Efficient Cyber Risk: Security and Competition in Financial Markets[*]

Michael Brolley[†]
Wilfrid Laurier University

David A. Cimon[‡]
Wilfrid Laurier University

Ryan Riordan[§]
Queen's University - Smith School of Business

February 12, 2020

Abstract

In financial markets, clients entrust their capital and data to financial infrastructure providers who are vulnerable to breaches. We develop a model in which infrastructure providers compete to provide secure and efficient client services, in the presence of a cyber-attacker. In equilibrium, provider competition leads to both lower fees and security investment, but potentially greater vulnerability, in comparison to a monopolistic platform. We find that providers prefer to consolidate into a single platform, whereas clients prefer a fragmented infrastructure. The inefficiency of consolidated providers stems from under-investment in security when the market is small, and over-investment when the market is large. Policy makers should be wary of consolidation of critical financial infrastructure, as the impacts to security do not compensate clients for the increase in fees. Instead, minimum security investment requirements may improve security in competitive environments while yielding higher utility than the comparable monopoly platform.

[*]We thank Sophie Moinas for thoughtful comments, and Michael Beckenhauer for excellent research assistance. David Cimon and Michael Brolley acknowledge financial support from the Social Sciences and Humanities Research Council, Grant No. 430-2019-00814.

[†]Email: mbrolley@wlu.ca; web: http://www.mikerostructure.com.

[‡]Contact Author; Email: dcimon@wlu.ca; web: https://www.davidcimon.ca.

[§]Email: ryan.riordan@queensu.ca; web: http://ryanriordan.ca/

1 Introduction

Modern financial systems employ digital technologies to store information, transfer capital, convey instructions, and match buyers and sellers, but such technology is vulnerable to hacks and data breaches. In recent years, financial infrastructure has proved vulnerable to groups of sophisticated hackers looking to profit from disruption in financial markets. In March of 2017 Equifax, a large credit scoring firm, suffered a data breach that was thought to affect nearly everyone in the U.S. with a credit score, costing Equifax upwards of $700 million USD, and their clients potentially much more; the 2014 hack of Mt. Gox, a cryptocurrency exchange, led to the loss of all client holdings in Bitcoin, worth close to $2 Billion USD. As these attacks become more prevalent, financial institutions have begun to invest heavily in cybersecurity[1]. Moreover, regulators have put further pressure on infrastructure providers, imposing heavy fines for noncompliance and failure to report data breaches through the EU's General Data Protection Regulation,[2]. It is unclear, however, whether improvements in security through regulation will in fact lead to a more secure system, and whether such improvements are efficient, and welfare-enhancing. Our paper fills this gap.

We model the problem using a variant on an attacker-defender game. Cyber-attackers may invest in attack power, increasing the probability of a successful attack, while defenders (platforms, or infrastructure providers) may counter-invest in security to decrease the probability of a successful disruption. We interpret platforms and infrastructure broadly to include financial markets, information intermediaries, or financial institutions. We depart from the simple attacker-defender framework by allowing the level of asset under protection by the defender to be endogenous. We model the asset as a volume of transactions that a client seeks to complete at a financial institution (a defender).

[1] JP Morgan spends roughly $600 million USD annually and employs 3,000 employs in cybersecurity, see https://www.jpmorganchase.com/corporate/investor-relations/document/ceo-letter-to-shareholders-2018.pdf, page 35.

[2] As one example, British Airways was fined £183.4 million for attack involving 500,000 customers, see https://www.bloomberg.com/news/articles/2019-07-08/british-airways-faces-230-million-fine-over-2018-data-theft.

By modelling client transactions as the asset, our model portrays the classic principal-agent problem faced by clients at financial institutions: clients pay fees to a platform to complete a transaction, but also bear some risk of loss that is inversely related to investments that the platform choose to make in security. Clients are thus at the center of the game: the attackers seek to acquire the client's assets, while the defender wishes to receive the fee for providing a service. In our model, we assume that the clients may lose (some or all) of their assets following a successful attack, whereas the platform forfeits (to the client) only the transaction fee. Hence, clients weigh their patronage decisions on the defender's level of security and transaction fee.

We consider two market structures, consolidated and fragmented, and compare them along the market-size dimension. When markets are large, as in the banking sector, fragmented platforms are more likely to be successfully attacked relative to monopolies. Large monopolies are also more profitable, leading to potential platform consolidation. On the surface, large consolidated platforms appear optimal, as they offer the highest security; however, the higher security requires greater investment, leading to higher fees, and making clients worse off. Policy makers can improve welfare by breaking-up large monopolies, paradoxically reducing security but reducing fees relatively more. We show that large monopolies over-invest in security relative to their fragmented counterparts. To do so, we demonstrate that by breaking up monopolist platforms and requiring fragmented platforms to invest in security equivalent to total monopoly investment attains higher client utility than the monopolist platform, while maintaining similar attack vulnerability.

The results have broad implications on financial industry investment and consolidation with respective to cybersecurity. The increased concentration of financial assets on single platforms may attract more cyber-attacks, counter-acting the higher level of security investment. An important point is that cyber-defenses are relative to cyber-attacking capabilities: greater investment in security may attract more client volume, but this increases the profitability of an attack, incentivizing attackers to improve the sophistication of their attack,

and so on. A fragmented infrastructure has the attractive feature that the gains from hacking a smaller, independent platform, are lower than for the consolidated platform. Moreover, clients gain substantial diversification benefits, by losing only a portion of their transactions in the event of a successful attack. As a result, clients prefer a slightly increased probability of loss and a relatively lower fee.

Our model highlights a principal-agent problem in that clients expect platforms to invest in security to protect their assets and institutions wish to consolidate platforms to increase fees relative to the security that they provide. Our model provides testable hypotheses; (1) large monopolists will experience fewer security events, on average, relative to a fragmented platform, (2) markets with a monopolist institution will charge higher fees for security relative to markets with competition, and (3) the more similar the operations of competing institutions, the lower fees for security they will charge. Our model concurs with the theme that monopolists, when providing a "higher quality" product, will extract higher rents from clients relative to competitive platforms. In this context, however, given that product is "platform security and financial system stability", it may be natural to insist that more security is always better. We caution, however, that governments should be wary of arguments to consolidate for security reasons, as the resultant security improvement is inefficient.

Our results also have implications for co-investment in security. Co-investment in common security measures is analogous to a consolidated platform. A common security system, even if it is more secure than the individual system, increases the assets available for theft. If the system is hacked once, all of the assets protected by that system are also hacked. This generates the prediction that security co-investment and common security protocols may lead to an expensive financial system with an over-invested security infrastructure, compared to a fragmented platform in which each provider operates independently. This does not preclude sharing of information on attacks or best practices, but does warn against commonality in procedures, software, and cybersecurity providers.

1.1 Related Literature

On the surface, the incentives to commit cyber crime may not appear entirely different from conventional crimes.[3] The nature of cyber-crime, however, is unique: security is expensive compared to the cost of attacking, and state actors may have the incentive to conceal security threats (Anderson 2001). Further, the coordination of defensive efforts may be counterproductive, and policing across international borders may be difficult (Moore, Clayton, and Anderson 2009). Thus, it is necessary to develop a model that properly reflects this reality.

The existing literature within the computer science discipline on the economics of cybersecurity is well-developed.[4] Dynes, Goetz, and Freeman (2007) discuss optimal security investment as a classic profit maximization problem, while Gordon and Loeb (2002) frames optimal security investment as a function of a particular vulnerability's importance. Several works in the information-security literature model the game-theoretic implications behind investments in cybersecurity. For example, Gueye and Marbukh (2012) and Farhang and Grossklags (2017) use attacker-defender games to model specific aspects of security investment. Gueye and Marbukh (2012) models a network that consists of several nodes vulnerable to attack, while Farhang and Grossklags (2017) focuses on the time-based nature of cyber-attacks. Finally, Moore (2010) and Massacci, Swierzbinski, and Williams (2017) focus on policy solutions such as cyberinsurance. Our model furthers the literature by analyzing the impact of cybersecurity on client transaction decisions in a financial markets environment.

A consistent theme in the information-security literature remains the difficulty in assessing the true cost of cyber-crime. Several studies (e.g., Anderson, Barton, Böhme, Clayton, Van Eeten, Levi, Moore, and Savage (2013), Biancotti (2017) and Paquet-Clouston, Haslhofer, and Dupont (2018)) have attempted to measure the costs of cybersecurity incidents in various contexts, finding direct losses to be low or difficult to quantify. Anderson, Barton, Böhme, Clayton, Van Eeten, Levi, Moore, and Savage (2013) suggests that direct losses

[3] Becker (1968) lays out the economics of crime in detail and the model of bank robbery in Ozenne (1974) has similar incentives to many types of theft.

[4] Anderson and Moore (2006) and Moore and Anderson (2011) provide surveys on the topic.

(such as money being stolen) may be similar to the spending on security, but that indirect losses (such as a loss in confidence in the banking system) may be much larger. Our model provides theoretical support for several sources of welfare loss including direct theft from market participants, overspending on security, and the loss of business.

Cyber attack and defence games in the economics literature focus on the node-based structure of networks. For example, Bier, Oliveros, and Samuelson (2007), Goyal and Vigier (2010), Dziubiński and Goyal (2013), Acemoglu, Malekian, and Ozdaglar (2016), Hoyer and de Jaegher (2016) and Kovenock and Roberson (2018) analyze the incentives for attackers and defenders who must expend resources over networks.[5] These studies share similarity with Colonel Blotto-style games, with the added complexity of the interdependent-nature of computer networks. In our paper, we depart from the network-structure setup, assuming a single point-of-failure or "weak point" for the entire network. The simplification allows us to tractably study the principal-agent relationship inherent in many financial market applications. In our model, it is not only the service provider who fears an attack, but also the financial market participant who relies on the service. This participant does not invest in security themselves, but instead incentivizes service providers to invest through fee payments and volume of business.

We argue that market fragmentation may impact security investment, contributing to the existing literature on market fragmentation in financial markets. Several studies have shown the importance of speed (Menkveld and Zoican (2017), Pagnotta and Philippon (2017) and Brolley and Cimon (2020 (forthcoming))), access fees (Colliard and Foucault (2012), Malinova and Park (2015) and Chao, Yao, and Ye (2016)) and order visibility (Zhu (2014)). In our model, platforms differentiate themselves by the level of security investment, which impacts the a client's asset vulnerability, similar to other means of platform differentiation.

In a similar vein, the possibility of overinvestment in security is not dissimilar to the concept of overinvestment in speed technology by high-frequency traders (HFTs). In that

[5] A simpler case of exogenous disruptions is similar to the literature on weather or natural disasters, as in Shkilko and Sokolov (2016).

sense, our paper is complementary to works such as Biais, Foucault, and Moinas (2015) and Budish, Cramton, and Shim (2015). Whereas HFTs may overinvest in speed to gain an advantage over their competitors, platforms may overinvest in security to attract more traders. We argue that overinvestment in security is an artifact of monopolistic platforms, finding that platform competition can lead to welfare improvement.

2 Model

We develop a model in which platforms compete for business from a client in the presence of cyber risk. A client pays a fee to a platform to complete a transaction of a predetermined volume of an asset through the platform, while a cyber-hacker attempts to disrupt the transaction and steal all (or part) of the asset from the platform. To combat attack attempts, the platform can invest in cybersecurity to lower the probability of a successful attack.

Agents. There are three types of agents: a client, a cyber-hacker, and two platforms. The client seeks to conduct a transaction of an asset of size $Q \in \mathbb{R}_+$ via platform, for which they are willing to pay a per-unit fee, f_i, upon the successful completion of a transaction. One can also think of Q as the value of assets to the client and cyber-hacker. Upon submitting an order request to the platform, the accompanying fee f_i is proposed as a take-or-leave-it-offer.[6] The client is aware of the presence of a cyber-hacker that may attempt to disrupt the transaction and steal assets, and thus takes the probability of losing their assets during the transaction into account. Moreover, the client earns disutility (e.g., unmodeled risk-aversion) from having their assets stolen at Platform i, which we model as a quadratic cost in the asset size, Q_i.[7]

The client's transaction and the asset that is put at risk can be viewed in several ways. In a simple sense, the transaction can be viewed as any type of securities trade. This can be

[6]The intuition of the take-it-or-leave-it (TIOLI) offer fee mechanism extends to a context where the client pays for the service in advance, which fails due to a cyber attack. In this context, we imagine the loss of fee from a failed transaction to proxy for, e.g., the loss of continued business in a repeated reputation game, or the penalty of legal action by the client.

[7]This assumption is similar in nature to the security cost in Bier, Oliveros, and Samuelson (2007).

a traditional trade, where theft would be quite difficult. Alternatively, it can be seen as a cryptocurrency or other non-traditional transaction, where the risk of theft is much higher. Finally, the transaction can be viewed as an information transaction, where the asset is some form of information. An example of one such transaction could be an investor who must store trade data or securities holding data at some form of repository.

Two platforms $i \in \{H, L\}$ are available to facilitate the transaction. Platforms are each endowed with a basic level of cybersecurity $\lambda_i \in \mathbb{R}_+$, where $\lambda_L \leq \lambda_H$, that reduces the probability that an attack on the platform is successful. Platforms may spend additional resources to increase security, $s_i \in \mathbb{R}_+$, at cost $p(s_L, s_H) = \frac{1}{2}(s_L + s_H)$. Thus, the cost function of security investment given by, $c_i(s_i) = \frac{1}{2}(S)s_i$ where $S = s_L + s_H$ (i.e., constant marginal cost of security). Investments in cybersecurity reduce the probability δ_i that an attack is successful. For each platform, the total security level is given by $\lambda_i + s_i$. A platform is not liable for losses occurred from a failed transaction, but does not earn the fee if the transaction fails.

A cyber-attacker, referred to as the 'hacker', monitors the platform for opportunities to disrupt transactions and steal assets. A hacker that attempts to attack Platform i may invest resources a_i to improve the probability that the attempt succeeds, δ_i. A successful attack on Platform i yields the hacker a reward of $r \times Q_i$, where $r \in [0, 1]$ is the fraction of assets successfully stolen. This implies that the client's disutility of loss from a successful attack at Platform i is $(rQ_i)^2$.

We offer two interpretations of r. First, we may interpret r as the inherent difficulty of the asset to steal, and/or a recovery rate. For example, records of physical asset ownership may have a difficulty parameter $r = 0$, as even if the records are stolen or corrupted, back-up copies may exist; digital assets (crypto wallet addresses, banking information) on centralized systems may have a higher r, as digital records of asset ownership may be accessed, and transactions authorized and cleared before the hacker can be interrupted.

Alternatively, we can interpret r as the relative value of data or assets that can be stolen or the ease with which they can be monetized by the hacker. This interpretation reflects the disparity between the transaction that the client wishes to complete, and the value of the asset truly at risk. For example, one's personal data may offer a hacker the *possibility* of stealing all of a client's assets, but in practice, the hacker may not be able to realize the full value of the data before the platform recognizes the breach, and denies access.

