B\}$ do not buy the product. The Pareto dominant equilibrium is the one where $\{1,B\}$ plays a pure strategy $\sigma_{\{1,B\}} = 1$ and $\{1,A\}$ plays a mixed strategy $\sigma_{\{1,A\}} = \frac{z_B}{z_A}$. The expected demand by one consumer in this Pareto dominant equilibrium is $z_B < \bar{z}$.*

Proof. Consumer types are fully concealed only when $\Delta\mathcal{L} = 0$. From (9), it then follows that types $\{0,A\}$ and $\{0,B\}$ would not buy the product at $p > 0$, while types $\{1,A\}$ and $\{1,B\}$ are willing to buy it as long as $p \leq 1$. Given this and the requirement of consistency of beliefs, it must be the case that $\Delta\mathcal{L} = \frac{z_A\tilde{\sigma}_{\{1,A\}} - z_B\tilde{\sigma}_{\{1,B\}}}{\tilde{Z}(1-\tilde{Z})} = 0$, where $\tilde{Z} = q_A z_A \tilde{\sigma}_{\{1,A\}} + (1-q_A) z_B \tilde{\sigma}_{\{1,B\}}$. Clearly there are multiple solutions to $z_A\tilde{\sigma}_{\{1,A\}} = z_B\tilde{\sigma}_{\{1,B\}}$ and as $\tilde{\sigma}_{\{1,B\}} \in (0,1]$ and $z_A > z_B$, it must be the case that $\{1,A\}$ uses a mixed strategy that is proportional to the strategy used by $\tilde{\sigma}_c = \breve{\sigma}$. It then follows that the expected demand by all consumers is $N\left(q_A z_A \left(\frac{z_B}{z_A}\breve{\sigma}\right) + (1-q_A) z_B \breve{\sigma}\right) = N z_B \breve{\sigma}$ and the firm's profit is $Npz_B\breve{\sigma}$. It is clear that it is optimal for the firm to set $p = 1$ and it is easy to confirm that both types $\{1,A\}$ and $\{1,B\}$ consumers are indifferent between buying and not buying and are willing to buy at any probability. As consumer surplus is zero, the joint surplus equals the firm's profit, which is maximized when $\breve{\sigma} = 1$. □

Proposition O.3.4 shows that there are always equilibria where some consumers forego the opportunity to buy a product they like to conceal their type. While there is no need for discounts in these PBE, the firm faces lower demand.

One may wonder if there are other mixed strategy equilibria. Given the above analysis, there are only two possible candidate belief structures to consider:

1. One where types $\{0, A\}$ and $\{0, B\}$ are believed to follow pure strategies not to buy, i.e., $\tilde{\sigma}_{\{0,A\}} = \tilde{\sigma}_{\{0,B\}} = 0$, type $\{1, B\}$ is believed to follow a pure strategy to buy, i.e., $\tilde{\sigma}_{\{1,B\}} = 1$, and type $\{1, A\}$ is indifferent and is believed to buy with probability $\tilde{\sigma}_{\{1,A\}} = \tilde{\sigma}'_A$, where $\tilde{\sigma}'_A \in (0, 1)$ and $\tilde{\sigma}'_A \neq \frac{z_B}{z_A}$.

2. One where type $\{0, A\}$ is believed to follow a pure strategy not to buy, i.e., $\tilde{\sigma}_{\{0,A\}} = 0$, types $\{1, A\}$ and $\{1, B\}$ are believed to follow pure strategies to buy, i.e., $\tilde{\sigma}_{\{1,A\}} = \tilde{\sigma}_{\{1,B\}} = 1$, and type $\{0, B\}$ is indifferent and is believed to buy with probability $\tilde{\sigma}_{\{0,B\}} = \tilde{\sigma}'_B$, where $\tilde{\sigma}'_B \in (0, 1)$.

We exclude both of these as being inconsistent with optimal strategies by consumers and firms.

