NERA
ECONOMIC CONSULTING

Economic Effects of Imposing Third-Party Liability on Payment Processors

Jeffrey A. Eisenach, Ph.D.

July 2014

Executive Summary

Payment processors ("Processors") are entities that contract with merchants to provide access to electronic payment networks and facilitate the transfer of funds over those networks. They may provide merchant acquisition services, transaction processing services, or both. Processors have direct incentives to monitor merchants' chargeback rates, because they are liable for chargebacks when merchants are unable or unwilling to pay; they are also required, both by internal risk management guidelines and payment network rules, to engage in limited underwriting of merchant accounts.

The U.S. Department of Justice ("DOJ") and other federal regulators are seeking to hold payment processors liable for the activities of third parties through Operation Choke Point and related efforts, the stated goal of which is to prevent fraudulent merchants from having access to the electronic payments processing system. This paper assesses the benefits and costs of third-party liability in general, and Operation Choke Point in particular, from a law and economics perspective. It explains the circumstances under which imposition of third-party liability can constitute an efficient approach to law enforcement, and analyzes whether those conditions are met with respect to Processors.

The paper concludes that imposition of third-party liability on Processors is unlikely to achieve the intended result of denying access to the financial system to wrongdoers, but would impose significant costs on reputable businesses and the economy overall, including higher costs for merchants and consumers, utilization of alternative payment arrangements by telemarketers and other "high-risk" merchants (which may be more susceptible to questionable conduct, such as in the card-not-present environment), and a smaller pool of resources available for consumer redress.

An alternative and superior approach would be to rely upon and support voluntary industry self-regulation. In particular, the Electronic Transactions Association (ETA) has developed a set of guidelines that identify thresholds for determining whether a merchant is a "bad actor." Processors already have incentives to avoid negotiations with bad actors; ETA's voluntary *Guidelines on Merchant and ISO Underwriting and Risk Monitoring* ("ETA Guidelines") will facilitate self-regulation and provide guidelines for processors to take appropriate necessary precautions. Reliance on voluntary guidelines would avoid the unintended consequences of Operation Choke Point and similar enforcement policies, while providing the flexibility necessary to adapt to a rapidly changing marketplace.

CONTENTS

I. Introduction

This paper provides an economic assessment of the benefits and costs of recent efforts by the U.S. Department of Justice and other Federal regulators to impose liability on payment processors for transactions associated with allegedly fraudulent merchants, efforts generally known as "Operation Choke Point."[1]

The Department of Justice (DOJ) began the implementation of Operation Choke Point in March 2013[2] through subpoenas issued under Section 951 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA).[3] By imposing third-party liability (also referred to as "indirect liability" or "vicarious liability") on payment processors, Operation Choke Point seeks to cut off fraudulent merchants from their financial networks, with the stated intent of eliminating those "bad actors" from the market. Other Federal agencies, such as the Federal Trade Commission, may be pursuing similar initiatives.[4]

Vicarious liability may enhance economic efficiency and improve consumer welfare under certain well-defined circumstances, notably when enforcement authorities are unable to ascertain the actual identity of a wrongdoer among a group of possible wrongdoers, when the third-party against whom liability is asserted has the ability to detect or deter wrongdoing that is not detectable by the enforcement authority, and when transactions costs or information imperfections prevent the optimal allocation of liability through contracting.[5] However, payment processors have no comparative advantage over enforcement agencies in determining whether merchants are violating the various statutes implicated in Operation Choke Point.[6] In addition, Processors already have strong incentives to detect harmful activity, by virtue of their obligations to backstop chargebacks when their clients' fail to do so.

The imposition of vicarious liability on Processors raises the cost of payment processing services, especially to merchants engaged in "high-risk" (but not necessarily harmful or unlawful) transactions, and ultimately to consumers. It also creates an incentive for payment processors to deny services to any merchant that may potentially be deemed "high-risk" by the regulators, leading to a variety of market distortions and unintended consequences, including the increased

---

[1] Jeffrey A. Eisenach is a Senior Vice President at NERA Economic Consulting and an Adjunct Professor at George Mason University Law School. The author is grateful to Andrea Lively at NERA for assistance in preparing this paper and to the Electronic Transactions Association for financial support. The views and conclusions herein are exclusively the author's.

