Electronic Companion

Bilateral Liability-Based Contracts in Information Security Outsourcing

Appendix A: Proof of Propositions

Proof of Lemma 1

We solve the two-stage profit maximization problem using backward induction. At the second stage, the client and the MSS provider will decide efforts simultaneously based on the first-order conditions (9) and (10). Note that these conditions only depend on the compensation rate β but not the contract price p We denote $q_k = q_k^*(\beta)$ and $q_s = q_s^*(\beta)$ as the joint solution of equations (9) and (10). Going back to the first stage, the MSS provider's profit maximization problem could be written as

$$\begin{aligned} &\max_{p,\beta} p - \mathcal{B}(a, q_k, q_s)\beta v - \mathcal{C}_s(q_s) \\ &\text{s.t. } u_1 \geq U_0^*, q_k = q_k^*(\beta), q_s = q_s^*(\beta) \end{aligned} \tag{A1}$$

The first set of constraints is to ensure the clients will receive at least the reservation utility, so that they are willing to outsource. We rewrite this constraint with a slack variable $y \geq 0$ to be $u_1 = U_0^* + y$, which could also be written as $p = [1 - \mathcal{B}(a, q_k, q_s)(1 - \beta)]v - \mathcal{C}_k(q_k) - U_0^* - y$. By substituting the price with this constraint, the maximization problem could be rewritten as

$$\begin{aligned} &\max_{y,\beta} w - U_0^* + y \\ &\text{s.t. } y \geq 0, , q_k = q_k^*(\beta), q_s = q_s^*(\beta) \end{aligned} \tag{A2}$$

Obviously, the profit is maximized with $y = 0$, meaning the MSS provider extracts all surplus from the client. Hence, the objective of profit maximization is equivalent to welfare maximization, but rather than directly choosing the efforts, the MSS provider can only choose a compensation rate to influence the efforts. Note that this result holds even if we introduce interdependent risk into the model, and the proof is similar and omitted here. ■

Proof of Proposition 1

We proof this proposition by contradiction. Suppose the first best welfare is achievable with a loss-based liability contract, which means $q_k^* = Q_k^*$ and $q_s^* = Q_s^*$ for some constant β^*. If q_k^* is interior, it should satisfy the first-order condition of utility stated in (9), and Q_k^* should satisfy the first-order condition of welfare with respect to the client's effort stated in (2). Solving (2) and (9) together at $q_k^* = Q_k^*$ gives

$$\beta v \frac{\partial \mathcal{B}}{\partial q_k}\Big|_{Q_k^*} = 0. \tag{A3}$$

Similarly, if q_s^* is interior, it should satisfy the first-order condition of profit stated in (10), and Q_s^* should satisfy the first-order condition of welfare with respect to the MSSP's effort stated in (3). Solving (3) and (10) together at $q_s^* = Q_s^*$ gives

$$(1-\beta) v \frac{\partial \mathcal{B}}{\partial q_s}\Big|_{Q_s^*} = 0. \tag{A4}$$

(A3) and (A4) is solvable only when $\frac{\partial \mathcal{B}}{\partial q_k}\Big|_{Q_k^*} = 0$ or $\frac{\partial \mathcal{B}}{\partial q_s}\Big|_{Q_s^*} = 0$. When $\frac{\partial \mathcal{B}}{\partial q_k}\Big|_{Q_k^*} = 0$, for interior Q_k^*, we have $\frac{\partial \mathcal{C}_k}{\partial q_k}\Big|_{Q_k^*} = 0$ from equation (2), which violates the assumption of increasing cost, $\partial \mathcal{C}_k / \partial q_k > 0$. Similarly, when $\frac{\partial \mathcal{B}}{\partial q_s}\Big|_{Q_s^*} = 0$, for interior Q_s^*, we have $\frac{\partial \mathcal{C}_k}{\partial q_s}\Big|_{Q_s^*} = 0$ from equation (3), which also violates the assumption of increasing cost, $\partial \mathcal{C}_s / \partial q_s > 0$. Therefore, the first best welfare is not achievable with a loss-based liability contract when first best efforts are interior, i.e. $Q_k^* > 0$ and $Q_s^* > 0$. ■

Proof of Proposition 2

From the main text, a variable liability contract with $\beta = \mathcal{B}(a, Q_k^*, Q_s^*) / \mathcal{B}(a, q_k, Q_s^*)$ satisfies the sufficient conditions for inducing socially optimal effort stated in (11) and (12) at $(q_k, q_s) = (Q_k^*, Q_s^*)$.