We model the hacker resource cost as linear with the vision that individual hackers are often small, so as lower their visibility to law enforcement. Thus, we assume that attackers often weight their resources towards increasing the number of attempts, versus improving the sophistication each attack.As an example, one common type of repeated attack is phishing attempts, wherein hackers attempt to acquire username and password information from many different employees at an organization.

The Hacking Game. Both the hacker and the platform may invest resources to increase or lower, respectively, the probability that a disruption and theft attack succeeds, δ_i. We model this probability with the following function for each Platform i;

$$\delta_i = 1 - \exp\left(-\frac{a_i}{\lambda_i + s_i}\right) \tag{1}$$

Our functional form for δ mirrors the shape of a binomial distribution where, from the perspective of the hacker, the probability of a single success increases at a decreasing rate with the number of attempts, conditional on the level of security investment (which determines the probability of success of an individual attempt). In this way, we can think of attack strength as simultaneous hacking attempts by a collective of agents, each paying a constant cost to participate in the hack. The larger the collective, the greater the probability of success. We note that the functional form in (1) is similar in shape to those found in Goyal and Vigier (2010) and others.

Timing and Information. Agents participate in a finite three-period game. At $t = 0$, the client sends transaction requests of sizes $Q_H \in \mathbb{R}_+$ and $Q_L = Q - Q_H$ to Platforms H

and L for completion, respectively. For the service, the client offers Platform i a percentage of her transaction as a fee f_i as a take-it-or-leave-it offer if her transaction is completed. At $t = 1$, each Platform i selects security investment s_i, given the transaction size and fee offered by the client. The hacker enters the market at $t = 2$ upon which time he selects platform-specific resource investment a_i. Given resource investment for attacking each platform, the hacker attempts an attack on both platforms. The timing and structure of the model are common knowledge to all market participants.

Payoffs. The hacker earns a payoff from the fraction of assets stolen upon a successful hack attempt at each platform, less the total resources spent on attack strength, $a_H + a_L$. The hackers payoff, denoted by the subscript 'A', is given by,

$$\pi_A(a_H, a_L) = (\delta_H \times rQ_H - a_H) + (\delta_L \times rQ_L - a_L) \tag{2}$$

Platforms earn profit through fees from completing transactions. To improve the probability of a successful transaction, platforms may invest in cybersecurity at the market rate $p(s_H + s_L)$. Taken together, a Platform i earns the following payoff from a client order.

$$\pi_i(s_i) = (1 - \delta_i) f_i Q_i - p(s_H + s_L) s_i \tag{3}$$

Finally, because a client *must* conduct a transaction of size Q, the implicit assumption is that the client earns sufficient negative utility outside of the model for not completing the transaction (e.g., assets cannot be consumed until they are converted to currency, etc.) such that their goal is to maximize utility (minimize disutility) by dividing the order up across two platforms. Hence, we define a client's payoff as the following utility function:

$$U(Q_L, Q_H, f_L, f_H) = (1 - \delta_H)(1 - f_H)Q_H - \delta_H(rQ_H)^2 + (1 - \delta_L)(1 - f_L)Q_L - \delta_L(rQ_L)^2 \tag{4}$$

We assume that the fraction of asset at risk, r, is asset-specific, and thus does not change across platforms.

3 Equilibrium

In this section, we study the role of venue competition in cybersecurity investment, platform market share, and client welfare. As a benchmark case, we begin with an examination of a single platform as a benchmark, and subsequently compare how fragmentation impacts the market. Moreover, because platform vulnerability as defined in (1) reflects a proportionality between transaction size Q and endowed platform security λ, we normalize $\lambda_H = 1$, so as to describe our results in Q, relative to endowed security. Then, as $\lambda_H \geq \lambda_L$, we assume $\lambda_L = \eta \in [0, 1]$.

3.1 Single Platform

We begin by simplifying to a single platform environment. Because we focus on a single platform in this subsection, we drop subscript i from all choice variables. We solve our model via backward induction, beginning with the hacker's investment decision a, given s, f and Q. The hacker selects $a \in [0, \infty)$ to maximize their payoff from (2). Taking the first-order condition and solving for $a^\star$,

$$\max_a \pi_A(a) = \max_a \left(1 - \exp\left(-\frac{a}{1+s}\right)\right) \times rQ - a \tag{5}$$

$$a^\star = \begin{cases} -(1+s)\ln\left(\frac{1+s}{rQ}\right) & s < rQ - 1 \\ 0 & s \geq rQ - 1 \end{cases} \tag{6}$$

Note that the solution $a^\star$ is zero if aggregate cybersecurity at the platform $1 + s$ exceeds the reward of the hack *conditional* on success. Using our solution to the hacker's problem, we can simplify the probability of a successful hack $\delta(s; a^\star)$ to,

$$\delta(s; a^\star) = \begin{cases} 1 - \frac{(1+s)}{rQ} & s < rQ - 1 \\ 0 & s \geq rQ - 1 \end{cases} \tag{7}$$

Equations (6) and (7) describe one of two possible results for the client. In the case where $a^\star = 0$ and $\delta(s; a^\star) = 0$, the client faces no asset vulnerability. The combination of high platform security $(1+s)$ and a small reward from attacking (rQ) create a situation in which the attacker ignores the platform altogether. Alternatively, if the security is sufficiently low, or the reward is sufficiently high, the client faces a positive probability of loss. While the reward for theft and base platform security are exogenous parameters, the platform's security investment is endogenously determined. Thus, whether (and at what intensity) the hacker attacks is a function of the platform's security investment.

Given the equilibrium hacker attack strength $a^\star$, we look to the platform's optimal security investment problem. The platform selects s to maximize profit, conditional on the quantity and fee conditions of the order submitted by the client. Optimizing payoff function (3) over s yields the following $s^\star$ where the subscript 'M' denotes a single platform market.

$$\max_s \pi_M(s) = \max_s (1-\delta) fQ - p(s)s \tag{8}$$

$$s^\star = \begin{cases} f/r & f < r(rQ-1) \\ rQ-1 & f \geq r(rQ-1) \end{cases} \tag{9}$$

Note that the condition $f \geq r(rQ-1)$ should bind with equality in equilibrium, as the client would not offer a higher fee given that security investment is independent of f for all $f \geq r(rQ-1)$.

Finally, we approach the client's asset allocation problem, given $a^\star$ and $s^\star$. Because only one platform operates, transaction size is fixed at Q. The client thus chooses a fee level f to

maximize the utility function in (4),

$$\max_f U(Q,f) = \max_f (1-\delta)(1-f)Q - \delta(rQ)^2 \tag{10}$$

$$f^\star = \begin{cases} 0 & Q \leq \frac{1}{r} \\ r(rQ-1) & \frac{1}{r} < Q \leq \frac{1+r}{r^2} \\ \frac{1+r(rQ-1)}{2} & Q > \frac{1+r}{r^2} \end{cases} \tag{11}$$

We summarize the solutions to the hacker, platform, and client problems in the following proposition.

Proposition 1 (Equilibrium: Single Platform) *Given $r \in (0,1)$ and $Q \in \mathbb{R}_+$, there exists unique values $(a^\star, s^\star, f^\star)$ from (6), (9) and (11) that, in order, solve the hacker, platform, and client problems in (5), (8), and (10). Moreover, if $Q \leq \frac{1+r}{r^2}$, then $a^\star = 0$.*

Proof (Proposition 1). Follows from the preceding discussion in-text. ■

[Figure 1 about here.]

The optimal fee offered by the client partitions the equilibrium into three regions characterized by Q. We illustrate these regions in Figure 1. We define these equilibrium regions based on the thresholds in Q which we denote $M_1 = \frac{1}{r}$ and $M_2 = \frac{1+r}{r^2}$.

For small transaction sizes ($Q \leq M_1$), the client does not need to incentivize the platform to invest in security, as the security endowment exceeds the value of the asset at risk, $rQ < 1$, which implies that $a^\star = 0$. Thus, for sufficiently small transactions, no fees is necessary, as it is not worthwhile for attackers to disrupt the transaction.

With larger transactions ($M_1 < Q \leq M_2$), the client finds it optimal to pay for additional security. The client now offers $f^\star > 0$, which incentivizes the platform to invest in additional security ($s^\star = rQ - 1$). At this stage, optimal security investment is large enough such that the hacker makes no effort to disrupt the transaction ($a^\star = 0$).

For very large transactions ($Q > M_2$), the nature of the equilibrium changes. As transaction size increases, the exchange's quadratic cost of security begins to outweigh the attack cost to the hacker. The investor offers a positive fee, however it no longer incentivizes the platform to fully secure its systems. The hacker now attacks with $a^\star > 0$, disrupting the transaction with positive probability. Thus, in the single-platform case, attackers disrupt transactions of sufficient value. The monopoly case captures the intuition of Becker (1968): the cost of enforcement—or in our case, prevention—impacts the optimal "crime level". As the value of the asset to the hacker grows too large, optimal security investment does not fully prevent cyber-crime.

3.2 Fragmented Market

Consider now two platforms H and L that operate with different endowments of security, $\lambda_H = 1$ and $\lambda_L = \eta \in [0, 1]$, respectively.

Similarly to Section 3.1, we solve the problem via backward induction. We begin by solving the hacker problem, where the hacker now selects an attack strength a_i for *each* platform given their security investment s_i, and the transaction volume share Q_i sent to each platform by the client. Because the hacker considers an attack on each venue $i \in \{H, L\}$ as independent events, the solution to the hacker's problem follows the single platform setting. Hence, investment in attack strength for Platform i is given by,

$$\max_{a_i} \pi_A(a_i) = \max_{a_i} \left(1 - \exp\left(-\frac{a_i}{\lambda_i + s_i}\right)\right) \times rQ_i - a_i \tag{12}$$

$$a_i^\star = \begin{cases} -(\lambda_i + s_i) \ln\left(\frac{\lambda_i + s_i}{rQ_i}\right) & s_i + \lambda_i < rQ_i \\ 0 & s_i + \lambda_i \geq rQ_i \end{cases} \tag{13}$$

Inputting the solution to the attacker's investment problem at each platform allows us to write platform vulnerability $\delta(s_i; a_i^\star)$ in terms of $s_i^\star$ and Q_i.

$$\delta_i(s_i; a_i^\star) = \begin{cases} 1 - \frac{(\lambda_i + s_i)}{rQ_i} & s_i + \lambda_i < rQ_i \\ 0 & s_i + \lambda_i \geq rQ_i \end{cases} \tag{14}$$

Similar to the single platform, the platforms in a fragmented market face a hacker that will attack a platform i when total security $s_i + \lambda_i$ is lower than the reward (fraction of total market share, rQ_i) that it can obtain. The difference between the single platform and the fragmented platforms is that the attacker considers each platform separately. Thus, the attacker may attack any one platform where their incentive at that platform i (rQ_i) exceeds that platform's security ($\lambda_i + s_i$). Unlike the single platform case, this condition depends on both the platform's security investment, and the division of the client's order flow. In this game, if the total reward $rQ < 1+\eta$, then this implies that the platform is sufficiently secure such that no attackers will make attempts on any platform; that is, there exists a partition of the total quantity $Q_H + Q_L = Q$ by the client across both platforms such that $rQ_H < 1$ and $rQ_L < \eta$, implying that $\delta_H^\star = \delta_L^\star = 0$ with $s_H^\star = s_L^\star = 0$. Since there is no security investment game to study in such a context, in what follows, we assume that $rQ > 1 + \eta$.

Given the inferred attack strength chosen by hackers at $t = 2$, each platform selects cybersecurity investment s_i at $t = 1$, conditional on $(a_i^\star, f_i, Q_i)$, to maximize their profit function in (3). We begin by characterizing the interior solution (i.e., $\delta_H^\star > 0$ and $\delta_L^\star > 0$), with any corner solutions to follow. Because the platforms choose cybersecurity investment simultaneously and the price of security $p(S)$ is a function of total security investment, the platforms play a Cournot-like competition game in security investment. In this game, we denote the opponent platform (to platform i) as $-i$.

$$\text{F.O.C} : \frac{\partial \pi_i(s_i)}{\partial s_i} = 0 \Rightarrow s_i(s_{-i}) = \frac{2f_i - rs_{-i}}{2r} \tag{15}$$

Solving the best response functions $s_i(s_{-i})$ and $s_{-i}(s_i)$ for $s_i^\star$, we write:

$$s_i^\star = \begin{cases} 0 & \text{if } 2f_i \leq f_{-i} \\ 2\left(\frac{2f_i - f_{-i}}{3r}\right) & \text{if } 2f_i > f_{-i} \end{cases} \tag{16}$$

While the hacker attacks each venue independently, the venues have interdependent solutions to their optimization problems. This arises because the competition for security resources among the two venues lead to higher prices as total security investment increases. Thus, venues invest in security based on the relative fee that they have been offered, taking into consideration security investment by the competing venue, which is implied by the competing platform's fee. We can see from (16) that the platform to be offered the higher fee invests the most in additional security, regardless of endowed security, λ_i.

Given solutions to the hacker and platform problems, the client jointly chooses their volume share per platform, Q_H and Q_L, and sets the fees that they offer each platform to fulfill their orders, f_L and f_L. To simplify exposition, we separate the overall volume level Q from the volume shares by writing $Q_i = q_i Q$, where $q_i \in [0, 1]$. Moreover, this simplification allows us to write the volume share constraint as $q_H + q_L = 1$, which provides that $q_H = 1 - q_L$. We rewrite the client payoff function from (4) as,

$$U(q_H, q_L, f_H, f_L) = \max_{q_L, q_H, f_L, f_H} \sum_{i \in \{H,L\}} (1 - \delta_i)(1 - f_i) q_i Q - \delta_i (r q_i Q)^2 \tag{17}$$

Because we optimize q_H and q_L subject to a constraint, we use the Lagrangian approach, where Γ is the Lagrange multiplier on the constraint $q_H + q_L = 1$. Computing the first-order conditions, we arrive at:

$$\text{F.O.C}(f_i) : \frac{2(2q_i - q_{-i})Qr^2 - 3\lambda_i r - 4(2f_i - f_{-i}) + 2}{3r^2} = 0 \tag{18}$$

$$\text{F.O.C}(q_i) : \frac{Q}{3}\left(4f_i - 2f_{-i} + 3r\lambda_i - 6r^2 Q q_i\right) - \Gamma \times Q = 0 \tag{19}$$

Using the first-order conditions in (18)-(19) across both Platforms i and $-i$, we solve for the fee offered to Platform i in terms of (q_i, q_{-i}),

$$f_i^\star = \frac{2 + 2Qr^2 q_i - r(2\lambda_i + \lambda_{-i})}{4},\ \delta_L^\star > 0, \delta_H^\star > 0. \tag{20}$$

Computing the fee and quantity for each $i \in \{H, L\}$, we solve for the optimal volume shares $(q_H^\star, q_L^\star)$ submitted to each platform.

$$(q_H^\star, q_L^\star) = \left(\frac{2Qr + 1 - \eta}{4Qr}, 1 - q_H^\star \right),\ \delta_L^\star > 0, \delta_H^\star > 0. \tag{21}$$

The interior solution for q_i given in (21) allows us to characterize the corner solutions of the problem. In what follows, we omit the solution $(q_H^\star, q_L^\star) = (1, 0)$, which occurs when $rQ \leq 1 + \eta$, because this would violate our supposition that $rQ > 1 + \eta$.