[2] *See* Remarks of Michael J. Bresnick, Executive Director, Financial Fraud Enforcement Task Force (March 20, 2013) (available at http://www.justice.gov/iso/opa/doj/speeches/2013/opa-speech-130320.html).

[3] 12 U.S.C. §1833a.

[4] *See* Letter from Chairman Darrell E. Issa, House of Representatives Committee on Oversight and Government Reform, to the Honorable Edith Ramirez, Chairwoman, Federal Trade Commission (June 26, 2014) (requesting documents related to the Federal Trade Commission's involvement in Operation Choke Point).

[5] In addition, a third party may be held liable for acts committed by an entity acting as its agent or "on its behalf."

[6] For example, Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits "unfair or deceptive acts or practices in or affecting commerce."

use of "unconventional" and foreign-domiciled payment mechanisms, which are more susceptible to questionable business practices than the mainstream payment processors they would replace.

Based on the evidence and analysis presented below, the imposition of vicarious liability on payment processors through Operation Choke Point is generating significant economic costs while generating little or no apparent benefits.

The remainder of this report is organized as follows. Section II presents background information, briefly describing relevant characteristics of the payment processing industry and Operation Choke Point. Section III discusses the economic criteria for imposition of vicarious liability under a law and economics framework. Section IV describes the negative consequences that follow from an inappropriate imposition of vicarious liability through Operation Choke Point. Section V examines industry self-regulation as an alternative approach, and concludes that voluntary self-enforcement mechanisms, such as the use of the ETA Guidelines, would distribute liability in a more efficient manner. Section VI presents a brief summary.

II. Background

This section describes the payment processing industry, the underwriting process used by payment processors, and the relevant characteristics of Operation Choke Point.

A. The Payment Processing Industry

Payment processors ("Processors") are entities that contract with merchants to provide access to electronic payment networks (such as the Visa and MasterCard credit and debit networks) and facilitate the transfer of funds over those networks.[7] Processors may provide merchant acquisition services, transaction processing services, or both.[8] Merchant acquisition services include signing up merchants to accept payment cards and providing them with the technology to do so.[9] Transaction processing services include communicating electronically with banks to confirm that the consumer has sufficient funds available to pay for the goods or services being sold (authorization),[10] handling the information and payment flows required to transfer funds from the consumer's account to the merchant's account (clearing and settlement),[11] managing chargebacks

[7] See Ramon P. DeGennaro, "Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box," *Federal Reserve Bank of Atlanta Economic Review* (2006) 27-42.

[8] DeGennaro at 30-32.

[9] *Id.* at 30. See also Aneet Bansal, Challenges & Opportunities for Merchant Acquirers," CapGemini Financial Services (2012) (available athttp://www.capgemini.com/sites/default/files/resource/pdf/Challenges___Opportunities_for_Merchant_Acquirers.pdf).

[10] "Payment Processing: What Developers Need to Know," PayPal White Paper (2008) at 4 ("The authorization process verifies that the customer's card is active, and that there is sufficient credit to pay for the transaction.").

[11] *Id.* ("During the settlement process, the customer's card account is charged and money from the customer's account is transferred to the merchant's account."). See also DeGennaro at 32 ("Clearing and settlement is the process of sending transactions through the Visa or MasterCard network so that the merchant can be paid for the sale.").