Note that the second order condition for the client $\partial^2 u_1/\partial q_k^2 = -v\partial^2 \mathcal{B}/\partial q_k^2 - \partial^2 \mathcal{C}_k/\partial q_k^2 < 0$ and for the MSS provider $\partial^2 \pi/\partial q_s^2 = -\beta v\partial^2 \mathcal{B}/\partial q_s^2 - \partial^2 \mathcal{C}_s/\partial q_s^2 < 0$ are satisfied. From Lemma 1, it is straightforward to see that the MSS provider will adopt this welfare-maximizing contract to maximize its profit, meaning the first best social welfare will be achieved with this contract. ■

Proof of Proposition 3

From the main text, a threshold-based liability contract with $\beta = \mathbf{1}_{q_k \geq Q_k^*}$ only satisfies the MSS provider's sufficient condition for inducing socially optimal effort stated in (12) at $(q_k, q_s) = (Q_k^*, Q_s^*)$. However, we shall see that the client will also choose $q_k = Q_k^*$ in this situation. Suppose the client's effort deviates from Q_k^*, if $q_k < Q_k^*$, the MSSP will response with zero effort because the compensation rate becomes zero. If $q_k > Q_k^*$, since the expected loss from system breach is fully covered by the MSSP, the client's utility $u_1 = v - \mathcal{C}_k(q_k) - p$ will only be lower. Therefore, the client's effort will not deviate from Q_k^*, and from Lemma 1, the MSS provider will use this welfare-maximizing contract to maximize its profit. Hence, a threshold-based liability contract with conditional compensation is socially optimal. ■

Proof of Proposition 4

As the proof for loss-based liability and threshold-based liability is similar to the baseline scenario, we focus our discussion on variable liability contract. For a variable liability contract with the form of optimal-to-actual breach ratio as compensation rate, i.e. $\beta_j = \mathcal{B}(a, Q_{ke}^*, Q_{se}^*)/\mathcal{B}\big(a, q_{kj}, Q_{se}^*\big)$, the MSSP's sufficient condition for inducing socially optimal effort stated in (31) is satisfied at $\big(q_{kj}, q_{sj}\big) = (Q_{ke}^*, Q_{se}^*)$. On the other hand, the client's condition stated in (30) becomes

$$\frac{\beta_j \mathcal{L}_j}{\mathcal{B}\big(a, q_{kj}, Q_{se}^*\big)} \frac{\partial \mathcal{B}\big(a, q_{kj}, Q_{se}^*\big)}{\partial q_{kj}} = \big[\beta_j + e(m-1)\big] \frac{\partial \mathcal{B}\big(a, q_{kj}, q_{sj}\big)}{\partial q_{kj}}, \qquad \text{(A5)}$$

which can be simplified to $\sum_{i=1,i\neq j}^{m}\mathcal{B}(a,q_{ki},q_{si})=(m-1)\mathcal{B}(a,Q_{ke}^{*},Q_{se}^{*})$ when $\left(q_{kj},q_{sj}\right)=(Q_{ke}^{*},Q_{se}^{*})$. This means if the protection efforts on other clients' systems are also socially optimal, the condition will be satisfied. However, the client may have incentive to over-protect the system if all other parties exert the socially optimal efforts. In particular, when $q_{ki}=Q_{ke}^{*}\ \forall i\neq j$ and $q_{si}=Q_{se}^{*}\ \forall i$, the second order derivative of the client's utility with respect to q_{kj} is

$$\frac{\partial^2 u_1}{\partial q_{kj}^2}=-\left[1+e(m-1)\beta_j^2\right]v\frac{\partial^2\mathcal{B}}{\partial q_{kj}^2}-\frac{\partial^2\mathcal{C}_k}{\partial q_{kj}^2}+\frac{e(m-1)\beta_j^2 v}{\mathcal{B}\left(a,q_{kj},Q_{se}^{*}\right)}\left[\frac{\partial\mathcal{B}}{\partial q_{kj}}\right]^2, \qquad \text{(A6)}$$

where $\partial\mathcal{B}/\partial q_{kj}$ and $\partial^2\mathcal{B}/\partial q_{kj}^2$ are evaluated at $q_{sj}=Q_{se}^{*}$. Note that the last term is positive, meaning that the function may change in concavity and the first-best effort could be a local maximum rather than a global one. In an extreme situation where $\mathcal{B}\left(a,q_{kj},Q_{se}^{*}\right)=0$ for some $q_{kj}>Q_{ke}^{*}$, the compensation will go to infinity and could be obtained from the loss due to the interdependent risk. Figure A1(a) shows an example of the client *j*'s utility curve with this issue from the serial configuration scenario, which could be solved by imposing a 100% limit liability, and the resulting utility curve is shown in Figure A1(b). Note that the local maximum issue may not exist for some parameter settings, for example in total effort security shown in Figure A1(c) and A1(d).