We begin with the solution to the attacker's problem in (12)-(13) that yields the equation for δ_i, (14). Here, a corner solution may exist where $\delta_i = 0$, if and only if platform i makes sufficient investment in security, $s_i^\star \geq rQq_i - \lambda_i$. Then, as $s_i^\star$ is a function of $f_L^\star(q_L^\star)$ and $f_H^\star(q_H^\star)$ which obtains via (16) and (20), we use the solutions $(q_H^\star, q_L^\star)$ from (21) to determine the parameter values (Q, r, η) (if any) for which $\delta_L^\star = 0$ and/or $\delta_H^\star = 0$, in equilibrium. Doing so, we arrive at the following lemma.

Lemma 1 (Equilibrium Full Security) *Let $rQ > 1 + \eta$. If Q satisfies: i) $Q \leq \frac{3r+2}{2r^2}$, then $\delta_H^\star = 0$ in equilibrium, and; ii) $Q \leq \frac{2+(1+2\eta)r}{2r^2}$, then $\delta_L^\star = 0$ in equilibrium. Moreover, $\frac{2+(1+2\eta)r}{2r^2} \leq \frac{3r+2}{2r^2}$.*

A platform that operates at full security is incentivized to invest in security only up to the point at which $s_i^\star = rQq_i - \lambda_i$. Clients infer this, and choose to offer a fee $f_i^\star$ that ensures a platform will invest exactly $s_i^\star = rQq_i - \lambda_i$. Thus, Lemma 1 suggests that we need to expand (16) to characterize $s_i^\star$ over all Q such that $rQ > 1 + \eta$, inclusive of regions where

$\delta_L^\star = 0$ and/or $\delta_H^\star = 0$. We write this pairwise function for $(s_L^\star, s_H^\star)$ below.

$$(s_L^\star, s_H^\star) = \begin{cases} \left(\max\left\{rq_LQ - \eta, 0\right\}, \max\left\{0, rq_HQ - 1\right\}\right) & Q < \frac{2+(1+2\eta)r}{2r^2} \\ \left(\frac{2f_L^\star - r(rQ(1-q_L^\star)-1)}{2r}, \max\left\{0, rq_HQ - 1\right\}\right) & \frac{2+(1+2\eta)r}{2r^2} \leq Q \leq \frac{3r+2}{2r^2} \\ \left(\frac{2f_L^\star}{3r}, \frac{2f_H^\star}{3r}\right) & Q > \frac{3r+2}{2r^2} \end{cases} \tag{22}$$

Finally, with the equilibrium security values from (22), we back out the optimal fee schedule in terms of market size, Q, which we summarize in the following lemma. When $\delta_i = 0$, the fact that $s_i^\star = rQq_i - \lambda_i$ leads the first-order condition for $s_i^\star$ in (15) to determine the solution to $f_i^\star$, as the client offers a fee that ensures the platform will offers exactly enough security to yield zero vulnerability. This solution differs from the interior solution given by (20), which we characterize in the following lemma.

Lemma 2 (Equilibrium Fee Schedules and Platform Volume Shares) *Let* $rQ > 1+\eta$. *Then, the equilibrium fee schedule* $(f_L^\star, f_H^\star)$ *accepted by the platforms is given by:*

$$(f_L^\star, f_H^\star) = \begin{cases} (r(rQ - 1 - \eta), 0) & \frac{1+\eta}{r} < Q \leq \frac{3+\eta}{2r} \\ \left(\frac{r(6rQ-7\eta-5)}{8}, \frac{r(6rQ-5\eta-7)}{8}\right) & \frac{3+\eta}{2r} < Q \leq \frac{2+(1+2\eta)r}{2r^2} \\ \left(\frac{2(2+Qr^2)-3(1+\eta)r}{8}, \frac{2(1+2Qr^2)-3(2+\eta)r}{8}\right) & \frac{2+(1+2\eta)r}{2r^2} < Q \leq \frac{3r+2}{2r^2} \\ \left(\frac{2(2+Qr^2)-3(1+\eta)r}{8}, \frac{2(2+Qr^2)-3(1+\eta)r}{8}\right) & Q > \frac{3r+2}{2r^2} \end{cases} \tag{23}$$

Moreover, the equilibrium volume shares $(q_L^\star, q_H^\star)$ *are given by:*

$$(q_L^\star, q_H^\star) = \begin{cases} \left(\frac{1}{rQ}, \frac{rQ-1}{rQ}\right) & \frac{1+\eta}{r} < Q \leq \frac{3+\eta}{2r} \\ \left(\frac{2Qr+1-\eta}{4Qr}, \frac{2Qr-(1-\eta)}{4Qr}\right) & Q > \frac{3+\eta}{2r} \end{cases} \tag{24}$$

Lemma 2 presents the equilibrium fee schedules of the two platforms, and the subsequent client volume shares in the fragmented market. Here, the client uses to combination of fees and volume shares to minimize their transaction costs. The result is that the client splits

their assets unevenly across the platforms (Equation 21). The fees offered by the client, however, depend on the total assets allocated to each platform. For relatively low total volume, the fee offered to platform H to induce full security ($\delta_H^\star = 0$) is lower than the fee offered to platform L, as it is cheaper to pay platform L a higher per-unit fee to secure their additional assets, rather than pay a positive per-unit fee $f_H^\star > 0$ at platform H on all their units to secure additional units at platform H.

If the total asset volume is large enough, $\left(Q > \frac{3r+2}{2r^2}\right)$, the client will offer both platforms a positive, but *identical* fee. As a consequence, both platforms invest identically in supplemental security, $s_H^\star = s_L^\star$. That is not to say that both platforms are equally secure, in equilibrium. The relative security at each platform, taken as the probability of a successful attack, depends not only on the supplemental investment, but also the inherent security at each platform λ_i, and the manner in which the client divides their volume. We obtain $s_i^\star$ from inputting Equation (23) into (16). Similarly, we obtain $a_i^\star$ by inputting $s_i^\star$ into (13). This allows us to arrive at the following Proposition.

Proposition 2 (Equilibrium: Fragmented Market) *Let $r \in (0,1)$ and $Q \in (0,\infty)$ satisfy $\eta \in [0,1]$, $rQ > 1+\eta$. Then there exists unique values $a_i^\star, s_i^\star$, and $(f_i^\star, q_i^\star)$ for $i \in \{H, L\}$ that solve the hacker, platform, and client problems in (12), (16), and (17), respectively. Moreover, if $rQ \leq 1+\eta$, then the unique equilibrium is such that $(a_i^\star, s_i^\star, f_i^\star) = (0,0,0)$, and $q_H^\star$ may take any value in $(0,1]$.*

Proof (Proposition 2). Follows from Lemmas 1 and 2 and the preceding discussion. ■

[Figure 2 about here.]

In a fragmented market, transaction volume partitions equilibrium actions into five regions characterized by the total size of the transaction Q. We define these equilibrium regions based on the parameter values $C_1 = \frac{1+\eta}{r}$, $C_2 = \frac{3+\eta}{2r}$, $C_3 = \frac{2+(1+2\eta)r}{2r^2}$ and $C_4 = \frac{3r+2}{2r^2}$. We illustrate these regions in Figure 2.

First, for a very small transaction volume ($Q \leq C_1$), the client pays no fee and the hacker does not attack. For low Q values in this region ($Q < \frac{1}{r}$), it can correspond to a monopoly where the small transaction size and security endowment at platform H render attacking unprofitable. Alternatively, for higher Q values in this region, it necessarily corresponds to a fragmented market where the low transaction size can be allocated across both platforms such that attacking either platform unprofitable.

The second and third regions are similar in nature. In both cases, the client suffers no risk of attack at either venue. In the second region ($C_1 < Q \leq C_2$), the client pays a positive fee to Platform L, while in the third region ($C_2 < Q \leq C_3$), the client pays positive fees to both platforms. These regions correspond to transactions where it is efficient for the client to fully protect their order. However, as transaction size grows, this becomes difficult to sustain.

Fourth, for large transactions ($C_3 < Q \leq C_4$), the client both splits their transactions between the two platforms and pays fees. Moreover, it is worthwhile for the hacker to attack the low-sophistication exchange despite their security investments. In this case, the client splits their transaction between both platforms and pays the platforms to invest in additional security. However, because of the decreasing returns to security investment, it is not profitable to fully secure the transactions at the low-sophistication platform.

Finally, for very large transactions ($C_4 < Q$), the client pays fees to and expects a positive probability of attack at both venues. As in the single platform case, it is simply not viable to fully secure transactions of this size.

In comparison to the monopoly case, the equilibrium regions for both the monopoly and fragmented market cases form an ordinal ranking that depends, in part, on the relative sophistication of the two platforms, η. For $\eta > 1/2$, $M_1 \leq C_1 \leq C_2 \leq M_2 \leq C_3 \leq C_4$, while $M_1 \leq C_1 \leq C_2 \leq C_3 \leq M_2 \leq C_4$ for $\eta \leq 1/2$. These comparisons are shown in Figure 3.

[Figure 3 about here.]

Under any relative sophistication, small transactions are perfectly secure and require no additional investment. In the fragmented market case, however, the client receives diversification benefits from the security endowment at both venues. Thus, the size of transaction under which the client pays no fees and puts no assets at risk is larger in the fragmented market case, than under the monopoly.

The relative quality of the low-sophistication venue (η) also plays a role. When the low-sophistication venue is relatively high quality ($\eta > \frac{1}{2}$), the total transaction size under which the hacker is induced to invest in attack strength is lower than in the monopoly case, as the closer quality of the venues leads to more intense competition in fees. Conversely, when the low-sophistication venue is lower quality ($\eta \leq \frac{1}{2}$), the total transaction size for which the hacker is induced to invest in attack strength is higher than the transaction size under which the monopoly is subject to attacks. While this may seem counter-intuitive, this result follows from the volume share at each platform. When η is low, the low-sophistication venue receives very little volume, making it an unattractive target for the attacker.

4 Competition, Security, and Welfare

Proposition 2 outlines that the equilibrium depends jointly on market size Q, the proportion of asset at risk r, and the relative sophistication level of the platforms, η. In this section, we continue to focus on the case where transaction size is sufficiently large such that the solution to the fragmented market problem admits two platforms with positive volume ($rQ > 1 + \eta$), to maintain a basis for comparison to the single platform case.

In equilibrium, competition between platforms for client transactions q_i manifests in fees. The client is incentivized, for sufficiently large transactions, to offer identical fees to each platform, while splitting their transactions q_i in favour of the more-sophisticated platform ($q_H^\star \geq q_L^\star$) to minimize asset risk. For smaller transactions, optimal security investment at Platform H yields zero vulnerability at that exchange, and as such, they are incentivized

to allocate more resources (i.e., a higher fee) to Platform L to protect their remaining vulnerable assets, such that $f_L^\star \geq f_H^\star$. The somewhat counter-intuitive implication is that more-sophisticated platforms are able to better compete against low-sophistication platforms in fees when it comes to security investment. As a result, their relative market share of client transactions is higher. Comparatively, the single platform setting faces no such competition, and because all assets are secured at a single venue, the fee contract offered to the monopolist is higher. We summarize this intuition in the following proposition.

Proposition 3 (Fee Competition) *Let the parameters (r, η, Q) satisfy Proposition 2. Then, $f_M \geq q_H^\star f_L^\star + q_L^\star f_H^\star$ and $f_L^\star \geq f_H^\star$, where $f_H^\star = f_L^\star$ for all $Q > \frac{3r+2}{2r^2}$. Moreover, $f_L^\star$ and $f_H^\star$ are decreasing in η.*

In equilibrium, platforms earn profits based on a combination of market share and fees. As with Lemma 2, sufficiently large markets lead competition to drive fees to be equal at both platforms. Thus, with competing platforms, the average fees paid by the client are lower than the fee paid in the single platform environment. This is not driven entirely by the endowment of base security λ_H and λ_L to each venue, where the sum of these innate security levels are larger than than of the monopolist, who is assumed to have the same λ as platform H. Indeed, if $\eta = 0$, one can show that in a large market ($Q > \frac{3r+2}{2r^2}$) where all platforms are not perfectly secure ($\delta_i < 0$), $f_M < f_H^\star = f_L^\star$. Hence, we observe that a fragmented market leads to competition on fees. Fees in the fragmented market compared to the single market are illustrated in Figure 4.

[Figure 4 about here.]

Is fee competition an ideal outcome for clients, when those fees are collected to provide cybersecurity, and minimize asset vulnerability? We define aggregate vulnerability under the single platform and fragmented platform cases as δ_M and δ_C, respectively, where δ_C is given by the value-weighted average of the vulnerability at each platform:

$$\delta_C = q_H^\star \delta_H^* + q_L^\star \delta_L^*. \tag{25}$$

Similarly, we write total investment in the fragmented market case as $S_C = s_H + s_L$. In the following proposition, we summarize a comparison of the equilibrium security investment level and vulnerability across the single and fragmented platform cases, in the context of market size, Q.

Proposition 4 (Security Investment and Vulnerability) *Let the parameters (r, η, Q) satisfy Proposition 2. Then, security investment in the single platform market is always greater than the fragmented market ($S_M^\star \geq S_C^\star$). For vulnerability δ_i, if $\eta > 1/2$ and the total market size Q is such that,*

- $Q \in \left[0, \frac{1+3r\eta}{r^2}\right]$, *then* $\delta_H^\star < \delta_M^\star$ *and* $\delta_M^\star \geq q_L^\star \delta_L^\star + q_H^\star \delta_H^\star$
- $Q > \frac{1+3r\eta}{r^2}$ *then* $\delta_H^\star < \delta_M^\star$ *and* $\delta_M^\star \leq q_L^\star \delta_L^\star + q_H^\star \delta_H^\star$

If $\eta \leq 1/2$, then $\delta_M^\star \leq q_L^\star \delta_L^\star + q_H^\star \delta_H^\star$ for all Q.

Proposition 4 suggests that diversification through competition creates a more secure venue in Platform H. As the market grows, however, the competition in fees impacts how much the platforms together will invest in cybersecurity. The competition for cybersecurity resources $s_i^\star$ by Platform i, in addition to the competition in price through fees, leaves a fragmented platform more vulnerable to attacks when the market is relatively large ($Q > \frac{1+3r\eta}{r^2}$) or platform L has a sufficiently lower security endowment ($\eta \leq 1/2$). In a fragmented market, Equation (23) illustrates that fees are less sensitive to changes in overall market size relative to the single-platform market in Equation (11). The implication is that in a fragmented market, clients derive utility from security, but only to a point. Even though clients bear the risk of increased vulnerability, the utility from fee competition dominates. Moreover, these two effects are substitutes in the client utility function, as security investment increases (linearly) in fees. Security investment and vulnerability in the fragmented market compared to the single market are illustrated in Figures 5 and 6.