Consider the first case. From (8) it follows that $\Delta\mathcal{L} = \frac{z_A\tilde{\sigma}'_A - z_B}{\tilde{z}'_A\left(1-\tilde{z}'_A\right)}$, where $\tilde{z}'_A = q_A z_A \tilde{\sigma}'_A + (1 - q_A)\, z_B$. As we have shown that it must hold that $\Delta\mathcal{L} > 0$ in any PBE equilibrium that does not involve consumers perfectly concealing their type, it must be the case that $\tilde{\sigma}'_A < \frac{z_A}{z_B}$. Note that this further implies that $\tilde{z}'_A \in (z_B, \bar{z})$. Furthermore, as type $\{1, A\}$ must be indifferent, it must be the case that $p = 1 - \frac{\epsilon}{2}\frac{z_A\tilde{\sigma}'_A - z_B}{\tilde{z}'_A\left(1-\tilde{z}'_A\right)} = 1 - \frac{\epsilon}{2}\frac{\tilde{z}'_A - z_B}{q_A\tilde{z}'_A\left(1-\tilde{z}'_A\right)}$. While we can verify using (9) that all consumers' optimal strategies are consistent with the conjectured beliefs, these beliefs are not consistent with the firm's optimal strategy. To see this, notice that when setting the price on-path, the firm must believe that the total demand is $N\tilde{z}'_A$. Hence its profit is $Np\tilde{z}'_A = N\left(1 - \frac{\epsilon}{2}\frac{\tilde{z}'_A - z_B}{q_A\tilde{z}'_A\left(1-\tilde{z}'_A\right)}\right)\tilde{z}'_A$. Differentiating this, we obtain that $\frac{\partial\left(Np\tilde{z}'_A\right)}{\partial\tilde{z}'_A} = N - N\frac{\epsilon}{2}\frac{1-2\tilde{z}'_A+z_B}{q_A\left(1-\tilde{z}'_A\right)^2}$ and $\frac{\partial^2\left(Np\tilde{z}'_A\right)}{\partial\tilde{z}'_A\partial\tilde{z}'_A} = N\epsilon\frac{\tilde{z}'_A - z_B}{q_A\left(1-\tilde{z}'_A\right)^2} > 0$ as $\tilde{z}'_A > z_B$. Because the firm's profit is convex in $\tilde{z}'_A$, it follows that it would set the price such that $\tilde{z}'_A$ is outside the range $(z_B, \bar{z})$, i.e., it would either have an incentive to set $p = 1$, in which case $\tilde{z}'_A = z_B$ and this choice corresponds to the PBE in Lemma O.3.4, or to set $p = 1 - \frac{\epsilon}{2}\frac{\bar{z}-z_B}{q_A\bar{z}(1-\bar{z})} = 1 - \frac{\epsilon}{2}\frac{z_A - z_B}{\bar{z}(1-\bar{z})}$, and this choice corresponds to the PBE in Lemma O.3.3.

Consider the second case. From (8) it follows that $\Delta\mathcal{L} = \frac{z_A - z_B - (1-z_B)\tilde{\sigma}'_B}{\tilde{z}'_B\left(1-\tilde{z}'_B\right)}$, where $\tilde{z}'_B = (1 - q_A)\,(1 - z_B)\,\tilde{\sigma}'_B + \bar{z}$. As it must hold that $\Delta\mathcal{L} > 0$, it must further hold that $\tilde{\sigma}'_B < \frac{z_A - z_B}{(1-z_B)}$. And as type $\{0, B\}$ must be indifferent, it must hold that $p = \frac{\epsilon}{2}\Delta\mathcal{L} = \frac{\epsilon}{2}\frac{z_A - z_B - (1-z_B)\tilde{\sigma}'_B}{\tilde{z}'_B\left(1-\tilde{z}'_B\right)}$. Using that the firm must expect the relationship between p and $\tilde{\sigma}'_B$ on path, its expected profit is $Np\tilde{z}'_B = N\frac{\epsilon}{2}\frac{z_A - z_B - (1-z_B)\tilde{\sigma}'_B}{\left(1-\tilde{z}'_B\right)} = N\frac{\epsilon}{2}\frac{z_A - z_B - (1-z_B)\tilde{\sigma}'_B}{\left(1-\bar{z}-(1-q_A)(1-z_B)\tilde{\sigma}'_B\right)}$. Differentiating this gives $\frac{\partial Np\tilde{z}'_B}{\partial\tilde{\sigma}'_B} =$

$-N\frac{\epsilon}{2}\frac{(1-z_B)(1-z_A)}{\left(1-\tilde{z}'_B\right)}$, which implies that the firm would set the price such that $\tilde{\sigma}'_B$ and $\tilde{z}'_B$ are as small as possible. In particular, the firm would set $p=\frac{\epsilon}{2}\frac{z_A-z_B}{\bar{z}(1-\bar{z})}$ such that $\tilde{\sigma}'_B=0$. However, this is outside the range. Furthermore, when $\tilde{\sigma}'_B=0$ the firm would have an incentive to deviate and set $p=1-\frac{\epsilon}{2}\frac{z_A-z_B}{\bar{z}(1-\bar{z})}$, which is higher and leads to the same demand.