Hence, given $\beta_j=\min\left\{\mathcal{B}(a,Q_{ke}^{*},Q_{se}^{*})/\mathcal{B}\left(a,q_{kj},Q_{se}^{*}\right),1\right\}$, the client will also exert $q_{kj}=Q_{ke}^{*}$, because the client's utility will become $u_1=v-\mathcal{C}_k\left(q_{kj}\right)-p_j$ for $q_{kj}\geq Q_{ke}^{*}$, which is decreasing in q_{kj} and so the client will not over-protect. As a result, a variable liability contract with the compensation rate equal to the optimal-to-actual breach probability ratio capped at 100% is socially optimal. ■

Remarkably, the optimal variable liability function could also be directly obtained from solving the differential equations from conditions (30) and (31). The solution of (30) is $\beta_j=\tilde{\beta}_j/\mathcal{L}_j-e(m-1)$, where $\tilde{\beta}_j$ is a constant, and condition (31) implies $\beta_j=1$. These two conditions suggest the MSS provider should choose $\tilde{\beta}_j$ that satisfies $\tilde{\beta}_j/\mathcal{L}_j-e(m-1)=1$, which is simply $\tilde{\beta}_j=[1+e(m-1)]\mathcal{L}_j$.

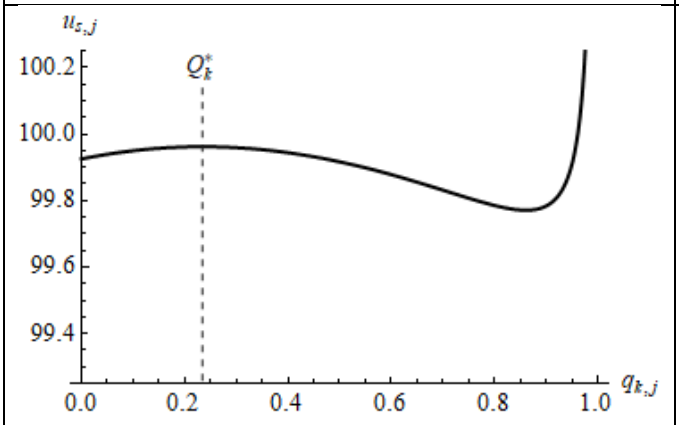
When every party exerts the first best effort, $\mathcal{L}_j = [1 + e(m-1)]\mathcal{B}(a, Q^*_{ke}, Q^*_{se})$. Hence, the socially optimal variable liability function based on the solution of (30) and (31) is

$$\beta_j = \frac{[1 + e(m-1)]^2 \mathcal{B}(a, Q^*_{ke}, Q^*_{se})}{\mathcal{B}\left(a, q_{kj}, Q^*_{se}\right) + e(m-1)\mathcal{B}(a, Q^*_{ke}, Q^*_{se})} - e(m-1). \qquad \text{(A7)}$$

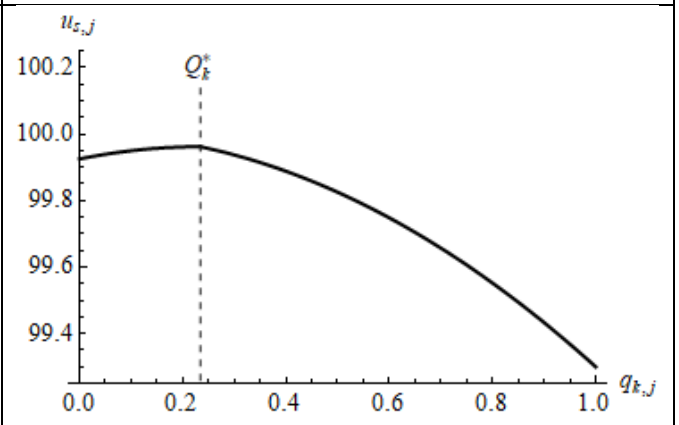
Figure A1: Utility from Optimal-to-actual Breach Variable Liability with Interdependent Risk

Parameters: $m = 101, a = 0.01, v = 100, \mathcal{B} = a\left(1 - q_{kj}\right)\left(1 - q_{sj}\right), \mathcal{C}_k = 0.7q^2_{kj},\ \mathcal{C}_s = 0.6q^2_{sj}, p_j = 0.$

(a) Unlimited liability (serial configuration)

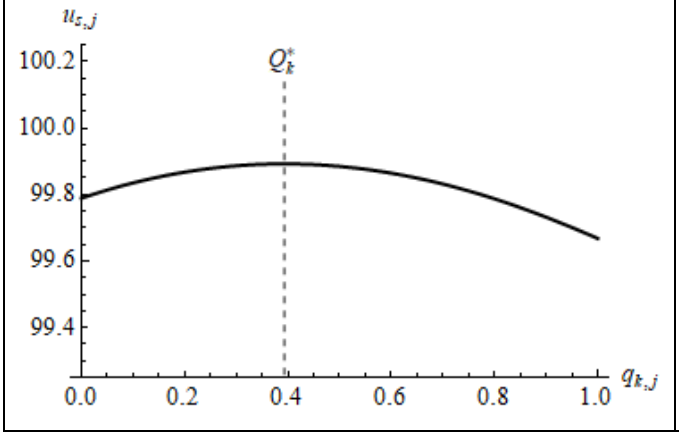


(b) Limited liability (serial configuration)