[Figure 5 about here.]

[Figure 6 about here.]

Taken together, Proposition 3 and Proposition 4 present an industrial organization dilemma for the client: on one hand, they prefer the lower fees associated with the fragmented market, but this leads to greater vulnerability in equilibrium, when compared to the monopolistic setting. To reconcile this issue, we compute the total client utility level $U(Q)$, aggregated over total transactions Q, for both market settings. What we find is that the fragmented market leads to utility that is no lower than in the single platform environment.

Proposition 5 (Client Utility) *Let the parameters (r, η, Q) satisfy Proposition 2. Then, the client earns (at least weakly) higher utility in a fragmented platform market versus a single platform market.*

Alongside Proposition 4, Proposition 5 illustrates that single-platform markets underinvest in cybersecurity in small markets, relative to what would obtain in a fragmented market: security investment is lower, and vulnerability is higher, without a fee level that compensates for the associated increased risk. For larger transactions, the single-platform market now overinvests in security, relative to the benefits to client utility: the single-platform market outspends the fragmented market on security, but at a cost of much higher fees that are disproportionately rent-extracting, leading to a net-reduction in client utility. That is, even though a single market faces a lower risk of attack than the combined two-platform market, it inefficiently invests in security to achieve its lower risk level. Hence, clients would prefer to diversify over two markets that are on aggregate riskier, as the competition in fees dominates. It is therefore important to note that in large markets, the utility-maximizing outcome is one in which there is a positive risk of cyber attacks. We illustrate client utility in the single market compared to the fragmented markets in Figure **??**.

[Figure 7 about here.]

Our model suggests that clients benefit from platform competition in both fees and cybersecurity investment. Intuitively, this follows from the fact that the client could replicate

the monopoly platform by simply allocating their entire transaction to one platform. The client would only split their transaction across both platforms if it were utility-enhancing. Thus, a client who can be seen splitting their transactions across multiple platforms must be better off than if only one platform existed.

As fee competition is important dimension for client utility, a related question is whether platforms have the incentive to circumvent this competition by consolidating into a single market platform, thereby worsening client welfare. To address this issue, suppose that the total market size Q is such that at least one platform in the fragmented market invests in security, that is, $rQ > 1+\eta$. Then, comparing the monopoly platform profit π_M to the value-weighted profits in the competitive market $\pi_C = q_H^\star \pi_H + q_L^\star \pi_L$, we arrive at the following proposition.

Proposition 6 (Consolidation) *If $rQ > 1 + \eta$, then the profit of a single platform π_M (weakly) exceeds combined platform profits in a fragmented market, π_C.*

Proposition 6 states that for any market where sufficiently large transactions lead security investment to be positive for *some market* in equilibrium, a single platform earns profits which exceed the combined profits of a two-platform market. This is similar in nature to the result of Cournot competition, in which a monopolist earns a higher profit than the combined profits of two Cournot competitors. Proposition 6 suggests that there exists a contract that stipulates an allocation of profits between the more-sophisticated and less-sophisticated platform such that consolidation into a single-platform would be (weakly) beneficial to both platforms (i.e., an allocation in the "core"). The potential existence of such a contract creates concerns for client welfare, as clients (weakly) prefer a fragmented platform market for any market size (Proposition 5). We illustrate the profits to the single platform compared to the fragmented platforms in Figure **??**.

[Figure 8 about here.]

5 Testable Implications and Policy

5.1 Testable Implications

In the market for cybersecurity, our results on client welfare (Propositions 5) and consolidation (6) underscore a principal-agent problem problem: clients that entrust institutions with their assets to perform a service for a fee, with the expectation that institutions will provide that service efficiently. Institutions, however, have the incentive to consolidate—through a merger or acquisition—into larger institutions that allow for greater rent extraction under the guise of greater client protection. Proposition 3 and 4 provide the intuition that monopolistic institutions will (optimally) invest more resources into security relative to what would be achieved in a (duopolostic) competitive environment, leading to lower attack vulnerability in sufficiently large markets, but higher average fees. We summarize this intuition in the following testable implications.

Testable Implication 1 (Vulnerability to Attacks) *Large markets with a dominant (monopolist) institution will experience fewer security events, on average, relative to large markets with competition.*

Testable Implication 2 (Competition in Fees) *Markets with a dominant (monopolist) institution will charge higher fees for security relative to markets with competition. Moreover, in a market with very similar markets (e.g., higher η), the fee differential between monopolistic and competitive markets will be larger.*

It is not novel that monopolists extract higher rents from clients relative to competitive markets such that clients experience lower welfare, even while providing a "higher quality" product. What makes this result important from a policy context, however, is that the the product in question is asset security, providing an argument against the break-up of large institutions in markets where security is a concern. While it is generally true for relatively large markets that single platform markets are more secure (Proposition 4), we suggest that

monopolistic providers of enhanced security do not compensate clients for the reduction in fee competition, and that governments should be wary of arguments to consolidate for security reasons.

5.2 Regulation and Breaking up Consolidated Platforms

Regulators face a dilemma when considering the breaking up large institutions. Client utility is unambiguously higher when dealing with two fragmented venues; however, large consolidated institutions may have lower system vulnerability. Thus, a regulator who wishes to break up a large venue may find it politically nonviable to propose such an action, despite the fact that clients are better off.

To improve upon the monopoly system through fragmentation, while maintaining the level of system-wide security, we posit that a regulator might use something of a "maximum breach probability requirement"—similar in notion to minimum capital requirements at lending institutions. By requiring venues that result from the break up of a monopoly to maintain a certain level of security, the regulator could prevents all equilibria in which the fragmented venues are riskier than the consolidated venue. In such a scenario, the regulator would require that the resulting two fragmented venues be necessarily as safe (or safer) than the monopolist. As it may be difficult to measure such a requirement in terms of probability, we note that security investment s in our model correlates with vulnerability $\delta(s)$, and hence this requirement could be framed in terms of minimum security investment.

Proposition 7 (Competition and Minimum Security Expenditure) *Suppose a regulator exogenously sets a minimum $\tilde{s}$ such that $\delta_C > \delta_M$. Then for all $\eta \geq 0$, there exist $q_L^\star$, $q_H^\star$, $f_M \leq f_L^\star \leq f_H^\star$ such that $\delta_C < \delta_M$ and the client earns (at least weakly) higher utility in a fragmented platform market versus a single platform market.*

Proposition 7 shows that there exist a level of security investment such that the fragmented market achieves a breach probability that is lower than the monopolist, at weakly

lower fees, implying that the client is better off than they were under the monopolist. Thus, through certain mandates on security investment, it is possible for a regulator to break up a large platform, while maintaining or reducing the rate of security breaches, leading to an improvement client utility. It is important to note that this second intervention beyond the break up of the monopolist platform, is is only necessary in the case of a sufficiently large market, or when breaking up the monopolist yields institutions with a wide dispersion in sophistication, η (Proposition 4). Otherwise, the default equilibrium with two platforms exhibits lower vulnerability without any further intervention.

6 Conclusion

We construct a strategic model in which clients wish to conduct financial transactions, but face the risk of a cyber attack. We contribute to the cyber crime literature by expanding beyond the infrastructure-focused problem to the agency relationship between infrastructure providers and their clients. In our model, clients pay fees to a financial infrastructure provider, which then invests in security to secure itself against cyber attacks. In the event of a security breach, the client and the platform both suffer losses from the failed transaction: the client loses (some or all) of their asset, and the platform forgoes their fee.

We compare a single venue equilibrium to a fragmented market with competition, in which clients have the choice between two competing venues. In equilibrium, clients derive utility gains from spreading their transaction across multiple venues, as they diversify their risk from cyber attacks. Moreover, the fee competition in a fragmented market leads equilibrium fees to be lower than those paid to a consolidated venue. This translates into a generally higher vulnerability of attack to fragmented markets relative to a monopoly, especially when transaction sizes are large. We show that despite this, client utility higher with platform competition, rather than a single consolidated venue. Our results suggest that monopolists

likely overinvest in security, to justify the extraction of higher rents from their users through commensurately higher fees.

A tension exists between client welfare and platform profitability, as a monopoly is always more profitable than a fragmented market. This creates a potential for venue consolidation. Hence, policymakers may improve consumer utility by breaking up infrastructure in markets with a single large venue. Policymakers should be aware, however, that this may lead to more security breaches in equilibrium, despite achieving higher consumer utility. Though a second-best for consumer utility, we show that regulators may be able to improve security post-break-up, if the two venues are regulated to remain at least as safe as the monopolist through a minimum security investment requirement. In equilibrium, such a policy results in higher client utility than the monopoly itself, with no increased risk to assets.

References

Acemoglu, Daron, Azarakhsh Malekian, and Asu Ozdaglar, 2016, Network security and contagion, *Journal of Economic Theory* 166, 536–585.

Anderson, Ross, 2001, Why information security is hard-an economic perspective, in *Proceedings 17th Annual Computer Security Applications Conference (ACSAC), 2001.* pp. 358–365. IEEE.

——— , Chris Barton, Rainer Böhme, Richard Clayton, Michel JG Van Eeten, Michael Levi, Tyler Moore, and Stefan Savage, 2013, Measuring the cost of cybercrime, in *The economics of information security and privacy* pp. 265–300.

Anderson, Ross, and Tyler Moore, 2006, The economics of information security, *Science* 314, 610–613.

Becker, Gary S., 1968, Crime and punishment: An economic approach, *Journal of Political Economy* 76, 169–217.

Biais, Bruno, Thierry Foucault, and Sophie Moinas, 2015, Equilibrium fast trading, *Journal of Financial Economics* 116, 292–313.

Biancotti, Claudia, 2017, The price of cyber (in) security: evidence from the italian private sector, *SSRN Working Paper 3082195*.

Bier, Vicki, Santiago Oliveros, and Larry Samuelson, 2007, Choosing what to protect: Strategic defensive allocation against an unknown attacker, *Journal of Public Economic Theory* 9, 563–587.

Brolley, Michael, and David A Cimon, 2020 (forthcoming), Order flow segmentation, liquidity and price discovery: The role of latency delays, *Journal of Financial and Quantitative Analysis*.

Budish, Eric, Peter Cramton, and John Shim, 2015, The high-frequency trading arms race: Frequent batch auctions as a market design response, *Quarterly Journal of Economics* 130, 1547–1621.

Chao, Yong, Chen Yao, and Mao Ye, 2016, What drives price dispersion and market fragmentation across us stock exchanges?, *SSRN Working Paper 2530572*.

Colliard, Jean-Edouard, and Thierry Foucault, 2012, Trading fees and efficiency in limit order markets, *Review of Financial Studies* 25, 3389–3421.

Dynes, Scott, Eric Goetz, and Michael Freeman, 2007, Cyber security: Are economic incentives adequate?, in *International Conference on Critical Infrastructure Protection* pp. 15–27.

Dziubiński, Marcin, and Sanjeev Goyal, 2013, Network design and defence, *Games and Economic Behavior* 79, 30–43.

Farhang, Sadegh, and Jens Grossklags, 2017, When to invest in security? empirical evidence and a game-theoretic approach for time-based security, *arXiv preprint arXiv:1706.00302*.

Gordon, Lawrence A, and Martin P Loeb, 2002, The economics of information security investment, *ACM Transactions on Information and System Security (TISSEC)* 5, 438–457.

Goyal, Sanjeev, and Adrien Vigier, 2010, Robust networks, .

Gueye, Assane, and Vladimir Marbukh, 2012, A game-theoretic framework for network security vulnerability assessment and mitigation, in *International Conference on Decision and Game Theory for Security* pp. 186–200.

Hoyer, Britta, and Kris de Jaegher, 2016, Strategic network disruption and defense, *Journal of Public Economic Theory* 18, 802–830.

Kovenock, Dan, and Brian Roberson, 2018, The optimal defense of networks of targets, *Economic Inquiry* 56, 2195–2211.

Malinova, Katya, and Andreas Park, 2015, Subsidizing liquidity: The impact of make/take fees on market quality, *Journal of Finance* 70, 509–536.

Massacci, Fabio, Joe Swierzbinski, and Julian Williams, 2017, Cyberinsurance and public policy: Self-protection and insurance with endogenous adversaries, .

Menkveld, Albert J, and Marius A Zoican, 2017, Need for speed? Exchange latency and liquidity, *Review of Financial Studies* 30, 1188–1228.

Moore, Tyler, 2010, The economics of cybersecurity: Principles and policy options, *International Journal of Critical Infrastructure Protection* 3, 103–117.

——— , and Ross Anderson, 2011, Economics and internet security: A survey of recent analytical, empirical, and behavioral research, .

Moore, Tyler, Richard Clayton, and Ross Anderson, 2009, The economics of online crime, *Journal of Economic Perspectives* 23, 3–20.

Ozenne, Tim, 1974, The economics of bank robbery, *The Journal of Legal Studies* 3, 19–51.

Pagnotta, Emiliano S., and Thomas Philippon, 2017, Competing on speed, *SSRN Working Paper 1967156*.

Paquet-Clouston, Masarah, Bernhard Haslhofer, and Benoit Dupont, 2018, Ransomware payments in the bitcoin ecosystem, *arXiv preprint arXiv:1804.04080*.

Shkilko, Andriy, and Konstantin Sokolov, 2016, Every cloud has a silver lining: Fast trading, microwave connectivity and trading costs, *SSRN Working Paper 2848562*.

Zhu, Haoxiang, 2014, Do dark pools harm price discovery?, *The Review of Financial Studies* 27, 747–789.

A Appendix

A.1 Notation summary

Variable Subscripts	
Subscript	Definition
H	pertaining to high security endowment platform
L	pertaining to low security endowment platform
Exogenous Parameters	
Parameters	Definition
λ_i	Security endowment for platform i.
η	The security endowment at platform L relative to platform H.
Q	Total client transaction quantity.
r	Fraction of client asset stolen by hacker after a successful hack attempt.
$p(S)$	Marginal price of security investment, as a function of total investment, S.
$c_i(s_i)$	Cost function of security investment by platform i.
π_i	Profit function for platform i.
$U(Q)$	Utility function for the client who seeks to transact amount Q.
Endogenous Quantities	
Variable	Definition
f_i	Fee charged per quantity transacted at platform i.
s_i	Investment in security by platform i.
S	Total security investment by all platforms.
q_i	Quantity sent by the client to platform i for transaction.
δ_i	Probability that a hack at platform i is successful (i.e., no transaction).
a_i	Investment by the hacker to attack platform i.
M_1, M_2	Equilibrium thresholds with a monopolist platform.
$C_1, ...C_4$	Equilibrium thresholds with competitive platforms.