O.4 Proofs of the solution to the Mechanism problem for auditing and financial contract design

The mechanism design problem is relevant for payment systems that are "symmetrically private"—those involving cash or its equivalents. This is because auditing is not needed, or is relatively cheap[2], when the firm's sales are recorded on the shared ledger. In this case, privacy concerns are moot, and the PBE in the product market is straightforward: the firm sets $p=1$, and all consumers with $v_n=1$ buy the product.[3] Because $p=1$, it holds that total obligations take the simpler form $\varphi_s\equiv\tau_s+\phi\left(S-\tau_s\right)$.

O.4.1 Optimal auditing policy

Building on Propositions 1-3 in Sanchez and Sobel, 1993, the optimal auditing policy takes the form[4]

$$\gamma_R=\begin{cases}\frac{1}{1+\delta}\text{ if }R<\bar{R}\\ 0\text{ if }R\geq\bar{R}\end{cases},\tag{10}$$

and it is optimal and incentive compatible for the firm to report

$$R=\begin{cases}S\text{ if }S\leq\bar{R}\\ \bar{R}\text{ if }S>\bar{R}\end{cases}.\tag{11}$$

That is, there exists an auditing threshold below which the firm's reports are optimally audited with a positive probability, while the highest reports are not necessarily audited. Consequently, it is optimal for the firm to report truthfully whenever its realized revenues are below this threshold and to report the minimum non-audited outcome when its revenues are higher.

While the full proofs do not need to be replicated, some key elements of the proofs are worth

[2] The analysis below shows that for it to be optimal to audit all firms, the auditing cost needs not to be zero.

[3] The logic of the proofs extends straightforwardly to other settings because the distribution remains Binomial (see O.2.1), but since auditing costs are negligible these results correspond to the ones with small c with the only difference being a lower price that only affects the magnitudes.

[4] The only minor difference in this context is that Sanchez and Sobel, 1993 consider continuous distribution, while this paper considers a discrete distribution.

re-emphasizing. First, it is never optimal for the firm to report $R > S$, as there is no reward from over-reporting and it leads to higher costs for the firm. Second, it is not optimal to set the auditing probability $\gamma_R > \frac{1}{1+\delta}$, as $\gamma_R = \frac{1}{1+\delta}$ already ensures that the firm prefers to report truthfully. Specifically, the difference between reporting $R = S$ and $R < S$ is $(\varphi_S - \varphi_R)(1 - (1+\delta)\gamma(R))$, which is non-negative whenever $\gamma(R) \leq \frac{1}{1+\delta}$ because $\varphi(.)$ is increasing. Auditing more frequently would only increase auditing costs without increasing the tax authority's and investors' revenues. Finally, because there are greater gains from under-reporting a greater amount if the firm is not audited, it follows that lower reports are the ones that need to be audited more frequently.

This implies that the optimal auditing policy boils down to determining the optimal auditing threshold $\bar{R}$, i.e., the question of whether it is sometimes optimal to tolerate some under-reporting at the highest sales outcomes instead of inducing truth-telling for all S.

Lemma O.4.1. *The optimal auditing policy sets the auditing threshold*

$$\bar{R}^* = \max\left\{\bar{R} \in \mathbb{Z}^+ |\left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right)\frac{1 - H_{\bar{R}-1}}{h_{\bar{R}-1}} - \frac{c}{1+\delta} \geq 0\right\}, \tag{12}$$

a sufficient condition for the threshold $\bar{R}^*$ to be unique is that $\frac{\left(\varphi_{\bar{R}+1} - \varphi_{\bar{R}}\right)}{\left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right)} < \frac{\left(1 - H_{\bar{R}-1}\right)h_{\bar{R}}}{(1 - H_{\bar{R}})h_{\bar{R}-1}}$. The latter holds when $\varphi(.)$ is weakly log-concave as assumed in the main paper.

Proof. Recall that the revenues of the tax authority and $\Phi(R) \equiv \mathbb{E}\left[\varphi_R + (1+\delta)\gamma_R(\varphi_S - \varphi_R) - c\gamma_R | R\right]$. Using (10) and (11) this can be expressed as

$$\begin{aligned}
\Phi\left(\bar{R}\right) &\equiv \mathbb{E}\left[\varphi_S - \frac{c}{1+\delta} \mid S < \bar{R}\right]\Pr\left(S < \bar{R}\right) + \varphi_{\bar{R}}\Pr\left(S \geq \bar{R}\right) \\
&= \sum_{S=0}^{\bar{R}-1}\left(\varphi_S - \frac{c}{1+\delta}\right)h_S + \varphi_{\bar{R}}\left(1 - H_{\bar{R}-1}\right),
\end{aligned}$$

and the optimal auditing policy must solve

$$\bar{R}^* = \arg\max_{\bar{R}} \Phi\left(\bar{R}\right).$$

This problem has a unique maximum if the difference $\Phi\left(\bar{R}+1\right) - \Phi\left(\bar{R}\right)$ changes sign at most once from positive to negative. We can write that

$$\Phi\left(\bar{R}+1\right) - \Phi\left(\bar{R}\right) = h_{\bar{R}}\left(\left(\varphi_{\bar{R}+1} - \varphi_{\bar{R}}\right)\frac{(1 - H_{\bar{R}})}{h_{\bar{R}}} - \frac{c}{1+\delta}\right).$$