(which occur when the consumer disputes a charge directly with the bank that issued the credit card) and managing fraud inquiries (dispute management).[12]

Some large merchant acquiring banks perform merchant acquisition and transaction processing functions in-house.[13] Other merchant banks outsource merchant acquisition and processing to third-party Processors. Such Processors are sponsored by their merchant banks (like Bank of America Merchant Services and Chase Paymentech), which are members of the Visa, MasterCard, and other card networks.[14] Some Processors use Independent Sales Organizations ("ISOs") to recruit merchants.[15] While ISOs typically do not perform payment processing services themselves,[16] some ISOs have sophisticated managements with banking or other relevant backgrounds and perform merchant underwriting and risk monitoring with respect to the merchants they refer to the Processor.[17]

Processors are required, both by internal risk management guidelines and payment network rules, to engage in underwriting of merchant accounts. The Visa and MasterCard networks require, among other things, that Processors (a) initially screen merchants to determine their financial viability and general background, (b) conduct ongoing monitoring to ensure that merchants continue to remain financially stable and refrain from engaging in fraud against the payments system and the card brand reputations, and (c) engage in increased monitoring for merchants with excessive instances of "chargebacks."[18] In addition to these payment network guidelines, processors commonly employ their own underwriting and monitoring best practices. Processors have direct incentives to monitor merchants' chargeback rates because they are liable for chargebacks when merchants are unable or unwilling to pay chargebacks.[19]

The underwriting activities engaged in by Processors in the ordinary course of business are designed to protect the financial integrity of the payment processing system, not to replace the law enforcement function of identifying and prosecuting merchants' fraudulent or illegal activities.

---

[12] DeGennaro at 34.

[13] Dale Schmidt, "Online Payment Processing Software Developers in the U.S.," IBISWorld Industry Report OD4521 (July 2012) at 12 ("Merchant banks, also referred to as member banks or acquiring banks, have direct access to the Visa and MasterCard networks… Due to this proximity, merchant banks are able to perform all of the functions associated with online payment processing. These include underwriting risk, acquiring merchants, operating transaction processing platforms and providing customer service functions.")

[14] See Bansal at 5 ("Third-party processors provide transaction processing services to acquirers as they possess economies of scale and advanced technological systems for cost effective processing. Processors charge a service-based or fixed fee from acquiring banks based on the type of pricing contract. Examples of third-party processors include: Global Payments Inc. and First Data.").

[15] Bansal at 5.

[16] *Id.* See also DeGennaro at 31 ("Most of the larger merchant acquirers also function as processors, but almost all of the smaller ones are resellers.").

[17] *See* http://merchantwarehouse.com/glossary/independent-sales-organization.

[18] *See, e.g.,* Visa Acquirer Risk Program Standards Guide, January 2010 at 4-12, found at: http://usa.visa.com/download/merchants/AcquirerRiskProgramStandardsGuide_2010.pdf

[19] DeGennaro at 34, 37.

Thus, Processors are not presently well positioned to identify, let alone police, the sorts of activities or actors that are the targets of Operation Choke Point.

B. Operation Choke Point

Operation Choke Point was implemented by the DOJ in the spring of 2013 with the stated goal of targeting fraudulent merchants by "putting a chokehold" on "the means by which fraudulent merchants are able to get paid."[20] The program is wide-ranging and significant in scale: By year-end 2013, the Department had issued more than 50 subpoenas to banks and payment processors.

The Operation has proven to be controversial, leading to reports in the media and at least one Congressional investigation, by the House Committee on Oversight and Government Reform. The primary concern policymakers have expressed is that the objectives of the program go beyond eliminating truly fraudulent merchants and include efforts to limit or eliminate access to the payment processing system by industries deemed by enforcement authorities to be socially or economically undesirable, such as the payday lending industry. In fact, the *Four-Month Status Report* on Operation Choke Point explicitly "identifies Internet payday lending as a fraudulent 'scam' being targeted by the initiative."[21] Questions have also been raised about the program's legal underpinnings.[22]

As discussed below, even leaving aside the program's legal basis and the extent to which it is inappropriately targeting lawful businesses, there is an even more fundamental question about whether Operation Choke Point constitutes sound public policy. Simply put, imposing liability on Processors for the activities of their merchant customers is not in most cases an efficient law enforcement strategy – that is, it is likely to generate costs in excess of any benefits.