A.2 Proofs from Section 3

Proof (Lemma 1). We begin by evaluating $\delta_H^\star$ and $\delta_L^\star$ at the equilibrium market share values, $q_H^\star$ and $q_L^\star$ to obtain:

$$\delta_H^\star = \frac{2rQ - 4s_H^\star - (3+\eta)}{2rQ + 1 - \eta} \tag{26}$$

$$\delta_L^\star = \frac{2rQ - 4s_L^\star - (1+3\eta)}{2rQ - 1 + \eta} \tag{27}$$

Given that $s_H^\star = s_L^\star$, the numerator of $\delta_H^\star$ is less than the numerator of $\delta_L^\star$, which implies that $\delta_H^\star \to 0$ first as Q becomes small. Then, computing the equilibrium value of $s_H^\star(f_H^\star(q_H^\star), q_H^\star)$ from (20) and (21), and inputting into (26)-(27), we arrive at,

$$\delta_H^\star = \frac{4r^2Q - 6r - 4}{3r(2rQ - 1 + \eta)} \tag{28}$$

Solving for Q such that $\delta_H^\star = 0$ admits $Q = \frac{3r+2}{2r^2}$. To check that the denominator is well-defined for all $Q \geq \frac{3r+2}{2r}$, we evaluate it at $Q = \frac{3r+2}{2r}$, which yields $\frac{3r+2}{2r} - 1 - \eta > 0 \ \forall r \in [0,1]$.

Next, we solve for the value of Q such that $\delta_L^\star(Q) = 0 (= \delta_H^\star)$. At this corner, it must be that $s_H^\star = rQq_H - 1$, as the platform would not invest more than what is required for full security. Similarly, the client offers a fee $f_H^\star$ that induces the platform to invest exactly $rQq_H - 1$. The implication is that solution to the first-order condition for $s_H^\star$ in the platform's problem must be equal to $rQq_H - 1$. Thus, we have:

$$s_H^\star = \frac{2f_H - rs_L^\star}{2r} = rQq_H - 1 \iff f_H^\star = r(rQq_H - 1) + \frac{rs_L^\star}{2} \tag{29}$$

Then, we obtain the first-order condition for $s_L^\star$ and solve:

$$s_L^\star = \frac{2f_L - rs_H^\star}{2r} \iff s_L^\star = \frac{2f_L - r(rQq_H - 1)}{2r} \tag{30}$$

Inputting the solution to $f_H^\star$ into the client's problem, we derive first-order conditions:

$$\text{F.O.C}(f_L^\star): \frac{2r^2Qq_L - (1+2\eta)r - 4f_L + 2}{2r^2} = 0 \tag{31}$$

$$\text{F.O.C}(q_H^\star): \frac{Q}{2}\left(1 + 3\frac{r}{2} - Q(3q_H + q_L)r^2\right) - \Gamma \times Q = 0 \tag{32}$$

$$\text{F.O.C}(q_L^\star): \frac{Q}{2}\left(2f_L - Q(q_H + 4q_L)r^2 + (1+2\eta)rq_i\right) - \Gamma \times Q = 0 \tag{33}$$

Solving, we obtain $\left(\frac{2Qr+1-\eta}{4Qr}, 1 - q_H^\star\right)$, and $f_L^\star(q_L^\star) = \frac{2(2+r^2Q)-3(1+\eta)r}{8}$. Lastly, computing $s_L^\star(f_L^\star, q_H^\star)$ from (30) yields:

$$s_L^\star = \frac{2 - \eta r}{4r} \tag{34}$$

Evaluating $\delta_L^\star(s_L^\star)$ and solving for Q such that $\delta_L^\star(Q; s_L^\star) = 0$, we obtain:

$$\delta_L^\star = \frac{2r^2Q - (2 - \eta r) - r(1+3\eta)}{r(2rQ - 1 + \eta)} \iff Q = \frac{2 + (1+2\eta)r}{2r^2}. \tag{35}$$

Finally, $\frac{3r+2}{2r^2} > \frac{2+(1+2\eta)r}{2r^2} \iff \eta \leq 1$, which holds by construction. ■

Proof (Lemma 2). To characterize the equilibrium fee schedule, we begin by inputting the solutions to $q_L^\star$ and $q_H^\star$ from (21) into the solution for f_i in (20), which from the proof of Lemma 1 is valid for all $Q > \frac{3r+2}{2r^2}$. Simplifying yields,

$$(f_L^\star, f_H^\star) = \left(\frac{2(2+Qr^2) - 3(1+\eta)r}{8}, \frac{2(2+Qr^2) - 3(1+\eta)r}{8}\right) \tag{36}$$

which is positive $\forall Q > \frac{3(1+\eta)r-4}{2r^2} > \frac{3r+2}{2r^2}$. For $Q \in \left(\frac{2+(1+2\eta)r}{2r^2}, \frac{3r+2}{2r^2}\right]$, we obtain $f_L^\star$ and $(q_H^\star, q_L^\star)$ directly from the proof of Lemma 1. Moreover, we compute $f_H^\star$ by inputting $s_L^\star$ and $q_H^\star$ from the proof of Lemma 1 into the equilibrium condition $s_H^\star(f_H^\star, s_L^\star) = rQq_H - 1$ obtained by the fact that $\delta_H^\star = 0$. Solving yields,

$$f_H^\star = r\left(rQ\left(\frac{2Qr + (1-\eta)}{4Qr}\right) - 1\right) + \frac{r(2-\eta r)}{8r} = \frac{2(1+2Qr^2) - 3(2+\eta)r}{8} \tag{37}$$

Now, let $Q < \frac{2+(1+2\eta)r}{2r^2}$, which implies that $\delta_H^\star = \delta_L^\star = 0$. Further, it must be that $s_H^\star = \max\{rQq_H^\star - 1, 0\}$ and $s_L^\star = \max\{rQq_L^\star - \eta, 0\}$. Similarly to the previous case, we can use the condition $s_i^\star(f_i, s_{-i}) = rQq_i - \lambda_i$ to obtain the solution for f_i, $i \in \{H, L\}$.

$$(s_L^\star, s_H^\star) : \left(\frac{2f_L^\star - \eta r s_H^\star}{2r}, \frac{2f_L^\star - \eta r s_L^\star}{2r}\right) = (rQq_L^\star - \eta, rQq_H^\star - 1) \tag{38}$$

$$\iff (f_L^\star, f_H^\star) = \left(\frac{r(rQ(2q_L^\star + q_H^\star) - (1+2\eta)}{2}, \frac{r(rQ(2q_H^\star + q_L^\star) - (2+\eta)}{2}\right) \tag{39}$$

Finally, we solve for $(q_L^\star, q_H^\star)$ by solving the client's utility maximization problem in (17), for $\delta_H^\star = \delta_L^\star = 0$ and $(f_L^\star, f_H^\star)$ as in (39). Taking first-order conditions and solving, we obtain:

$$(q_L^\star, q_H^\star) = \left(\frac{2Qr + (1-\eta)}{4Qr}, \frac{2Qr - (1-\eta)}{4Qr}, \right), \tag{40}$$

which, following substitution, yields $(f_L^\star, f_H^\star)$:

$$(f_L^\star, f_H^\star) = \left(\frac{r(6rQ - 7\eta - 5)}{8}, \frac{r(6rQ - 5\eta - 7)}{8}\right). \tag{41}$$

Equation (41) holds only for $f_L^\star > 0$ and $f_H^\star > 0$. As $\eta \in [0, 1]$, it must be that $f_L^\star \geq f_H^\star$ and $f_H^\star \to 0$ before $f_L^\star$. However, $f_H^\star = 0 \iff Q = \frac{5\eta+7}{6r} < \frac{3+\eta}{2r} = Q(s_H^\star = 0)$ implying that $s_H^\star(Q) \to 0 \Rightarrow f_H^\star \to \epsilon > 0$. Hence, at $s_H^\star = 0$, $f_H^\star$ falls (discontinuously) to zero. Thus, $\forall Q \in \left(\frac{3+\eta}{2r}, \frac{2+(1+2\eta)r}{2r^2}\right]$, $(f_L^\star, f_H^\star)$ is as in (41).

Last, we examine the case of $\delta_L^\star = \delta_H^\star = f_H^\star = s_H^\star = 0$. We use the equilibrium condition for $s_H^\star$ to solve for $q_H^\star$:

$$s_H^\star = rQq_H^\star - 1 = 0 \iff (q_H^\star, q_L^\star) = \left(\frac{1}{rQ}, \frac{rQ-1}{rQ}\right), \tag{42}$$

Hence, the piece-wise equation (24) of Lemma 2 is complete. Moreover, a zero security investment confirms a $f_H^\star = 0$. As $s_L^\star = rQq_L^\star - \eta$, we must have:

$$s_L^\star = \frac{2f_L^\star - r s_H^\star}{2r} = rQq_L^\star - \eta \iff f_L^\star = r(rQ - 1 - \eta) \tag{43}$$

Thus, we arrive at equation (23) of Lemma 2, completing the proof. ■

A.3 Proofs from Section 4

Proof (Proposition 3). We prove this proposition in two steps. First, we show that $f_H^\star = f_L^\star$, and that $f_H^\star$ is decreasing in η. From inspection of Equation (23) of Lemma 2, we see that all coefficients of η are negative, implying that $f_H^\star$ and $f_L^\star$ both decrease in η. Moreover, Lemma 2 provides, by inspection, that for all $Q > \frac{3r+2}{2r^2}$, $f_L^\star = f_H^\star$ and for $Q \leq \frac{2+(1+2\eta)r}{2r^2}$ that $f_L^\star \geq f_H^\star$. By computing $f_L^\star - f_H^\star$ on $Q \in (\frac{2+(1+2\eta)r}{2r^2}, \frac{3r+2}{2r^2}]$, we arrive at:

$$f_L^\star - f_H^\star = \frac{2(1-Qr^2)+3r}{8}, \tag{44}$$

which is zero for $Q = \frac{3r+2}{2r^2}$, and positive for any lower Q in the range. Thus, $f_L^\star \geq f_H^\star$.

To show that $f_M^\star \geq f_C^\star$, where M denotes the single platform case and C denotes volume-weighted fees from the competition case, we compute the differences across all regions, defined by the ordering of M_j. $j \in \{1,2\}$ and C_k. $k \in \{1,2,3,4\}$. First, assume that $\eta < 1/2$. Then, it must be that the thresholds in Q that partition f_M and f_C satisfy $M_1 < C_1 < C_2 < C_3 < M_2 < C_4$, as $M_2 = \frac{1+r}{r^2} > \frac{2+(1+2\eta)r}{2r^2} = C_3 \iff \frac{1-2\eta}{2r} > 0$. Next, we show that the function, $f_M - f_C$ given by the difference of equations (11) and (23), must be increasing in Q on all intervals of Q. First, examine the case where $\eta < 1/2$.

$$\frac{\partial}{\partial Q}(f_M - q_H^\star f_H^\star - q_L^\star f_L^\star; \eta < 1/2) = \begin{cases} (1+\eta)Q^{-2} & C_1 < Q \leq C_2 \\ \frac{4(Qr)^2-(1-\eta)^2}{16Q^2} & C_2 < Q \leq C_3 \\ \frac{20Q^2r^3-3r(1-\eta)-2(1-\eta)}{32Q^2(1+r)} & C_3 < Q \leq M_2 \\ \frac{4Q^2r^3-3r(1-\eta)-2(1-\eta)}{32Q^2(1+r)} & M_2 < Q \leq C_4 \\ r^2/4 & Q > C_4 \end{cases} \tag{45}$$

The function $\frac{\partial}{\partial Q}(f_M - q_H^\star f_H^\star - q_L^\star f_L^\star)$ is positive for all Q by inspection, except the interval $M_2 < Q \leq C_4$. Note that the lowest value in the range, $Q = M_2 = \frac{1+r}{r^2} > 2/r$, and thus, because $rQ > 1+\eta$, it must be that the numerator is positive. Next, note that the function for $\frac{\partial}{\partial Q}(f_M - q_H^\star f_H^\star - q_L^\star f_L^\star)$ when $\eta < 1/2$ is identical for the interval $Q \in [M_1, C_2] \bigcup [C_4, \infty)$.

For $Q \in [C_2, C_4]$, the intervals change to $[C_2, M_2]$, $[M_2, C_3]$, and $[C_3, M_4]$. Because the results for $[C_2, M_2]$ and $[M_2, C_4]$ should be the same as $[C_2, C_3]$ and $[C_3, C_4]$ above for all Q, we only require reevaluating the function $f_M - q_H^\star f_H^\star - q_L^\star f_L^\star$ for $[M_2, C_3]$.

$$\frac{\partial}{\partial Q}(f_M - q_H^\star f_H^\star - q_L^\star f_L^\star; \eta \geq 1/2) = -\frac{4(Qr)^2 + (1-\eta)^2}{16Q^2}, \; M_2 < Q \leq C_3 \tag{46}$$

Equation (46) is negative, implying that for this interval, we need to evaluate the difference function at the upper-bound Q of C_3 instead.

With the previously computed derivatives, we can now prove the proposition by evaluating each region of $f_M - f_C$ at the Q lower bound of the region. First assume that $\eta < 1/2$:

$$f_M - q_H^\star f_H^\star - q_L^\star f_L^\star = \begin{cases} r\eta & Q = C_1 \\ \frac{(1+5\eta+2\eta^2)r}{2(3+\eta)} & Q = C_2 \\ \frac{4+20\eta r+4\eta r^2+17\eta^2 r^2}{8(2+r+2\eta r)} & Q = C_3 \\ \frac{8+(7+11\eta)r^2}{32(1+r)} & Q = M_2 \\ \frac{2+(2+3\eta)r}{8} & Q = C_4 \end{cases} \tag{47}$$

By inspection, equation (47) is positive for all $rQ \geq 1$, which we assume to hold. Now, assume that $\eta \geq 1/2$, implying that the thresholds in Q that partition f_M and f_C satisfy $M_1 < C_1 < C_2 < M_2 < C_3 < C_4$. Evaluating at the lower bounds of each region,

$$f_M - q_H^\star f_H^\star - q_L^\star f_L^\star = \begin{cases} r\eta & Q = C_1 \\ \frac{(1+5\eta+2\eta^2)r}{2(3+\eta)} & Q = C_2 \\ \frac{4+4(1+3\eta)+(2+4\eta+9\eta^2)r^2}{8(2+(1+2\eta)r)} & Q = C_3^- \\ \frac{4+4(1+3\eta)r+(2+4\eta+9\eta^2)r^2}{8(2+(1+2\eta)r} & Q = C_3 \\ \frac{2+(2+3\eta)r}{8} & Q = C_4 \end{cases} \tag{48}$$

where equation (47) is positive for all $rQ \geq 1$, which we assume to hold. Note that because of the derivative of (48) being negative on $[M_2, C_3]$, we evaluate it at C_3 (denoted C_3^- in the above function). As the function is positive here, it must be positive for all values in the range $[M_2, C_3]$. ■

Proof (Proposition 4). Let the parameters of the model satisfy Proposition 2. To compare aggregate security investment under the single and fragmented platform environments, we compute the weighted differences $S_M - S_C$ across all regions as in the proof of Proposition 3, where $S_C = q_H^\star s_H^\star + q_L^\star s_L^\star$. First, assume that $\eta < 1/2$. Then, it must be that the thresholds in Q that partition S_M and S_C satisfy $M_1 < C_1 < C_2 < C_3 < M_2 < C_4$.