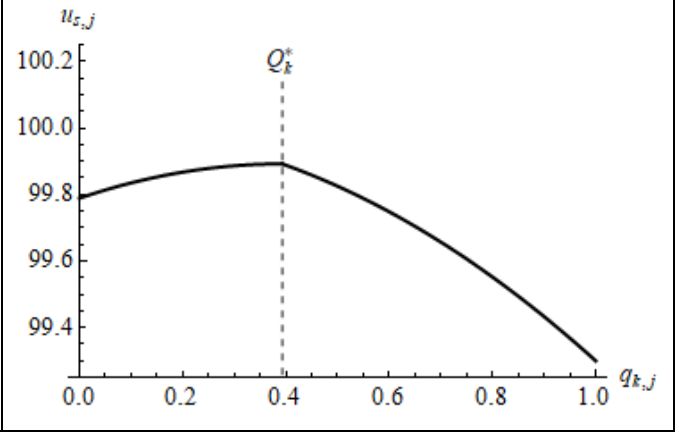


Parameters: $m = 101, a = 0.01, v = 100, \mathcal{B} = a\left(1 - 0.5q_{kj} - 0.5q_{sj}\right), \mathcal{C}_k = 0.7q^2_{kj},\ \mathcal{C}_s = 0.6q^2_{sj}, p_j = 0.$

(c) Unlimited liability (total effort)



(d) Limited liability (total effort)



Appendix B: Additional Notes on Limited Liability

In loss-based liability, suppose β^* is the optimal compensation rate without limited liability, the MSS provider will simply choose $\beta = \min\{\beta^*, \gamma\}$ to maximize the welfare because of the quasi-concavity. The first-order conditions for the client and the MSS provider remain the same as in (9) and (10). Therefore, the liability upper bound introduces further distortion on loss-based liability only when $\gamma < \beta^*$, meaning the MSS provider can only choose the liability upper bound instead of the optimal rate as the actual compensation rate.

In variable liability, the compensation rate function could be written as $\beta = \min\{\tilde{\beta}/\mathcal{B}(a, q_k, S), \gamma\}$, where $\tilde{\beta}$ and S are constants decided by the MSSP. To encourage the client to exert Q_k^{sb}, the compensation rate should reach the maximum, i.e. $\beta = \gamma$, when the effort is at the desirable level Q_k^{sb}. However, the client may have incentive to over-protect, which is similar to the case in threshold-based liability, and the incentive compatibility constraint for regulating over-protection is the same as (38). Yet, unlike threshold-based liability, the client may also have incentive to under-protect because the MSS provider will still provide effort and compensation. The incentive compatibility constraint for regulating under-protection is

$$\left.\frac{\partial u_1}{\partial q_k}\right|_{q_k = Q_k^{sb-}} = (1-\gamma)\frac{\partial q_s}{\partial q_k}\frac{\partial \mathcal{B}}{\partial q_s}v + \gamma\frac{\partial \mathcal{B}}{\partial q_k}v + \mathcal{B}\frac{\partial \beta}{\partial q_k}v \geq 0, \tag{A8}$$

which means further decrease effort from Q_k^{sb} will decrease the utility. This condition is similar to (38) except an additional term $\mathcal{B}\partial\beta/\partial q_k$ is included, and the condition requires to be positive instead of negative. This implies $\mathcal{B}\partial\beta/\partial q_k$ has to be sufficiently large to deter the client from under-protection. Remarkably, this condition in threshold-based liability is always positive because $\partial\beta/\partial q_{k,j} = +\infty$ at $q_k = Q_k^{sb-}$ due to the property of stepwise function. Therefore, the granularity of variable liability may hurt the welfare in limited liability as it potentially gives incentive for the client to underwork.

Note that the explicit form of $\partial q_s/\partial q_k$ could be obtained by applying implicit function theorem on the MSS provider's best response constraint stated in (37):

$$\frac{\partial q_s}{\partial q_k} = -\gamma \frac{\partial^2 \mathcal{B}}{\partial q_k q_s} v \Big/ \left(\gamma \frac{\partial^2 \mathcal{B}}{\partial q_s^2} v + \frac{\partial^2 \mathcal{C}_s}{\partial q_s^2} \right), \tag{A9}$$

and the sign will be solely determined by the cross partial derivative of the breach function.