III. The Law and Economics of Third-Party Liability for Payment Processors

Economic theories of liability focus on maximizing consumer welfare by allocating risk-bearing and incentives so as to minimize the total social costs of harmful activities.[23] In general, that objective is met when the parties that commit harmful acts are made to bear the costs,[24] either

---

[20] http://www.justice.gov/iso/opa/doj/speeches/2013/opa-speech-130320.html

[21] U.S. House of Representatives Committee on Oversight and Government Reform, *The Department of Justice's "Operation Choke Point": Illegally Choking Off Legitimate Businesses?*, Staff Report (May 29, 2014) at 2 (hereafter *Staff Report*).

[22] *Id.*, at 3-4.

[23] See e.g., Robert D. Cooter, "Economic Theories of Legal Liability," *Journal of Economic Perspectives* 5;3 (Summer 1991) 11-30 at 11.

[24] In the absence of transaction and enforcement costs, and with perfect information, an efficient outcome will also be achieved if property rights are defined in such a way that "victims" of harmful acts can compensate "wrongdoers" for refraining. See Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3 (October 1960). Those conditions are not met here.

through contractual and other market institutions or through law enforcement and *ex post* adjudication. Third-party liability is justified only when it is impossible to efficiently allocate risk or impose consequences directly on the wrongdoer, *and* when a third party is in a position efficiently to deter harmful actions or ameliorate their consequences. The first section below describes the conditions under which third-party liability *may* be justified. The second section explains why those conditions are not met in the case of payment processors.

A. The Necessary Conditions for Efficient Imposition of Third-Party Liability

Third-party liability arises when one party is held liable for the harmful actions of a different party.[25] In the law, third-party liability may arise from the existence of a principal-agent relationship, such as when a corporation is held liable for torts or criminal acts committed by its employees, or a telemarketing firm violates marketing regulations while acting on behalf of a client;[26] when it is impossible to identify a wrongdoer from among a group of potential wrongdoers;[27] or, when a third party is believed to have the capacity efficiently to detect, deter or prevent harmful conduct, as when a tavern is held liable for serving alcohol to patrons who subsequently drive under the influence[28] or when property owners are held liable when their premises are used to sell counterfeit or gray market goods.[29]

In the case of a principal-agent relationship, such as between Processors and merchants , the central issue is the ability of a third party (the agent) to efficiently detect and deter the principal's illegal activities, a role sometimes referred to as "gatekeeping."[30]

In this context, the efficient imposition of third-party liability requires that two sets of necessary conditions be satisfied. First, the primary wrongdoer must be out of the reach of the enforcement

---

[25] See, e.g., Alan Sykes, "The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines," *Harvard Law Review* 101 (1988) 563-609 at 563 ("'Vicarious liability' may be defined as the imposition of liability on one party for a wrong committed by another party.").

[26] Nuno Garoupa, "Corporate Criminal Law and Organization Incentives: A Managerial Perspective," *Managerial and Decision Economics* 21 (2000) 243-252, at 244 ("Within the context of corporate liability, shareholders become quasi-enforcers."); and, Federal Communications Commission, *In the Matter of Dish Network et al Petition for Declaratory Ruling re: TCPA Rules: Declaratory Ruling* (FCC-13-54A1; May 9, 2013).

[27] See e.g. *Ybarra v. Spangard* 154 P.2d 687 [Cal. 1944] (in which the court ruled that a patient injured during an operation could collect from several health professionals involved in the procedure, even though only one of them may have actually been at fault); see also Thomas J. Miceli and Kathleen Segerson, "Punishing the Innocent Along with the Guilty: The Economics of Individual Versus Group Punishment," *The Journal of Legal Studies*, 36(1) (2007) 81-106.