Next, we show that the function, $S_M - S_C$ must be increasing in Q on all intervals of Q. First, examine the case where $\eta < 1/2$.

$$\frac{\partial}{\partial Q}(S_M - S_C; \eta < 1/2) = \begin{cases} (1+\eta)/(rQ^2) & C_1 < Q \leq C_2 \\ \frac{4(Qr)^2-(1-\eta)^2}{16Q^2} & C_2 < Q \leq C_3 \\ \frac{4(Qr^2)^2+20Q^2r^3-(3-2\eta-\eta^2)r^2-r(3-4\eta+\eta^2)-4(1-\eta)}{32(rQ)^2} & C_3 < Q \leq M_2 \\ \frac{4(Qr^2)^2+4Q^2r^3-(3-2\eta-\eta^2)r^2-r(3-4\eta+\eta^2)-4(1-\eta)}{32(rQ)^2} & M_2 < Q \leq C_4 \\ r/3 & Q > C_4 \end{cases} \quad (49)$$

The function $\frac{\partial}{\partial Q}(S_M - S_C)$ is positive for all Q by inspection, except the interval $M_2 < Q \leq C_4$. Note that the lowest value in the range, $Q = M_2 = \frac{1+r}{r^2} > 2/r$, and thus, because $rQ > 1 + \eta$, it must be that the numerator is positive. Next, note that the function for $\frac{\partial}{\partial Q}(S_M - S_C)$ when $\eta < 1/2$ is identical for the interval $Q \in [M_1, C_2] \bigcup [C_4, \infty)$. For $Q \in [C_2, C_4]$, the intervals change to $[C_2, M_2]$, $[M_2, C_3]$, and $[C_3, M_4]$. Because the results for $[C_2, M_2]$ and $[M_2, C_4]$ should be the same as $[C_2, C_3]$ and $[C_3, C_4]$ above for all Q, we only require reevaluating the function for $[M_2, C_3]$.

$$\frac{\partial}{\partial Q}(S_M - S_C; \eta \geq 1/2) = -\frac{(1-\eta)^2}{8Q^2 r}, \; M_2 < Q \leq C_3 \quad (50)$$

Equation (50) is negative, implying that for this interval, we need to evaluate the difference function at the upper-bound Q of C_3 instead.

Thus, we can prove the proposition by evaluating each region of $S_M - S_C$ at the Q lower bound of the region:

$$S_M - S_C = \begin{cases} \eta & Q = C_1 \\ \frac{(1+\eta)^2}{3+\eta} & Q = C_2 \\ \frac{(2+3r\eta)(6+(4+11\eta)r-(2-\eta)r^2)}{16r(2+(1+2\eta)r)} & Q = C_3 \\ \frac{(2+(1+\eta)r)(6+(9+\eta)r-(1+\eta)r^2)}{32r(1+r)} & Q = M_2 \\ \frac{2+(1+\eta)r}{4r} & Q = C_4 \end{cases} \tag{51}$$

By inspection, equation (47) is positive for all $rQ \geq 1$, which we assume to hold. Now, assume that $\eta \geq 1/2$, implying that the thresholds in Q that partition S_M and S_C satisfy $M_1 < C_1 < C_2 < M_2 < C_3 < C_4$. By inspection, we see that, for all Q, $S_M - S_C$ given by the difference of equations (11) and (23) is increasing in Q. Thus, we can prove the proposition by evaluating each region of $S_M - S_C$ at the Q lower bound of the region:

$$S_M - S_C = \begin{cases} \eta & Q = C_1 \\ \frac{(1+\eta)^2}{3+\eta} & Q = C_2 \\ \frac{4(1+r)+8r\eta+3r^2\eta(2+\eta)}{r^2} & Q = C_3^- \\ \frac{12+8(2+3\eta)r+((6+17\eta)+(8-6r)+\eta r)\eta r^2}{16r(2+(1+2\eta)r)} & Q = C_3 \\ \frac{2+(1+\eta)r}{4r} & Q = C_4 \end{cases} \tag{52}$$

where equation (47) is positive for all $rQ \geq 1$, which we assume to hold.

Similarly, we compare vulnerability under the single and fragmented platform environments, δ_M and δ_C, respectively, by computing $\delta_M^* - \delta_C$ within each of the regions. Suppose $\eta < 1/2$ which implies that $M_1 < C_1 < C_2 < C_3 < M_2 < C_4$. First, note that for any

$Q \leq C_3 < M_2$, $\delta_M = \delta_H^\star = \delta_L^\star = 0$, thus we need only check $Q > C_3$. Computing, we obtain:

$$\delta_M - \delta_C = \begin{cases} \frac{-Qr^2+(2+r+2r\eta)}{2Qr^2} & C_3 < Q \leq M_2 \\ \frac{2\eta-1}{4rQ} & M_2 < Q \leq C_4 \\ \frac{-Qr^2+1+3r\eta}{6Qr^2} & Q > C_4 \end{cases} \tag{53}$$

which, evaluated at the lowest bounds of the region, we see that $\delta_M - \delta_C$ evaluated at $Q = C_4$ simplifies to $\frac{r(2\eta-1)}{2(2+3r)} < 0$ given $\eta < 1/2$. Thus, $\delta_M - \delta_C > 0$ for all $Q > C_4$. Further, $\delta_M - \delta_C = 0$ when evaluated at $Q = C_3$, implying that $\delta_M - \delta_C < 0$ for any $Q \in (C_3, M_2]$.

Suppose that $\eta \geq 1/2$, and thus, $M_1 < C_1 < C_2 < M_2 < C_3 < C_4$. Because $\delta_M = \delta_H^\star = \delta_L^\star = 0$ for any $Q \leq M_2 < C_3$, we need only check $Q > M_2$. Computing $\delta_M - \delta_C$:

$$\delta_M - \delta_C = \begin{cases} \frac{Qr^2-(1+r)}{2Qr^2} & M_2 < Q \leq C_3 \\ \frac{2\eta-1}{4rQ} & C_3 < Q \leq C_4 \\ \frac{-Qr^2+1+3r\eta}{6Qr^2} & Q > C_4 \end{cases} \tag{54}$$

Similarly, $\delta_M - \delta_C = 0$ when evaluated at $Q = M_2$, implying that $\delta_M - \delta_C \geq 0$ for all $Q \in (M_2, C_3]$, and all $Q \in (C_3, C_4]$ given $\eta \geq 1/2$. Finally, at $Q = C_4$, $\delta_M - \delta_C \geq 0$ for any $\eta \geq 1/2$, unless $Q \geq \frac{1+3r\eta}{r^2}$. ■

Proof (Proposition 5). To show that the client utility function in the competition case U_C is always (weakly) greater than in the monopoly case, U_M, we proceed similarly to the proof of Proposition 3, by taking the difference of these utility functions, and showing three things: i) the derivative of the difference in Q is negative, and ii) when evaluated at the lower bounds of the equilibrium regions, this difference is positive for all η.

First, we show that the function, $U_M - U_C$ must be increasing in Q on all intervals of Q. Let $\eta < 1/2$. Then we have:

$$\frac{\partial}{\partial Q}(U_M - U_C; \eta < 1/2) = \begin{cases} -(1+\eta)r & C_1 < Q \leq C_2 \\ -\frac{r(2rQ+3\eta-1)}{4} & C_2 < Q \leq C_3 \\ -\frac{(16Q+2Q(1-r)+1-2\eta)r^2-(11-6\eta)r-6}{16} & C_3 < Q \leq M_2 \\ -\frac{2+(2Q(1-r)+8Q+1-2\eta)r^2+3(1-2\eta)r}{16} & M_2 < Q \leq C_4 \\ -\frac{8Qr^2-2-3(1-\eta)r}{12} & Q > C_4 \end{cases} \tag{55}$$

The function $\frac{\partial}{\partial Q}(U_M - U_C)$ is negative $\forall Q$, except the interval $(C_3, M_2]$. Note that the lowest value in the range, $Q = C_3 = \frac{2+r(1+2\eta)}{2r^2}r$. Evaluating at this value yields,

$$\frac{\partial}{\partial Q}(U_M - U_C; \eta < 1/2, Q = C_3) = -\frac{3 - r(1-6\eta) - \eta r^2}{4} < 0 \tag{56}$$

and thus, because $rQ > 1 + \eta$, it must be that the numerator of (55) is negative for all Q. Next, note that the function for $\frac{\partial}{\partial Q}(U_M - U_C)$ when $\eta < 1/2$ is identical for the interval $Q \in [M_1, C_2] \bigcup [C_4, \infty)$. For $Q \in [C_2, C_4]$, the intervals change to $[C_2, M_2]$, $[M_2, C_3]$, and $[C_3, M_4]$. Because the results for $[C_2, M_2]$ and $[M_2, C_4]$ are the same on $[C_2, C_3]$ and $[C_3, C_4]$ above for all Q, we only require reevaluating the function for $[M_2, C_3]$.

$$\frac{\partial}{\partial Q}(U_M - U_C; \eta \geq 1/2) = -\frac{2 + (1+3\eta)r}{4}, \ M_2 < Q \leq C_3 \tag{57}$$

Equation (57) is negative, which is what we sought to show.

Part ii) is given by the difference function, evaluated at the lower bounds of the equilibrium regions, first for the case where $\eta \leq 1/2$:

$$U_M - U_C = \begin{cases} -(1+\eta) \times \eta & Q = C_1 \\ -\frac{1+5\eta+2\eta^2}{4} & Q = C_2 \\ -\frac{4+20\eta r+(4\eta+17\eta^2)r^2}{16r^2} & Q = C_3 \\ -\frac{4+4(1+3\eta)r+(2+6\eta+5\eta^2)r^2}{16r^2} & Q = M_2 \\ -\frac{4+4(2+3\eta)r+(7+8\eta+5\eta^2)r^2}{16r^2} & Q = C_4 \end{cases} \tag{58}$$

Now, let $\eta > 1/2$.

$$U_M - U_C = \begin{cases} -(1+\eta) \times \eta & Q = C_1 \\ -\frac{1+5\eta+2\eta^2}{4} & Q = C_2 \\ -\frac{4+4(1+3\eta)r+(1+10\eta+\eta^2)r^2}{16r^2} & Q = M_2 \\ -\frac{4+20\eta r+(13\eta^2+8\eta-1)r^2}{16r^2} & Q = C_3 \\ -\frac{4+4(2+3\eta)r+(7+8\eta+5\eta^2)r^2}{16r^2} & Q = C_4 \end{cases} \tag{59}$$

Then, the differences in the above utility functions are decreasing in Q and non-positive for all Q, which completes the proof. ■

Proof (Proposition 6). To show that institutions in the fragmented market environment have the incentive to consolidate into a monopolist, we compare the sum of platform profit in the fragmented market $\pi_H + \pi_L$ to the monopolist profit π_M. The logic here is that if the monopolist platform profit exceeds the sum of fragmented platform profits, then there exists a revenue-sharing contract across the two platforms such that consolidating leaves each platform ex-post better off.

First, we show that the function, $\pi_M - \pi_C$, must be increasing in Q on all intervals of Q. Let $\eta < 1/2$. Then we have:

$$\frac{\partial}{\partial Q}(\pi_M - \pi_C; \eta < 1/2) = \begin{cases} r & C_1 < Q \leq C_2 \\ \frac{r(2rQ+\eta-1)}{4} & C_2 < Q \leq C_3 \\ \frac{2r(Qr^3-(\eta+8Q+3)r^2+(2\eta+15Q+6)r-(7\eta+5)r)}{32} & C_3 < Q \leq M_2 \\ \frac{8+2Qr^4-r(5+7\eta-r(4\eta+6Q+12)+(3+8Q+\eta)r^2}{16} & M_2 < Q \leq C_4 \\ \frac{7Qr^2+5+5(1-2\eta)r}{36} & Q > C_4 \end{cases} \tag{60}$$

The function $\frac{\partial}{\partial Q}(\pi_M - \pi_C)$ is positive for all Q by inspection, except the interval $C_3 < Q \leq C_4$. As the value of the derivative in each interval has positive Q coefficients, by evaluating the derivative that the lowest value in each interval, we can show that at its lowest point, the derivative is positive. Evaluating at each lower bound yields,

$$\frac{\partial}{\partial Q}(\pi_M - \pi_C; \eta < 1/2, Q = C_3) = \frac{7(2-(1+\eta)r) + r^2((6+4\eta)-(1+\eta)r)}{32} > 0$$
$$\frac{\partial}{\partial Q}(\pi_M - \pi_C; \eta < 1/2, Q = M_2) = \frac{30-(6-23\eta)r + r^2(10-4\eta-(1+\eta)r)}{32} > 0$$

Thus, must be that the numerator of (60) is positive for all Q. Next, note that the function for $\frac{\partial}{\partial Q}(\pi_M - \pi_C)$ when $\eta < 1/2$ is identical for the interval $Q \in [M_1, C_2] \bigcup [C_4, \infty)$. For $Q \in [C_2, C_4]$, the intervals change to $[C_2, M_2]$, $[M_2, C_3]$, and $[C_3, M_4]$. Because the results for $[C_2, M_2]$ and $[M_2, C_4]$ are the same on $[C_2, C_3]$ and $[C_3, C_4]$ above for all Q, we only require reevaluating the function for $[M_2, C_3]$.

$$\frac{\partial}{\partial Q}(\pi_M - \pi_C; \eta \geq 1/2) = \begin{cases} \frac{1-\eta r-r^2 Q}{4} & M_2 < Q \leq C_3 \end{cases} \tag{61}$$

Equation (57) is negative, implying that we need to evaluate this region at the upper-bound in the next section of the proof.

Similarly to the proof of Proposition 3, by taking the difference of the monopolist and total fragmented market profit functions, evaluated at their equilibrium values, and show that this difference is positive for all η.