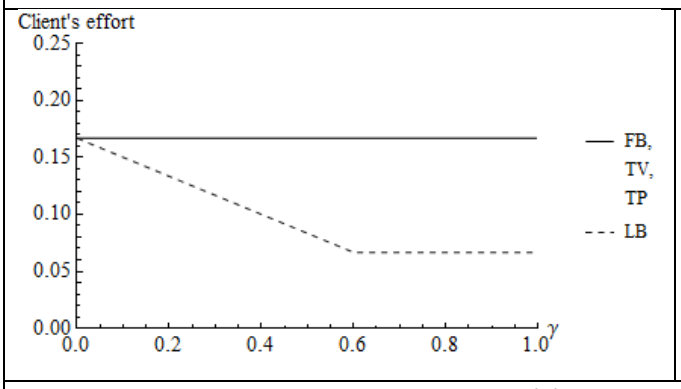
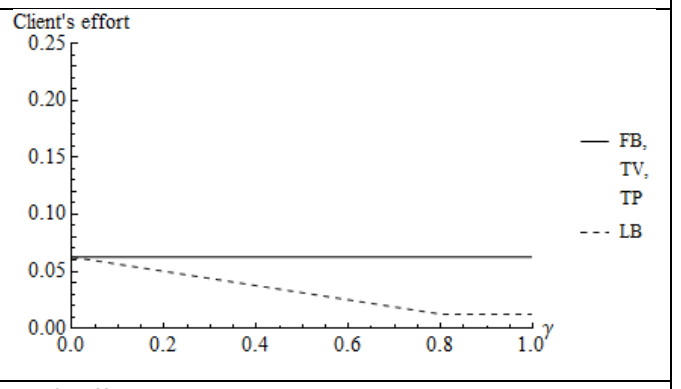
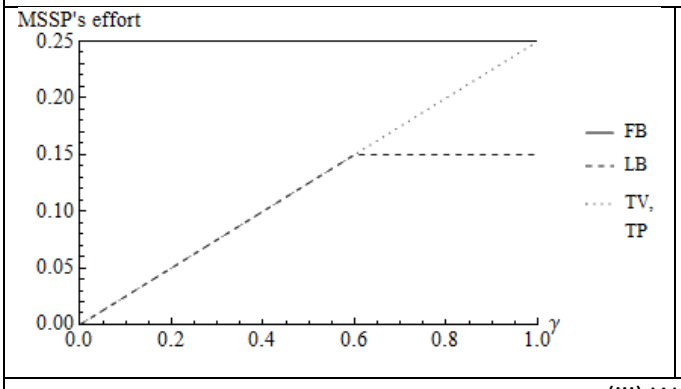
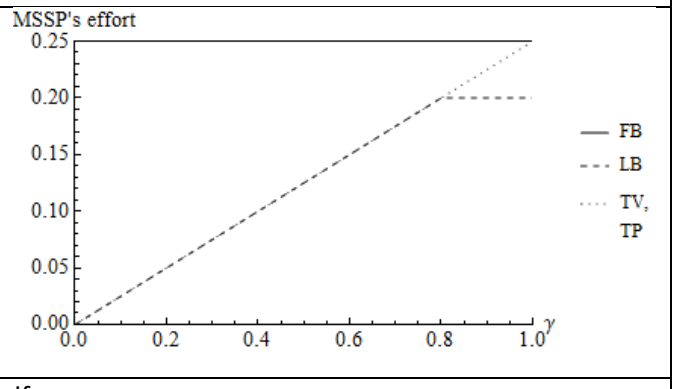
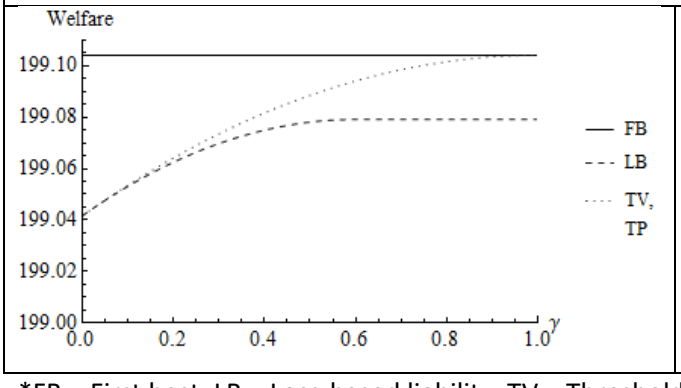
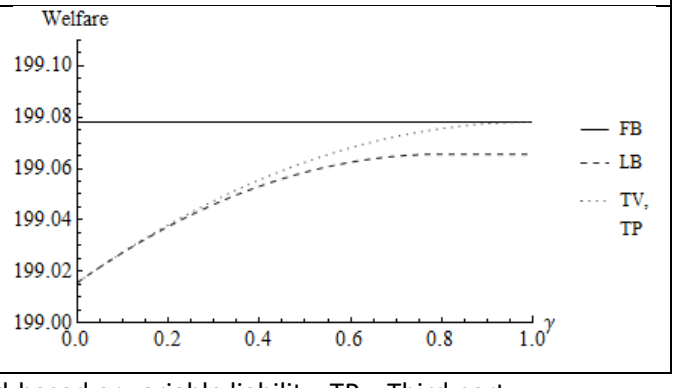
We now apply the three security scenarios into the limited liability model. For total effort security, condition (38) becomes $-\gamma \lambda_k a v \leq 0$, and (A8) is simply zero when $\beta = \min\{\gamma(1-\lambda_k Q_k^{sb} - \lambda_s Q_s^{sb})/(1-\lambda_k q_k - \lambda_s Q_s^{sb}), \gamma\}$, meaning the MSS provider can use threshold-based and variable liability contracts to ensure second-best effort from the client. For illustration, we compare the contracts numerically, and the result is shown in Figure B1. The client's effort is actually first best in threshold-based liability, variable liability and third-party contract even with limited liability, because the limited liability constraint only affects the MSS provider's effort and it will not further affect the client's effort as efforts are independent in total effort security. However, client will underwork with loss-based liability when the compensation rate is positive. On the other hand, the MSS provider will underwork for all contracts with limited liability, and this situation is most severe for loss-based liability whereas the effort is the same for the other three contracts. Interestingly, when the liability upper bound is lower than the optimal compensation rate in loss-based liability, the MSS provider will exert the same effort in all types of contract. The welfare of loss-based liability is always lower than that in the other three contracts, and become stable for $\gamma \geq \beta^*$.