[28] In North Dakota, for example, any person "injured by any obviously intoxicated person has a claim for relief . . . against any person who knowingly disposes, sells, barters, or gives away alcoholic beverages to a person under twenty-one years of age, an incompetent, or an obviously intoxicated person." D. Cent. Code 5-01-06.1.

[29] See, e.g., *Fonovisa v. Cherry Auction*, 76 F.3d 259 (9th Cir. 1996).

[30] See e.g., Reinier H. Kraakman, "Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy," Journal of Law, Economics and Organization, 2:1 (Spring 1986) 53-104.

authority (because the offender is either difficult to identify or judgment proof); or, transactions costs must be sufficiently high to deter the parties from contracting to efficiently reallocate liability among them.[31] Second, and in addition, the economic efficiency of third-party liability hinges on the assumption that third parties can monitor and deter bad acts more effectively than the enforcement authority itself. This implies that the third party must be in a superior position (relative to the enforcement authority) to either detect and deter bad acts directly, or at least to indirectly decrease their frequency by internalizing their expected costs and curtailing the economic activity that ultimately leads to bad acts.[32] Thus, the social desirability of third-party liability depends on the degree that the enforcement authority cannot (through, e.g., investigation) significantly increase the likelihood of apprehending the true offender.[33]

To be clear, the criteria above are *necessary*, and not sufficient, conditions. For third-party liability to be efficient, it must also be the case that the benefits associated with increased enforcement efficiency must exceed both the direct and indirect costs of third-party monitoring, an assessment that can only be made on a case-by-case basis.[34] For instance, the efforts that third parties must engage in to detect and deter bad acts may impose excessive costs on other parties, which may exceed any benefits associated with deterrence.[35] In addition, imposing third-party liability may

---

[31] See e.g., Doug Lichtman and Eric Posner, "Holding Internet Service Providers Accountable," *Supreme Court Economic Review* 14 (2006) 221-259 at 229 ("Conventional economic analysis suggests that an explicit rule imposing indirect liability is not necessary when two conditions are simultaneously met: first, the relevant direct actors are subject to the effective reach of the law, by which we mean that the employees, drivers, and merchants discussed in our previous examples are easy to identify and have assets that are sufficient to pay for any harm caused; and, second, transaction costs are such that those direct actors can use contract law to shift responsibility to any party that might otherwise be an attractive target for indirect liability.").

[32] See, e.g., Lichtman and Posner at 230 ("[E]conomic analysis identifies two additional factors: first, indirect liability should be attractive in cases where the potentially liable party is in a good position to detect or deter the relevant bad act; and, second, indirect liability should be attractive in cases where it can encourage the liable party to internalize some significant negative externality unavoidably associated with its activities").

[33] See e.g., Miceli and Segerson at 83 [W]hen the enforcer can invest in detection to increase the likelihood of apprehending the true offender, then individual punishment will always be preferred under the deterrence goal, while the ranking of the two approaches under the retribution goal will depend on the accuracy of the detection technology.")

[34] See Lichtman and Posner at 231 ("These factors—call them "control" and "activity level"—are neither alone nor together sufficient to justify the imposition of an indirect liability rule. Instead, these are merely prerequisites that help to identify cases where liability might be attractive. The actual question of whether liability should be imposed typically turns on other, often setting-specific considerations."); see also Kraakman at 54 ("The ability to disrupt misconduct, however, is only a requisite for gatekeeper liability. Some gatekeepers may be ineffectual or costly enforcement agents under any legal regime, while others-such as accountants or underwriters in the securities markets-face powerful market incentives to oppose wrongdoing even without collateral liability.").