Consider first, the case where $\eta \leq 1/2$:

$$\pi_M - \pi_C = \begin{cases} \frac{(2+\eta)\eta}{2} & Q = C_1 \\ \frac{1+3\eta+2\eta^2}{4} & Q = C_2 \\ \frac{68-(64+12\eta)r+(108+44\eta+25\eta^2)r^2-(30-20\eta+2\eta^2)r^3+(2-\eta)^2r^4}{128r^2} & Q = C_3 \\ \frac{4+4(1-\eta)r+(1+10\eta+9\eta^2)r^2}{16^2} & Q = M_2 \\ \frac{8+r^2(9+12\eta+10\eta^2)+16(1-\eta)r}{32r^2} & Q = C_4 \end{cases} \tag{62}$$

Now let $\eta > 1/2$.

$$\pi_M - \pi_C = \begin{cases} \frac{(2+\eta)\eta}{2} & Q = C_1 \\ \frac{1+3\eta+2\eta^2}{4} & Q = C_2 \\ \frac{68-(100\eta+20)r+(69+110\eta+49\eta^2)r^2-10(1+\eta)^2r^3+(1+\eta)^2r^4}{128r^2} & Q = C_3 \\ \frac{68-(96-52\eta)r+(88+60\eta+73\eta^2)r^2-(30-20\eta+2\eta^2)r^3+(2-\eta)^2r^4}{128r^2} & Q = C_3 \\ \frac{8+r^2(9+12\eta+10\eta^2)+16(1-\eta)r}{32r^2} & Q = C_4 \end{cases} \tag{63}$$

Thus, both functions (62) and (63) are increasing in Q and positive at the lower bounds of each region, which we can achieve by graphical representation of any of the numerators in (r, η)-space. Thus, this completes the proof. ■

Proof (Proposition 7). We prove that we can achieve $\delta_M \geq q_H^\star \delta_H^\star + q_L^\star \delta_L^\star$ while maintaining $U_C \geq U_M$ when breaking up a monopolist into platform H and platform L. We prove by example. If $\delta_M \geq q_H^\star \delta_H^\star + q_L^\star \delta_L^\star$ in equilibrium, we are done. Instead, suppose that Q and η are such that $\delta_M < q_H^\star \delta_H^\star + q_L^\star \delta_L^\star$. Then, consider the (post-break-up) fragmented case where the client chooses to offer $f^\star = f_M$ for both platform H and platform L. In this case,

$(s_H^\star, s_L^\star) = \left(\frac{2f_M}{3r}, \frac{2f_M}{3r}\right)$. Then, we have that,

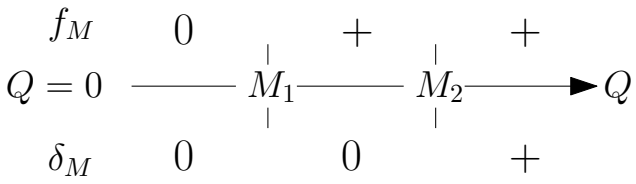
$$\delta_M > q_H^\star \delta_H^\star + q_L^\star \delta_L^\star \tag{64}$$

$$1 - \frac{1 + \frac{f_M}{r}}{rQ} > q_H^\star \times \left(1 - \frac{1 + \frac{2f_M}{3r}}{rQq_H^\star}\right) + q_L^\star \times \left(1 - \frac{\eta + \frac{2f_M}{3r}}{rQq_L^\star}\right) \tag{65}$$

$$\Rightarrow 1 - \frac{1 + \frac{f_M}{r}}{rQ} > 1 - \frac{1 + \eta + \frac{4f_M}{3r}}{rQ} \tag{66}$$

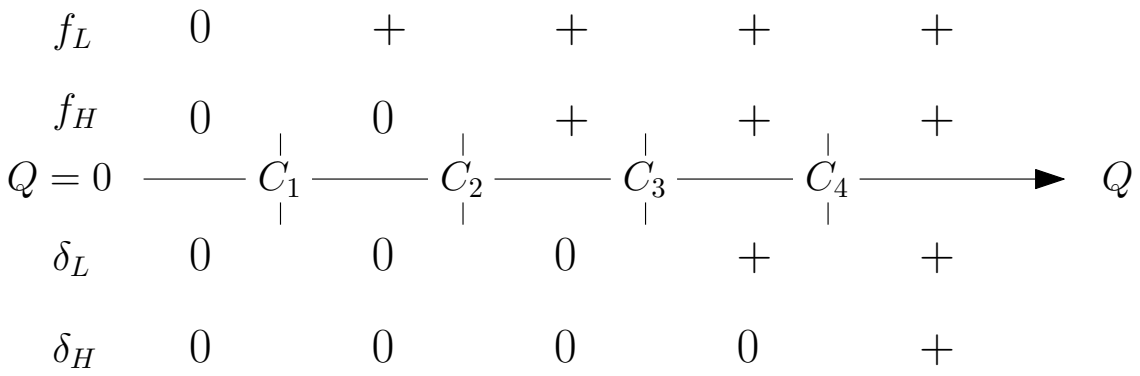
which holds for all $\eta \in [0, 1]$ and $q_H^\star \in (0, 1)$. If, instead, $s_i^\star = \frac{2f_M}{3r} \Rightarrow \delta_i = 0$, then the above holds for $q_i = 1$. Thus, a regulator setting $\tilde{s} = \frac{2f_M}{3r}$ will induce the above outcome. ■

Figure 1: Equilibrium in the monopoly case



This figure represents the equilibrium in the monopoly case. For $Q < M_1$, the client pays the venue no fee and the venue invests in no additional security. However, the transaction is small enough such that the attacker does not attack. For $M_1 \leq Q \leq M_2$, the client pays a fee that induces the venue to invest in additional security such that the attacker does not attack. For $M_2 \leq Q$, the client pays the venue a fee and the venue invests in additional security. However, the security investment is not sufficient to fully deter the attacker, and a successful attack occurs with positive probability.

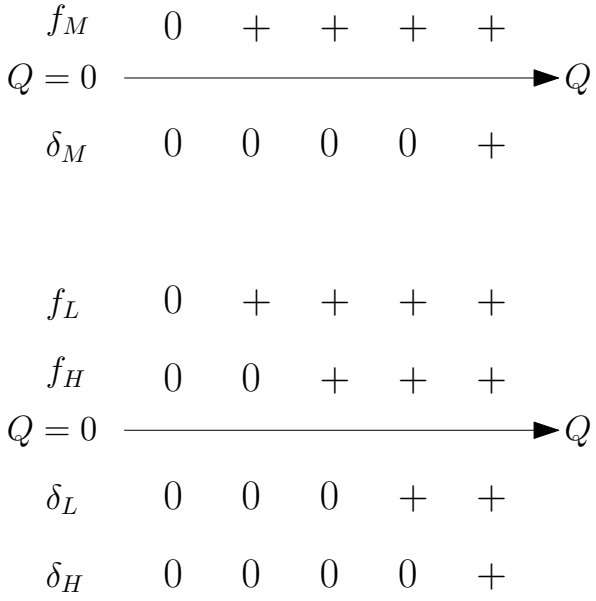
Figure 2: Equilibrium in the competitive case



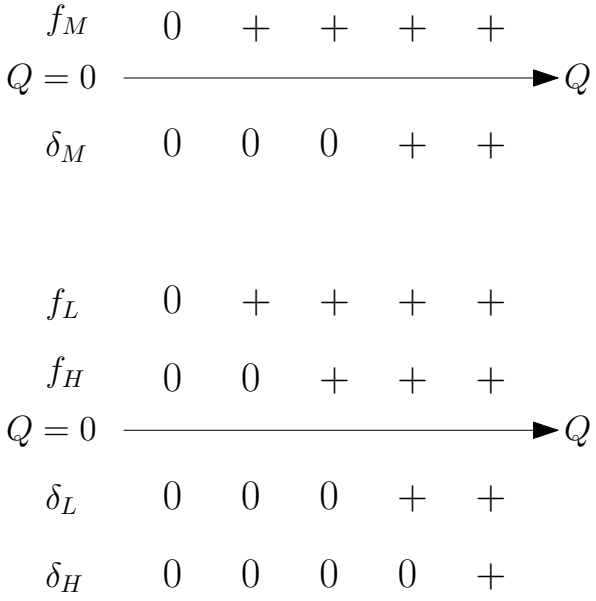
This figure represents the equilibrium in the competitive case. For $Q < C_1$, the client pays no fee to either venue and they invest in no additional security. However, the transaction is small enough such that the attacker does not attack. For $C_1 \leq Q < C_2$, the client pays a fee to the less-sophistication venue that induces it to invest in additional security such that the attacker does not attack. The client pays no fee to the high-sophistication venue, but the baseline security is sufficient such that the attacker does not attack. For $C_2 \leq Q < C_3$, the client pays fees to both venues that induce them to invest in additional security such that the attacker does not attack. For $C_3 \leq Q < C_4$, the client pays the low-sophistication venue a fee and the venue invests in additional security. However, the security investment is not sufficient to fully deter the attacker, and a successful attack occurs with positive probability. The fee paid to the high-sophistication venue is sufficient to fully deter the attacker. For $C_4 \leq Q$, the client pays both venues fees and both invest in additional security. However, the security investment is not sufficient to fully deter the attacker, and a successful attack occurs with positive probability at both venues.

Figure 3: Comparison of Monopoly and Competition

Panel A: Monopoly and competitive equilibria when $\eta \leq \frac{1}{2}$.

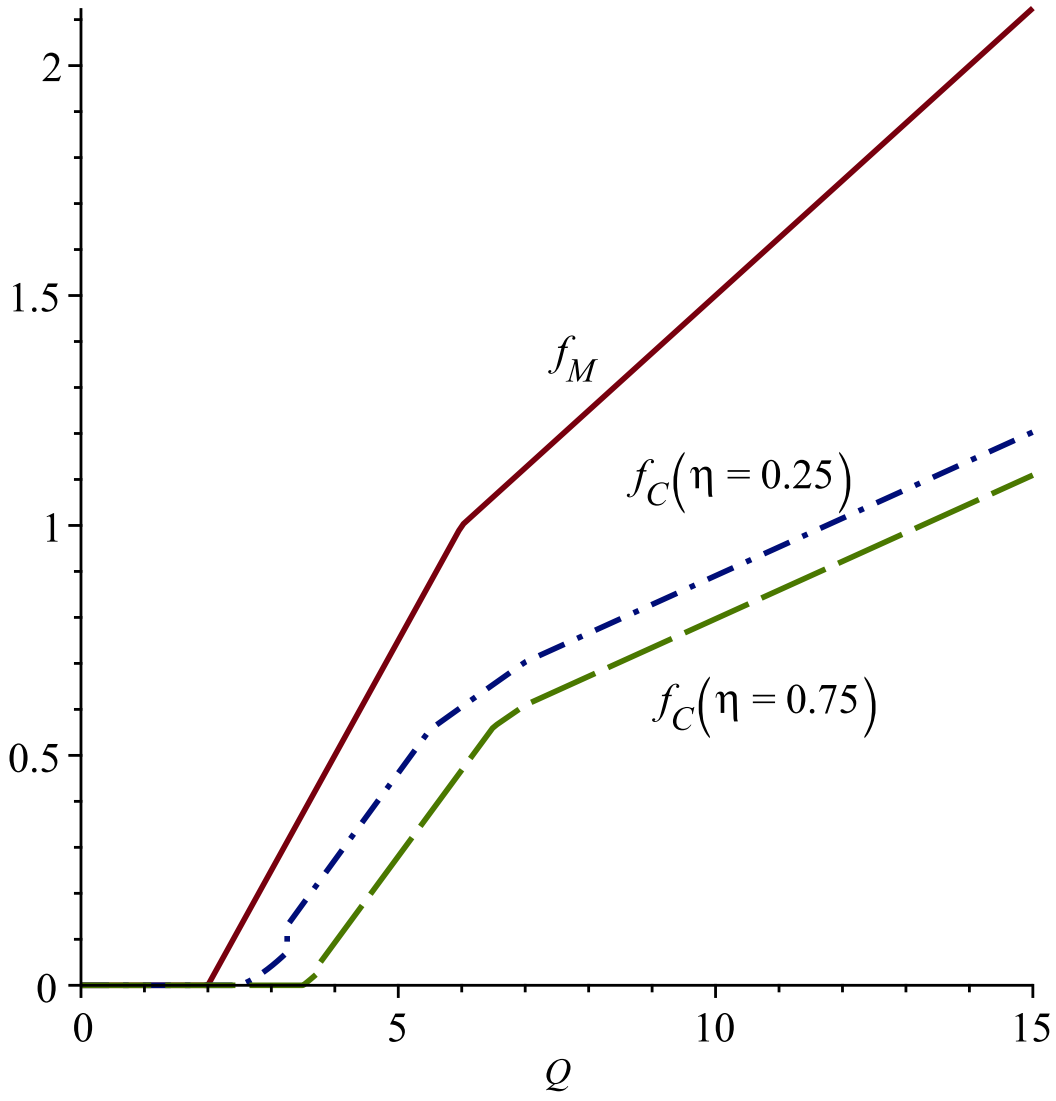


Panel B: Monopoly and competitive equilibria when $\eta > \frac{1}{2}$.



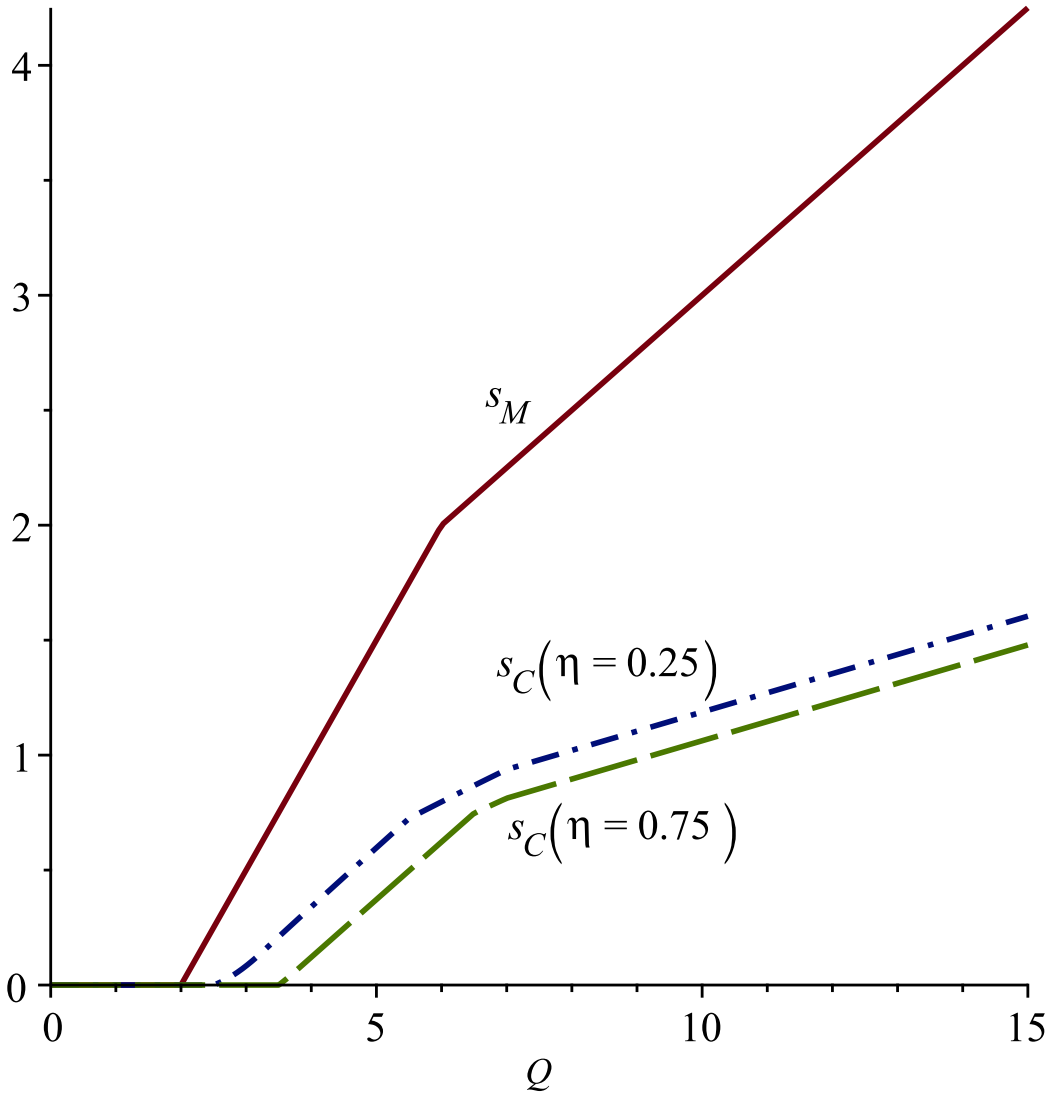
This figure compares the order of the monopoly and competitive equilibria. Panel A represents the case where $\eta \leq \frac{1}{2}$. When $\eta \leq \frac{1}{2}$, the total transaction size Q at which $\delta_L > 0$ is less than the transaction size at which $\delta_M > 0$. That is to say the low-sophistication exchange suffers attacks at a smaller total transaction size than the monopolist. Panel B represents the case where $\eta > \frac{1}{2}$. When $\eta > \frac{1}{2}$, the total transaction size Q at which $\delta_L > 0$ is greater than the transaction size at which $\delta_M > 0$. That is to say the monopolist suffers attacks at a smaller total transaction size than the low-sophistication exchange.