Because $h_{\bar{R}} > 0$ for any $\bar{R}$, it is sufficient to show that $\left(\varphi_{\bar{R}+1} - \varphi_{\bar{R}}\right) \frac{(1-H_{\bar{R}})}{h_{\bar{R}}}$ is strictly decreasing in $\bar{R}$, i.e., that

$$\Lambda\left(\bar{R}\right) \equiv \left(\varphi_{\bar{R}+1} - \varphi_{\bar{R}}\right) \frac{(1-H_{\bar{R}})}{h_{\bar{R}}} - \left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right) \frac{\left(1-H_{\bar{R}-1}\right)}{h_{\bar{R}-1}}$$

is decreasing for any $\bar{R} > 0$.

We can rewrite this as

$$\Lambda\left(\bar{R}\right) \equiv \left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right) \left(\frac{\left(\varphi_{\bar{R}+1} - \varphi_{\bar{R}}\right)}{\left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right)} \frac{(1-H_{\bar{R}})}{h_{\bar{R}}} - \frac{\left(1-H_{\bar{R}-1}\right)}{h_{\bar{R}-1}} \right). \tag{13}$$

Because φ is increasing and the Binomial distribution has an increasing Hazard function (i.e., $\frac{h_{\bar{R}}}{1-H_{\bar{R}}} > \frac{h_{\bar{R}-1}}{1-H_{\bar{R}-1}} \Leftrightarrow \frac{(1-H_{\bar{R}})}{h_{\bar{R}}} < \frac{\left(1-H_{\bar{R}-1}\right)}{h_{\bar{R}-1}}$, see Section O.2.2 in this Online Appendix), it follows that $\Lambda\left(\bar{R}\right)$ is decreasing when φ is weakly concave, as assumed in the main paper. This is because weak concavity requires that $\varphi_{\bar{R}+1} + \varphi_{\bar{R}-1} - 2\varphi_{\bar{R}} \leq 0 \Longleftrightarrow \frac{\left(\varphi_{\bar{R}+1}-\varphi_{\bar{R}}\right)}{\left(\varphi_{\bar{R}}-\varphi_{\bar{R}-1}\right)} \leq 1$.

The sufficient condition for a unique solution is somewhat weaker and requires that the firm's total external obligations are not too convex, i.e.,

$$\frac{\left(\varphi_{\bar{R}+1} - \varphi_{\bar{R}}\right)}{\left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right)} < \frac{\left(1-H_{\bar{R}-1}\right) h_{\bar{R}}}{\left(1-H_{\bar{R}}\right) h_{\bar{R}-1}},$$

where the right-hand side of this inequality is larger than 1 because of the increasing Hazard function.

Finally, it is immediate that when $\bar{R} = 0$, the firm is never audited, and no revenues are raised, and for the problem to be interesting, it must be the case that the marginal benefit of auditing is positive at least for $\bar{R} = 1$ should the firm pledge all its revenues from one sale to external parties, i.e., when $\varphi_1 = 1$, which holds as $\Phi(1) - \Phi(0)|_{\varphi_1=1} = h_0 \left(\frac{1}{h_0} - \frac{c}{1+\delta}\right) = (1-\bar{z})^N \left(\frac{\varphi_1}{(1-\bar{z})^N} - \frac{c}{1+\delta}\right) > 0$ as long as $c < \frac{(1+\delta)}{(1-\bar{z})^N}$ and the main setting assumes that $c < \frac{1}{(1-\bar{z})^N}$. $\square$

Corollary O.4.1.1. *The optimal auditing threshold, $\bar{R}$, is weakly decreasing in auditing cost c, and weakly increasing in $\varphi_{\bar{R}} - \varphi_{\bar{R}-1}$.*

Proof. The optimal threshold is given by (12). The proof of Lemma O.4.1 demonstrated that $\left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right) \frac{1-H_{\bar{R}-1}}{h_{\bar{R}-1}}$ is decreasing in $\bar{R}$ under the assumed constraint. It then follows that $\left(\varphi_{\bar{R}} - \varphi_{\bar{R}-1}\right) \frac{1-H_{\bar{R}-1}}{h_{\bar{R}-1}} - \frac{c}{1+\delta}$ is decreasing c and in $\bar{R}$, which implies that the optimal threshold, $\bar{R}^*$, is weakly decreasing in c. It is weakly decreasing only because $\bar{R}^*$ must be an integer, and small changes in c may not affect the optimal threshold. From inequality (4) in Section O.2.2, it also holds that $\frac{\left(1-H_{\bar{R}-1}\right)}{h_{\bar{R}-1}}$ is decreasing in $\bar{R}$, and thus any fixed $\varphi_{\bar{R}} - \varphi_{\bar{R}-1}$ weakly increases $\bar{R}^*$.[5] $\square$

[5] Note that under proportional taxes and linear financing contracts, $\varphi_{\bar{R}} - \varphi_{\bar{R}-1}$ is a constant.