Next, we apply the limited liability model into serial configuration. The incentive compatibility conditions are are all satisfied since (38) becomes $-\gamma a v\left[1 - av\left(1 - Q_k^{sb}\right)/c_s\right] \leq 0$, and (A8) becomes $\gamma(1-\gamma)\left(1 - Q_s^{sb}\right)(av)^2/c_s \geq 0$ when $\beta = \min\{\gamma(1 - Q_k^{sb})/(1-q_k), \gamma\}$. The comparison for different contracts is shown in Figure B2. Client will overwork with limited liability in general, except in some cases in loss-based liability. The client's effort is always higher in a third-party contract compared

with threshold-based or variable liability. Similarly, the MSS provider will underwork in most of the case, and its effort is always lower in a third-party contract compared with threshold-based or variable liability. In terms of welfare, threshold-based or variable liability is a slightly higher compared with a third-party contract, and again loss-based liability is the worst.

For parallel configuration, condition (38) becomes $-(1+\gamma)Q_s^{sb}av/2 \leq 0$, and (A8) could be satisfied with $\tilde{\beta} = \gamma\mathcal{B}\left(a, Q_k^{sb}, S\right)$ and a sufficiently large S. The contract comparison result is shown in Figure B3. Client will underwork with limited liability, and the distortion is least severe in threshold-based or variable liability. The effort in loss-based liability has an interesting pattern: half of the first best effort for $\gamma \geq 0.5$, and an inverted u-shape curve, which could be more than $Q_k^*/2$, for $\gamma < 0.5$. The MSS provider will also underwork with limited liability, and similarly the effort in threshold-based or variable liability is the closest to the first best effort. With limited liability, threshold-based or variable liability has the highest welfare, followed by third-party contract, and finally loss-based liability.

Figure B1: Liability Upper Bound (Total Effort)