[35] See Lichtman and Posner at 232 ("Thus, while the telephone company surely has the ability to deter crank phone calls by more carefully monitoring calling patterns, it is unlikely that telephone company liability would be attractive, both because of obvious privacy concerns and because of worries that, in its attempts to address the problem of crank calls, the telephone company would inadvertently interfere with a sizeable percentage of legitimate telephone activity. To reject indirect liability in this situation is in essence to announce that the costs of crank telephone calls are not sufficiently high as compared to the costs of indirect prevention.").

cause other parties to make economically inefficient decisions by preventing them from internalizing the economic costs associated with their actions.[36]

B. The Relationship between Processors and Merchants Does Not Meet the Necessary Requirements for Third-Party Liability

The criteria for efficient third-party liability are not present in the relationship between Processors and merchants. As a general matter, the primary alleged offender is in no way unknown to, or "out of the reach," of enforcement authorities. Federal enforcement authorities, such as the DOJ and the Federal Trade Commission, have the capability of identifying offenders, and possess the legal authority to prosecute them.

More broadly, Processors possess no comparative advantage in monitoring violations. Unlike an employer capable of overseeing and structuring a worker's daily activities, or an accountant with intimate knowledge of a corporation's finances, processors operate at arm's length from their clients. Further, unlike a regulator with subpoena and enforcement power, Processors have no special ability to monitor or enforce merchants' compliance. Many Processors handle portfolios consisting of hundreds of thousands of merchants, with tens of thousands of new applicants each year. The underwriting activities currently undertaken by processors are consistent with the strong incentives they face by virtue of their obligation to backstop chargebacks when a merchant fails to do so.[37] However, there is no basis for believing that a processor's ability to monitor return and chargeback transactions, and to do financial underwriting on the basis of such data, translates into the ability to make meaningful inferences about law enforcement matters. Indeed, categories of merchants generally regarded as "high risk" based on chargeback rates include airlines, cruise lines and furniture dealers.

IV. Operation Choke Point Imposes Third-Party Liability, Distorting Competition and Harming Consumers

The DOJ's implementation of Operation Choke Point has direct and potentially far-reaching consequences. By effectively imposing vicarious liability on processors, it forces processors to internalize the risk of merchants' potentially illegal act. The effect, over time, will be to fundamentally alter processors' approach to risk management, in their new role as enforcement

---

[36] *Id.* at 232 ("Similarly, the mere fact that an airport provides a venue from which airlines impose on neighbors a pollution and noise externality does not itself justify imposing liability for that harm. After all, the neighbors are themselves making decisions that increase and decrease the importance of these externalities; and, in a world where the airport absorbed these costs in full, neighbors might inefficiently decide to use their properties to raise livestock and care for the elderly, two uses that are so sensitive to noise and pollution that they likely should be disfavored given the proximity of the airport.").

[37] See DeGennaro at 34 ("A merchant acquirer suffers losses if a merchant is unable to make good on credit transactions disputed by customers, called chargebacks. Chargebacks usually occur when a consumer is dissatisfied with a product or service… Because of this feature, the merchant (and ultimately the merchant acquirer) is at risk of loss for up to several months because the transaction can be reversed. In the language of payments, the transaction is not final. This feature greatly enhances the appeal of credit cards to cardholders, but it also shifts the risk of chargebacks to the merchant acquirer.").

deputies and guarantors for their merchants. For instance, the scope of due diligence reviews would have to be expanded to ensure merchant compliance with a variety of state and federal laws and regulations, which could include the introduction of, e.g., mandatory on-site visits, increased scrutiny of any merchant that might potentially be engaged in illegal activities, periodic audits and investigations into business contacts, contacting and surveying merchants' customers, and mystery shopping.

Because processors are not well-positioned to conduct such investigations, these increased underwriting activities are likely to be subject to high rates of both Type I and Type II error: That is, relatively high proportions of fraudulent merchants are likely to go undetected (Type I error) while relatively high proportions of legitimate ones are likely to be denied access to the system (Type II error).

In any case, the expansion in risk management duties that seems to be the intended effect of Operation Choke Point will inevitably raise the cost of payment processing services to merchants (and ultimately to consumers). Furthermore, the increased cost of merchant acquisition—and the increased risk of adding new, untested merchants to the network—would cause at least some processors to deny services to "high risk" merchants, including most notably merchants involved in "card-not-present" transactions, which are regarded as more prone to fraud.