Proposition O.4.2. *There exist two key thresholds, $\bar{R}_m^*$ which determines whether external financing is possible, and $\bar{R}_\tau^*$ which establishes the minimal threshold for tax purposes only, i.e.,*

$$\bar{R}_m^* = \max\left\{\bar{R} \in \mathbb{Z}^+ | \frac{1 - H_{\bar{R}-1}}{h_{\bar{R}-1}} - \frac{c}{1+\delta} \geq 0\right\}. \tag{14}$$

$$\bar{R}_\tau^* = \max\left\{\bar{R} \in \mathbb{Z}^+ | \left(\tau_{\bar{R}} - \tau_{\bar{R}-1}\right) \frac{1 - H_{\bar{R}-1}}{h_{\bar{R}-1}} - \frac{c}{1+\delta} \geq 0\right\}. \tag{15}$$

It holds that $\bar{R}_m^* \geq \bar{R}^* \geq \bar{R}_\tau^*$.

Proof. The threshold for $\bar{R}_m^*$ is defined under the premise that the most the firm can credibly pledge is all its after-tax revenues, i.e., offer a financing contract that sets $\varphi_R = R = S$ for any $R \leq \bar{R}_m^*$ and thus $\varphi_{\bar{R}+1} - \varphi_{\bar{R}} = 1$. The optimal auditing threshold for tax purposes considers no payments to investors. The rank order follows from Corollary O.4.1.1 as $\tau_{\bar{R}} - \tau_{\bar{R}-1} \leq \varphi_{\bar{R}+1} - \varphi_{\bar{R}} \leq 1$ under any increasing tax policy and financial contracts that are weakly increasing is revenues. $\square$

O.4.2 Optimal financing contracts

Given the optimal auditing and reporting policies (10) and (11), the firm's financing contract problem can be restated as choosing the function $\phi(.)$ to maximize

$$\mathbb{E}[S] - \Pr\left(S < \bar{R}^*\right) \mathbb{E}\left[\tau_S + \phi\left(S - \tau_S\right) | S < \bar{R}^*\right] - \Pr\left(S \geq \bar{R}^*\right) \mathbb{E}\left[\tau_{\bar{R}^*} + \phi\left(\bar{R}^* - \tau_{\bar{R}^*}\right) | S \geq \bar{R}^*\right],$$

subject to the auditing threshold, (12), and the financiers' break-even constraint

$$\begin{aligned}&\Pr\left(S < \bar{R}^*\right) \mathbb{E}\left[\phi\left(S - \tau_S\right) | S < \bar{R}^*\right] + \Pr\left(S \geq \bar{R}^*\right) \mathbb{E}\left[\phi\left(\bar{R}^* - \tau_{\bar{R}^*}\right) | S \geq \bar{R}^*\right] \geq \\ &I + \Pr\left(S < \bar{R}^*\right) \frac{c}{1+\delta}\end{aligned} \tag{16}$$

It is clearly optimal for the firm to offer a financing contract that sets the financiers' breakeven constraint to hold with equality. Using this, we can rewrite the firm's objective function as

$$\pi \equiv \mathbb{E}[S] - I - \Pr\left(S < \bar{R}^*\right) \frac{c}{1+\delta} - \Pr\left(S < \bar{R}^*\right) \mathbb{E}\left[\tau_S | S < \bar{R}^*\right] - \Pr\left(S \geq \bar{R}^*\right) \tau_{\bar{R}^*}, \tag{17}$$

which implies that the financing contract the firm offers to investors only affects its payoff if it affects the optimal auditing threshold, $\bar{R}^*$. And if so, the firm benefits from offering a contract that sets $\bar{R}^*$ to be as low as possible to minimize the auditing costs and tax payments.[6]

[6]Notice that $\Pr\left(S < \bar{R}^*\right) \mathbb{E}\left[\tau_S | S < \bar{R}^*\right] + \Pr\left(S \geq \bar{R}^*\right) \tau_{\bar{R}^*} = \Pr\left(S < \bar{R}^*\right) \mathbb{E}\left[\tau_S - \tau_{\bar{R}^*} | S < \bar{R}^*\right] + \tau_{\bar{R}^*} =$

Given that some auditing is already optimal for tax purposes only, it follows that whenever $\bar{R}^* = \bar{R}^*_\tau$ defined in (15), there are many contracts that are payoff equivalent. In particular, when the auditing cost is small, all financing contracts that satisfy the financiers' breakeven constraint (16) are equivalent.