Figure 4: Fees in the Single Platform and the Fragmented Platforms



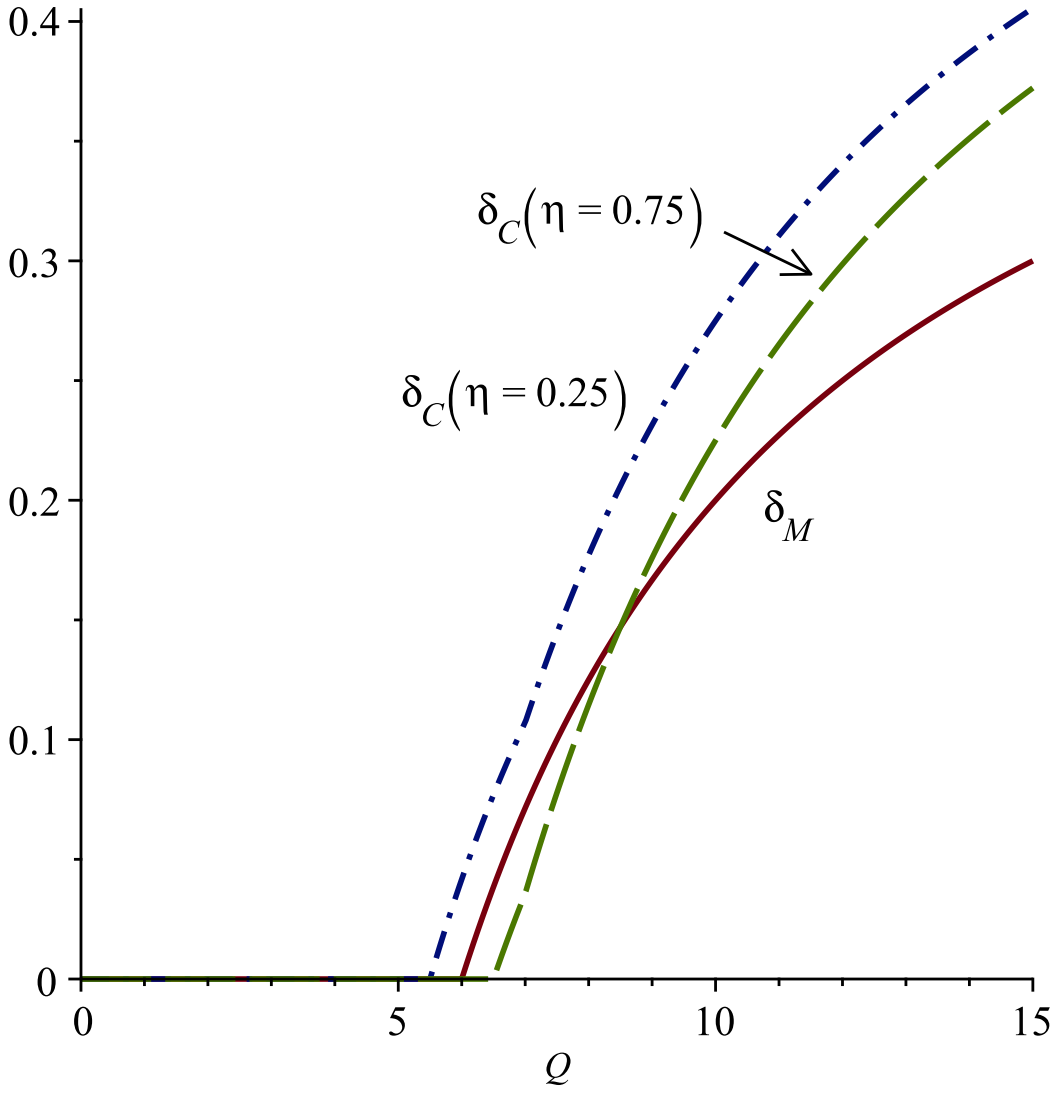
This figure represents total fees paid to the fragmented platforms (f_C) compared to the single platform (f_M), as the size of the transaction Q increases. In all cases, the single platform is paid higher fees than the combined fees paid to the fragmented platforms. When the fragmented platforms are very different in baseline security ($\eta = 0.25$), fees paid are higher than when they are similar in baseline security ($\eta = 0.75$).

Figure 5: Security Investment in the Single Platform and the Fragmented Platforms



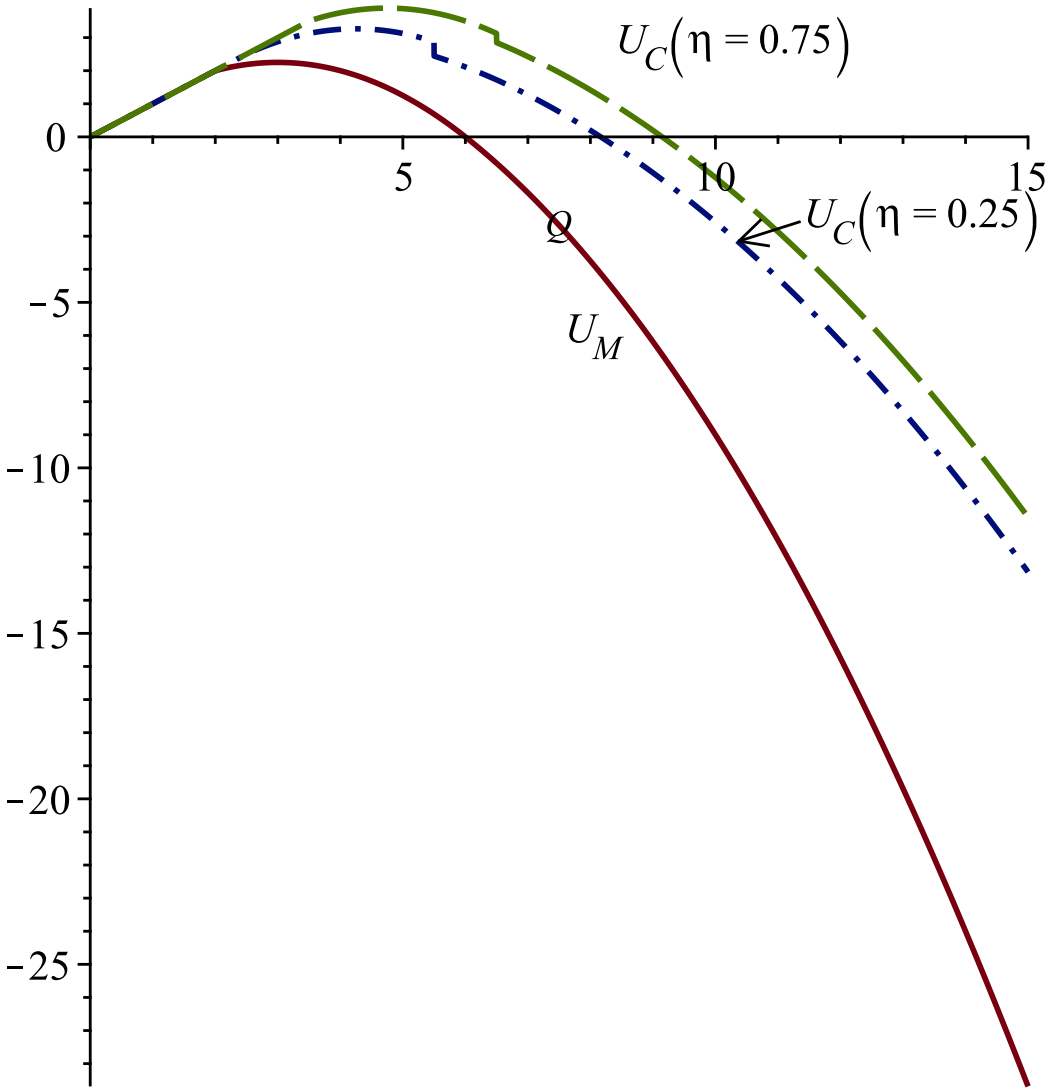
This figure represents total additional security investment in the fragmented platforms (s_C) compared to the single platform (s_M), as the size of the transaction Q increases. In all cases, the single platform invests in more additional security than the combined investment of the fragmented platforms. When the fragmented platforms are very different in baseline security ($\eta = 0.25$), security investment is higher than when they are similar in baseline security ($\eta = 0.75$).

Figure 6: Vulnerability in the Single Platform and the Fragmented Platforms



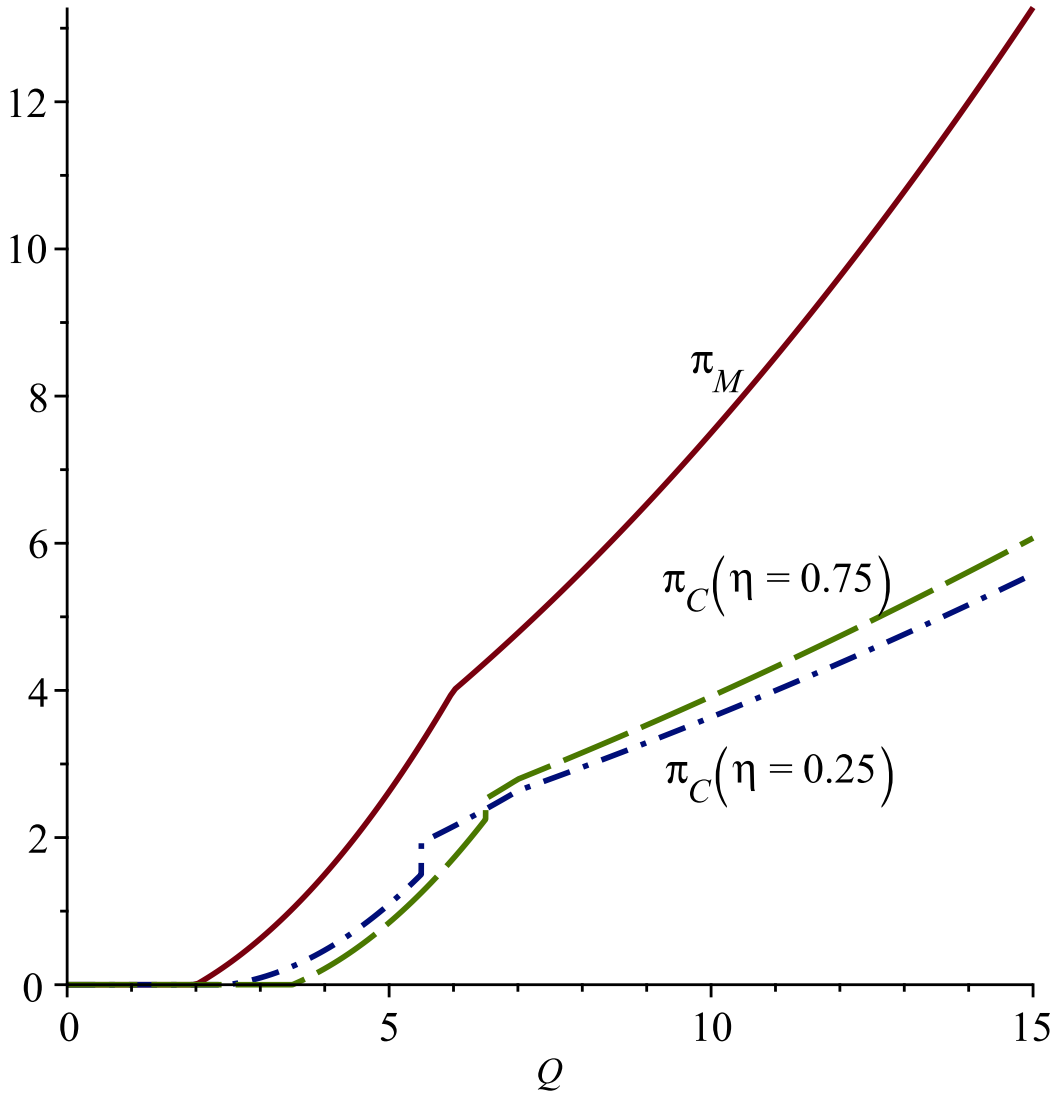
This figure represents vulnerability in the fragmented platforms (δ_C) compared to the single platform (δ_M), as the size of the transaction Q increases. When the fragmented platforms are very different in baseline security ($\eta = 0.25$), vulnerability is strictly higher in the fragmented case. When fragmented platforms are similar in baseline security ($\eta = 0.75$), the vulnerability of fragmented platforms is lower for small transactions, but higher for large transactions.

Figure 7: Client Utility in the Single Platform and the Fragmented Platforms



This figure represents total client utility in the fragmented platforms (U_C) compared to the single platform (U_M), as the size of the transaction Q increases. In all cases, client utility is higher in the fragmented platforms than the single platform. When the fragmented platforms are very different in baseline security ($\eta = 0.25$), client utility is lower than when they are similar in baseline security ($\eta = 0.75$).

Figure 8: Platform Profit in the Single Platform and the Fragmented Platforms



This figure represents total platform profit in the fragmented platforms (π_C) compared to the single platform (π_M), as the size of the transaction Q increases. In all cases, the single platform earns a high profit than the combined investment of the fragmented platforms.