The available evidence suggests that Operation Choke Point is already having such effects, if not by design then at least as a practical matter. According to the Committee on Oversight and Government Reform, the program has intentionally "target[ed] industries deemed 'high-risk' or otherwise objectionable by the Administration,"[38] including the firearm, adult entertainment, check cashing, and payday lending industries.[39] According to the Committee on Oversight and Government Reform, "a wide variety of fully lawful and legitimate businesses received notices that their bank accounts were being abruptly terminated."[40] Thus, the Committee concludes, DOJ "is using [Operation Choke Point] to *forcibly conscript* banks to serve as the 'policemen and judges' of the commercial world"[41] and forcing banks to either "discontinue longstanding, profitable relationships with fully licensed and legal businesses, or face a potentially ruinous lawsuit by the Department of Justice."[42].

---

[38] *Staff Report* at 2.

[39] *Staff Report* at 2, citing Kelly Riddell, *'High risk' label from feds puts gun sellers in banks' crosshairs, hurts business*, WASH.TIMES, May 18, 2014; Glenn Harlan Reynolds, *Justice Department shuts down porn money: Column*, USA TODAY, May 26, 2014; William Isaac, *'Operation Choke Point: Way Out of Control*, AMERICAN BANKER, Apr. 27, 2014; Jessica Silver-Greenberg, *Justice Department Inquiry Takes Aim at Banks' Business With Payday Lenders*, N.Y. TIMES, Jan. 26, 2014.

[40] *Staff Report* at 2.

[41] *Staff Report* at 4, citing Frank Keating, Op-Ed., *Justice Puts Banks in a Choke Hold*, WALL ST. J., Apr 24, 2014, emphasis in original.

[42] *Staff Report at* 9.

Further unintended consequences of Operation Choke Point's *de facto* expansion of third-party liability are likely to include the increased use of "unconventional" or foreign-based payment mechanisms, which are more susceptible to questionable business practices than the mainstream processors they would replace and produce precisely the opposite of the intended effect,[43] While forcing legitimate firms (and their consumers) to bear higher costs..[44] Moreover, higher due diligence costs are likely to fall disproportionately on new entrants and innovative business models.

Thus, the increased compliance costs imposed on Processors by third-party liability costs would be borne by a wide group of legitimate businesses in the hope that a few illegitimate businesses might be deprived of access to the payment system. Furthermore, consumers would suffer harm in the form of: 1) higher prices; and 2) to the extent that use of these alternate payment mechanisms drives unscrupulous merchants off shore, would increase the difficulty of receiving compensation in the event that fraudulent charges occur increasing the risk that there will be inadequate funds to cover consumer chargebacks.

Although prosecuting fraudulent merchants seems like an efficient way to protect consumers from merchants' harmful behavior, Operation Choke Point imposes costs on third-party payment processors by having them "act as the moral arbiters and policemen of the commercial world."[45] Obliging processors to internalize extra risk, and thus engage in activities that could be better performed by enforcement agencies, makes processors reluctant to engage in transactions with any potentially "high-risk" merchants, driving out not only fraudulent, but also lawful and legitimate merchants from the market, effectively reducing competition and harming consumers.

V. Self-Regulation is an Alternative and Superior Approach

Rather than using third-party liability as an enforcement mechanism, a more efficient way to distribute liability would be through a self-regulating mechanism. As mentioned above, the incentives of processors and regulatory agencies are generally aligned: Processors have direct incentives to monitor merchants' chargeback rates because they are liable for chargebacks when merchants are unable or unwilling to pay.

The ETA has undertaken an initiative for industry self-regulation by providing guidelines on merchant and ISO underwriting and risk monitoring that would "effectively mitigate merchant risk

---

[43] See e.g. Kraakman at 66 ("Illicit markets are markets in proscribed goods or services. In the gatekeeping context, they are markets that cater specifically to wrongdoers…small numbers of corrupt gatekeepers may be able to satisfy much of the demand for illicit support and thus render enforcement by honest gatekeepers largely irrelevant to wrongdoers who know the market.").