Lemma O.4.3. *There exists a threshold for the auditing cost*

$$c \leq c_{min} = (1+\delta)\left(\tau_N - \tau_{N-1}\right) \frac{\bar{z}}{N\left(1-\bar{z}\right)}, \tag{18}$$

such that $\bar{R}^* = \bar{R}^*_\tau = N$. In such case, the expected tax payment is $\mathbb{E}\left[\tau_S\right]$ and the firm's payoff is $\pi_{c \leq c_{min}} = N\bar{z} - I - \left(1-\bar{z}^N\right)\frac{c}{1+\delta} - \mathbb{E}\left[\tau_S\right]$.

Proof. Using (15) we can find that c_{min} by setting $\left(\tau_N - \tau_{N-1}\right)\frac{1-H_{N-1}}{h_{N-1}} - \frac{c_{min}}{1+\delta} = 0$. It is clear that if (15) holds for c_{min}, it also holds for any $c < c_{min}$. Using the functional form of the binomial distribution we find that $\frac{1-H_{N-1}}{h_{N-1}} = \frac{h_N}{h_{N-1}} = \frac{\bar{z}^N}{N\bar{z}^{N-1}(1-\bar{z})} = \frac{\bar{z}}{N(1-\bar{z})}$. Furthermore, by Proposition O.4.2 $\bar{R}^* \geq \bar{R}^*_\tau$under any financing contract, and thus $\bar{R}^* = \bar{R}^*_\tau = N$ as well. It then follows that the expected tax payment is $\Pr\left(S<N\right)\mathbb{E}\left[\tau_S|S<N\right] + \Pr\left(S \geq N\right)\tau_N = \mathbb{E}\left[\tau_S\right]$. The firm' s expected profit is $\pi_{c \leq c_{min}} = N\bar{z} - I - \Pr\left(S<N\right)\frac{c}{1+\delta} - \mathbb{E}\left[\tau_S\right]$ and $\Pr\left(S<N\right) = 1 - \Pr\left(S=N\right) = 1 - h_N = 1-\bar{z}^N$, where the latter equation uses the functional form of the Binomial distribution. □

Lemma O.4.3 shows that when auditing costs are low, auditing all reports except the highest one is optimal already for tax purposes and the specific form of the financing contract does not affect the firm's profit. While optimal financing contracts in this case can take many shapes, the one in the simplest form is an equity contract

$$\phi\left(S - \tau_S\right) = \bar{\phi}_E \cdot \left(S - \tau_S\right),$$

where ϕ_E is a constant that sets the investors' breakeven constraint (16) to hold with equality, i.e.,

$$\bar{\phi}_E = \frac{I + \left(1-\bar{z}^N\right)\frac{c}{1+\delta}}{N\bar{z} - \mathbb{E}\left[\tau_S\right]}.$$

The highest investment cost that can be covered in this case is $I^m_{c \leq c_{min}} = N\bar{z} - \mathbb{E}\left[\tau_S\right] - \left(1-\bar{z}^N\right)\frac{c}{1+\delta}$, which corresponds to the firm pledging all its after-tax sales to the financiers.

$\sum_{S=0}^{\bar{R}^*-1}\left(\tau_S - \tau_{\bar{R}^*}\right)h_S + \tau_{\bar{R}^*}$. Therefore, the increase of the threshold by one unit from $\bar{R}^*$ to $\bar{R}^*+1$ corresponds to $\sum_{S=0}^{\bar{R}^*}\left(\tau_S - \tau_{\bar{R}^*}\right)h_S + \tau_{\bar{R}^*+1} - \sum_{S=0}^{\bar{R}^*-1}\left(\tau_S - \tau_{\bar{R}^*}\right)h_S - \tau_{\bar{R}^*} = \tau_{\bar{R}^*+1} - \tau_{\bar{R}^*} > 0$, because taxes are assumed to be increasing in sales.

Let us then consider that $c > c_{min}$ such that it is suboptimal to audit all reports for tax purposes only. Whether or not the functional form of the financing contract matters for the firm's payoff depends on the investment cost. Namely, if the investment cost is small, then it may still be the case that $\bar{R}^* = \bar{R}^*_\tau$. However, when the investment cost is higher, it is in the interest of the firm to offer a contract that keeps the optimal auditing threshold as low as possible. Finally, there exists a maximal investment cost that can be covered, which corresponds to the firm pledging all its after-sale revenues to the financiers. The following Proposition summarizes this and defines the threshold investment costs.