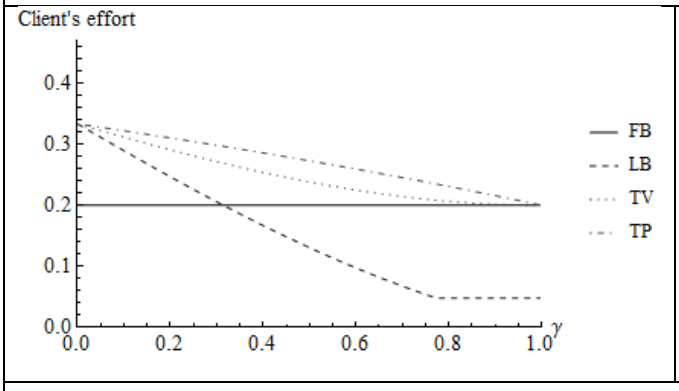
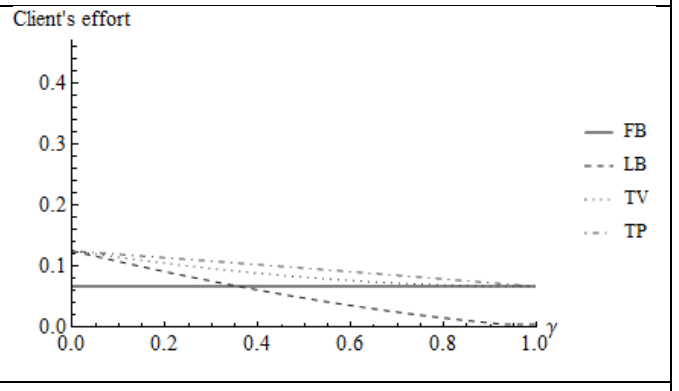
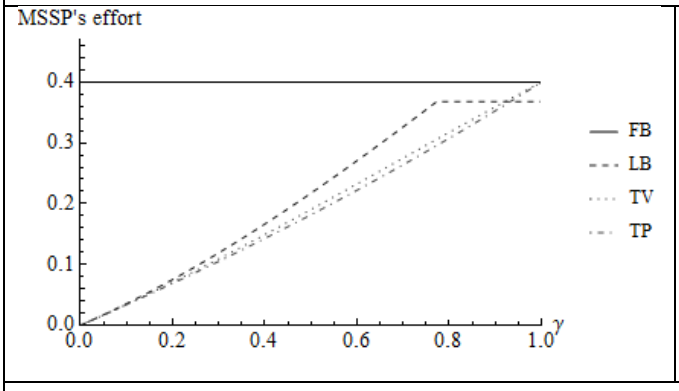
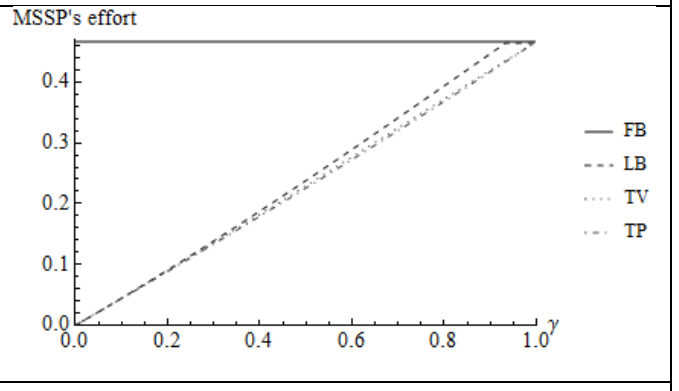
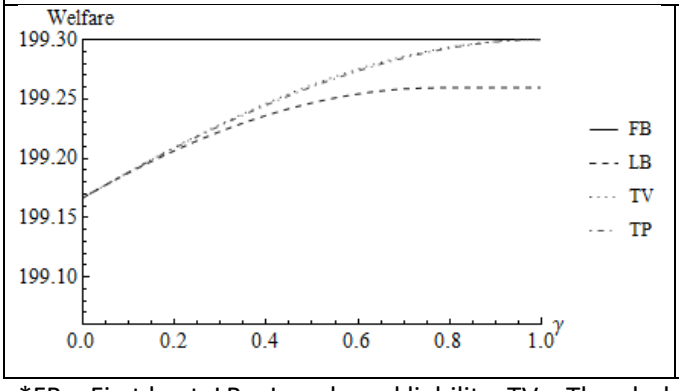
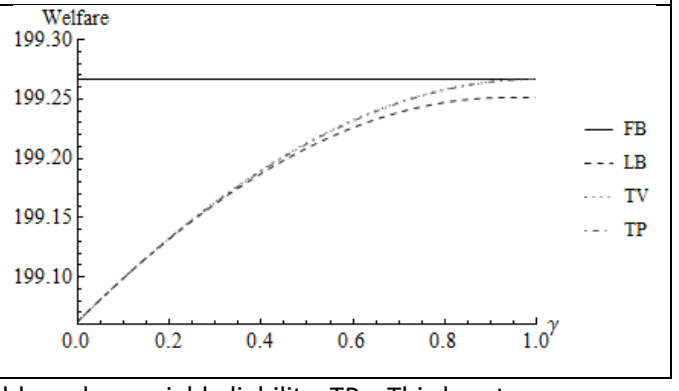
$c_k = 1.5$	$c_k = 4$
(i) Client's effort	
	
(ii) MSS provider's effort	
	
(iii) Welfare	
	

*FB = First best, LB = Loss-based liability, TV = Threshold-based or variable liability, TP = Third party contract.

Parameters: $m = 2, a = 0.005, v = 100, c_s = 1, \mathcal{B} = a\left(1 - \lambda_k q_{kj} - \lambda_s q_{sj}\right), \lambda_k = \lambda_s = 0.5$

Clients are assumed to be subsidized by $\beta_j^*\left(1 - \lambda_k q_{kj}^* - \lambda_s q_{sj}^*\right)av$ in third-party contracts.

Figure B2: Liability Upper Bound (Serial Configuration)