Proposition O.4.4. *Assume that $c > c_{min}$. The following holds for different investment costs*
1) If the investment cost $I \leq I_\tau$, where

$$I_\tau \equiv \Pr\left(S < \bar{R}^*_\tau\right) \mathbb{E}\left[S - \tau_S - \frac{c}{1+\delta} | S < \bar{R}^*_\tau\right] + \Pr\left(S \geq \bar{R}^*_\tau\right) \mathbb{E}\left[\bar{R}^*_\tau - \tau_{\bar{R}^*_\tau} | S \geq \bar{R}^*_\tau\right],$$

then the firm can raise external financing and it is optimal to offer any contract that keeps the auditing threshold $\bar{R}^* = \bar{R}^*_\tau$ defined in (15). If $I = I_\tau$, then the optimal financing contract is a debt contract with face value $\bar{R}^*_\tau$ and the financiers have a claim to all after-tax sales revenues when $S < \bar{R}^*_\tau$. If $I < I_\tau$ then there are multiple financing contracts that give the same profit to the firm and these contracts still have the feature that all pledges for cash flows $S > \bar{R}^*_\tau$ are constant.
2) If the investment cost $I > I_m$, where

$$I_m \equiv \Pr\left(S < \bar{R}^*_m\right) \mathbb{E}\left[S - \tau_S - \frac{c}{1+\delta} | S < \bar{R}^*_m\right] + \Pr\left(S \geq \bar{R}^*_m\right) \mathbb{E}\left[\bar{R}^*_\tau - \tau_{\bar{R}^*_m} | S \geq \bar{R}^*_m\right],$$

and where $\bar{R}^*_m$ is defined in (15) then the firm cannot raise external financing.
3) If the investment cost $I_\tau < I \leq I_m$, then the firm can raise external financing and it is optimal for it to offer a debt (or debt-like) contract where the firm pledges all its after-takes sales revenues to the financiers up to the threshold $\bar{R}^*$ that solves the optimal auditing problem under this contract.

Proof. For Part 1 consider the financiers' breakeven constraint (16) under the threshold $\bar{R}^*_\tau$. Because it is optimal for the firm to keep the threshold as low as possible, it is in the best interest of the firm to offer a financing contract that maintains the threshold at $\bar{R}^*_\tau$ and it can achieve this as long as pledging all its after-tax revenues to investors satisfies (16). This determines the threshold, I_τ, as the one that corresponds to $\Pr\left(S < \bar{R}^*_\tau\right) \mathbb{E}\left[S - \tau_S | S < \bar{R}^*_\tau\right] + \Pr\left(S \geq \bar{R}^*_\tau\right) \mathbb{E}\left[\bar{R}^*_\tau - \tau_{\bar{R}^*_\tau} | S \geq \bar{R}^*_\tau\right] = I_\tau + \Pr\left(S < \bar{R}^*_\tau\right) \frac{c}{1+\delta}$. If the investment cost is lower, then the breakeven constraint remains satisfied, while the auditing threshold remains at $\bar{R}^*_\tau$. Consequently, there are multiple financing contracts that give the same payoff to the firm. These contracts must still have the feature that the firm cannot credibly commit to make different payments if its sales exceed the optimal auditing threshold.

Part 2 follows from the fact that under limited liability the firm can at most pledge all its audited after-sales revenues to the financiers, and because it is too costly to audit the highest revenues, there is an upper limit on the investment cost that can satisfy the investors break-even constraint (16) given by $\Pr\left(S < \bar{R}_m^*\right) \mathbb{E}\left[S - \tau_S | S < \bar{R}_m^*\right] + \Pr\left(S \geq \bar{R}_m^*\right) \mathbb{E}\left[\bar{R}_m^* - \tau_{\bar{R}_m^*} | S \geq \bar{R}_m^*\right] = I_m + \Pr\left(S < \bar{R}_m^*\right) \frac{c}{1+\delta}$.

For Part 3 notice that these investment costs can be covered as the financiers' breakeven constraint can be satisfied at least when the firm pledges all its after-tax revenues to financiers until the threshold $\bar{R}^*$. This is because it is in the best interest of the firm to keep the auditing threshold as low as possible, it is is best achieved by offering a debt-like contract where the firm commits as much as its lower sales revenues to the financiers. To see this, note that unless the threshold does not change due to sales distribution being discrete, offering more funds to financiers must increase the total funds raised at any fixed threshold $\bar{R}$, i.e., it must be the case that $\Phi\left(\bar{R}; \phi_H(.)\right) > \Phi\left(\bar{R}; \phi_L(.)\right)$ for some contracts $\phi_H(.)$ and $\phi_L(.)$ where the contract ϕ_H offers greater payments to financiers. Suppose that the corresponding optimal auditing thresholds are $\bar{R}_H^*$ and $\bar{R}_L^*$ and consider that the total funds raised under these contracts are the same, $\Phi\left(\bar{R}_H^*; \phi_H(.)\right) = \Phi\left(\bar{R}_L^*; \phi_L(.)\right) \iff \Phi\left(\bar{R}_H^*; \phi_H(.)\right) - \Phi\left(\bar{R}_H^*; \phi_L(.)\right) = \Phi\left(\bar{R}_L^*; \phi_L(.)\right) - \Phi\left(\bar{R}_H^*; \phi_L(.)\right)$. Because the left-hand side of the last equality is positive, the right-hand side must be positive as well. As Appendix O.4.1 proved that the change in funds raised is proportional to a decreasing function (i.e., $\Lambda\left(\bar{R}\right) < 0$), it follows that $\bar{R}_L^* > \bar{R}_H^*$.

Therefore, to minimize the optimal auditing threshold (12), it is best for the firm to have $\varphi_S = \tau_S + \phi(S - \tau_S) = S$ for all $S < \bar{R}^*$, and the firm offers a debt contract

$$\phi(S - \tau_S) = \begin{cases} S - \tau_S \text{ if } S < \bar{R}^* \\ \bar{\phi}_D\left(\bar{R}^* - \tau_{\bar{R}^*}\right) \text{ if } S = \bar{R}^* \\ \bar{R}^* - \tau_{\bar{R}^*} \text{ if } S > \bar{R}^* \end{cases},$$

where $\bar{\phi}_D \in (0,1]$ is a constant that guarantees that the financiers' breakeven constraint holds with equality and is there because the sales distribution is discrete. The pair $\left(\bar{R}^*, \bar{\phi}_D\right)$ solves a system of equations, where $\bar{\phi}_D$ is set such that $\bar{R}^*$ is an integer and where for any tax system it holds that

$$\begin{cases} \left(1 - \left(1 - \bar{\phi}_D\right)\left(\bar{R}^* - \tau_{\bar{R}^*}\right)\right) \frac{1 - H_{\bar{R}^*-1}}{h_{\bar{R}^*-1}} - \frac{c}{1+\delta} = 0 \\ \bar{\phi}_D = \frac{I + H_{\bar{R}^*-1} \frac{c}{1+\pi} + \sum_{S=0}^{\bar{R}^*} (S - \tau_S) h_S}{h_{\bar{R}^*}\left(\bar{R}^* - \tau_{\bar{R}^*}\right)} \end{cases}. \tag{19}$$

It is straightforward to verify that the above contract is incentive compatible and consistent with the optimal reporting policy (11). While there exist other contracts that are payoff equivalent, these exist just because the payoffs are discrete in this setting. For example, instead of the above contract, the firm could offer

$$\phi\left(S-\tau_S\right)=\begin{cases}\bar{\phi}'_D\left(S-\tau_S\right) \text{ if } S\leq\bar{R}^* \\ \bar{R}^*-\tau_{\bar{R}^*} \text{ if } S>\bar{R}^*\end{cases},$$

where $0<\bar{\phi}'_D<1$ is a different constant than $\bar{\phi}_D$ and leads to the same payoffs as long as it implies the same $\bar{R}^*$. □

We can derive the firm's profit under the optimal financing contract using (17) and insights from Proposition O.4.4 as

$$\begin{aligned}\pi &= \mathbb{E}\left[S\right]-I-\Pr\left(S<\bar{R}^*\right)\frac{c}{1+\delta}-\mathbf{E}_\tau\left(\bar{R}^*\right), \text{ where} \\ \mathbf{E}_\tau\left(\bar{R}^*\right) &\equiv \Pr\left(S<\bar{R}^*\right)\mathbb{E}\left[\tau_S|S<\bar{R}^*\right]+\Pr\left(S\geq\bar{R}^*\right)\tau_{\bar{R}^*}\end{aligned} \tag{20}$$

and $\bar{R}^*=\bar{R}^*_\tau$ if $I\leq I_\tau$, and $\bar{R}^*$ solves (12) under the debt contract that sets financiers' breakeven constraint to hold with equality.

Finally, we using the law of total expectations, we can rewrite the maximum investment cost that can be covered as

$$I_m=N\bar{z}-\mathbf{E}_\tau\left(\bar{R}^*_m\right)-H_{\bar{R}^*_m-1}\frac{c}{1+\delta}.$$