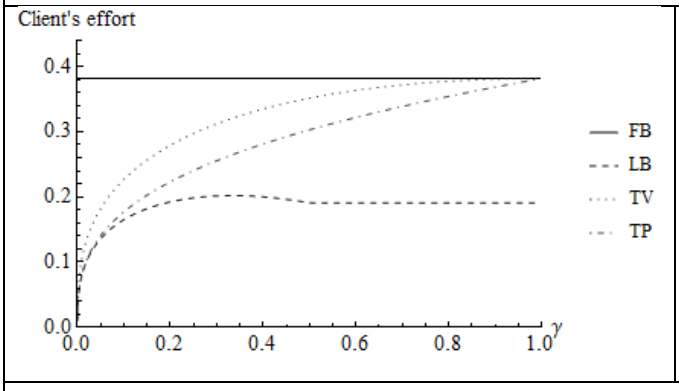
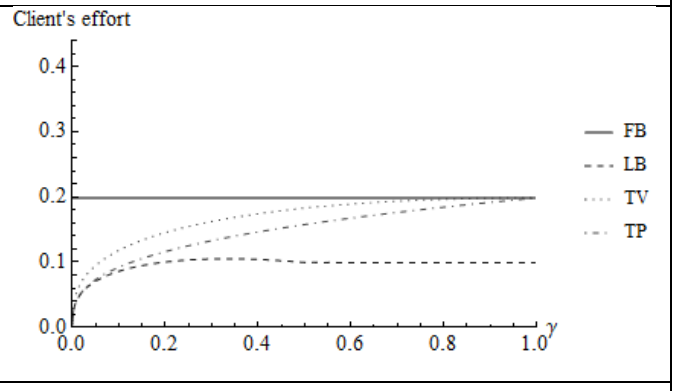
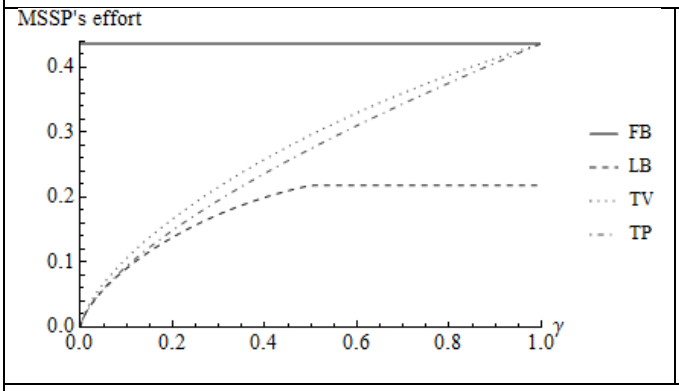
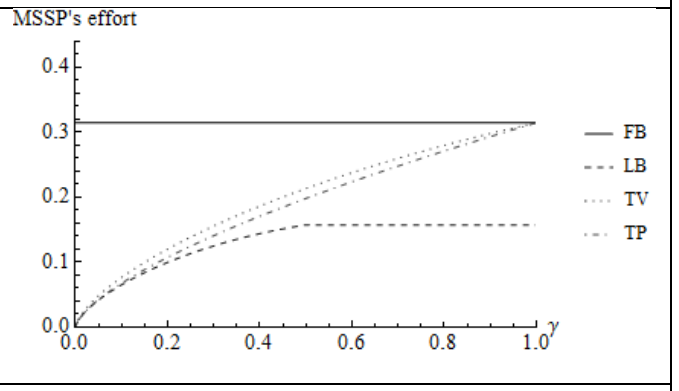
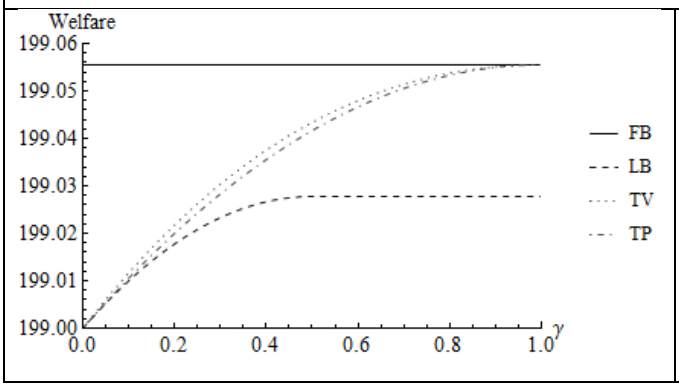
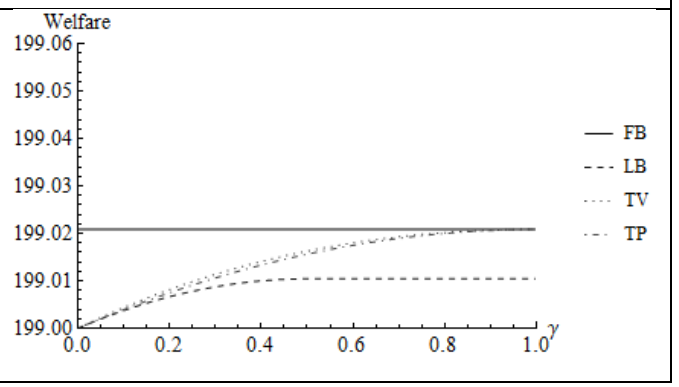
$c_k = 1.5$	$c_k = 4$
(i) Client's effort	
	
(ii) MSS provider's effort	
	
(iii) Welfare	
	

*FB = First best, LB = Loss-based liability, TV = Threshold-based or variable liability, TP = Third party contract.

Parameters: $m = 2, a = 0.005, v = 100, c_s = 1, \mathcal{B} = a(1 - q_{kj})(1 - q_{sj})$

Clients are assumed to be subsidized by $\beta_j^*(1 - q_{kj}^*)(1 - q_{sj}^*)av$ in third-party contracts.

Figure B3: Liability Upper Bound (Parallel Configuration)

$c_k = 1.5$	$c_k = 4$
(i) Client's effort	
	
(ii) MSS provider's effort	
	
(iii) Welfare	
	

*FB = First best, LB = Loss-based liability, TV = Threshold-based or variable liability, TP = Third party contract.

Parameters: $m = 2, a = 0.005, v = 100, c_s = 1, \mathcal{B} = a\left(1 - q_{kj}q_{sj}\right)$

Clients are assumed to be subsidized by $\beta_j^*\left(1 - q_{kj}^* q_{sj}^*\right)av$ in third-party contracts.