[44] *Id.* at 75 ("The private costs of gatekeeping include not only the performance cost" of discharging a prescribed monitoring obligation but also the gatekeeper's residual legal risk and the cost of strategies to limit this risk, such as disrupting the activities of risky but innocent clients or customers.").

[45] *Staff Report* at 11.

in the U.S. card acceptance ecosystem."[46] ETA's Guidelines on Merchant and ISO Underwriting and Risk Monitoring:

> provide effective tools for the underwriting and risk management of merchants. They also provide intermediary underwriting and risk management of merchants for banks and processors… [and] could help eliminate prohibited and undesirable merchants from entering into or remaining in the card acceptance ecosystem.[47]

The guidelines provide clearer thresholds of "high-risk" behavior, facilitating self-regulation, and provide guidelines for processors to take appropriate necessary precautions against potentially fraudulent merchants. Because the Guidelines provide clear and comprehensive guidance for Processors on what constitutes adequate underwriting conduct, they reduce uncertainty and limit regulatory risk – precisely the opposite of Operation Choke Point's litigation-focused approach. At the same time, because they are "a 'living' document, which will be reviewed and updated by a select group consisting of risk professionals and other personnel from various ETA Member companies,"[48] they are more likely than formal regulatory actions by Federal agencies to provide the flexibility necessary to adapt to a rapidly changing marketplace. Thus, self-regulation can achieve the desired outcome of helping to keep fraudulent merchants from the payment system, while avoiding the unintended consequences brought about by federal regulations.

VI. Conclusion

The obligation of processors to backstop customer chargebacks already causes them to internalize risks they can efficiently observe – that is, primarily, the risk observed when dissatisfied consumers of products or services charged on payment networks demand refunds and chargebacks. Thus, Processors already have strong incentives to monitor merchant conduct and to reflect the costs of high levels of consumer dissatisfaction back onto the responsible merchants through higher reserve accounts or the threat of termination.

Imposing upon processors the *additional* liability associated with affirmatively policing fraudulent or other illegal activities is not consistent with economic efficiency, ultimately for the simple reason that processors do not have a competitive advantage over federal regulators to accurately identify violations *and because it there is no basis for believing it would be economically efficient to force them to acquire that capacity*.

The DOJ and other regulatory agencies should keep in mind the law of unintended consequences. As Kraakman notes:

---

[46] ETA Guidelines on Merchant and ISO Underwriting and Risk Monitoring, §1.1.
[47] *Id.*
[48] *Id.*

> [G]atekeeping costs are as potentially volatile and difficult to predict as the enforcement benefits of gatekeeper regimes are likely to be. Indeed, one of the critical features that distinguishes third-party enforcement in general from direct liability is precisely the uncertainty created by a third party's limited (but unknown) ability to observe misconduct and the latitude enjoyed by third parties and enforcement targets to reshuffle their relationships on the market.[49]

At a minimum, before drafting processors into the war against fraudulent merchants, the DOJ should have a factual and analytical basis for concluding they would be effective soldiers. Such an analysis would need to take into account: (a) the direct cost to Processors of duplicating the investigative and other resources of the DOJ and other federal regulators, and the extent to which those costs would be passed on to merchants and ultimately to consumers;[50] (b) the likelihood that processors would accurately identify and adjudicate legal violators violations (relative to the DOJ itself and other enforcement agencies); (c) the likely frequency, nature and effects of enforcement errors by processors, including both Type I and Type II error (under-inclusion and over-inclusion, respectively); (d) the ability of processors' to "avoid the draft" by refusing to serve merchants altogether; and, (e) the consequences for the war effort of forcing merchants away from mainstream processors into higher-risk, less-monitored processing alternatives, which may not have the same incentives as mainstream processors to police and identify harmful conduct.

The fact that the incentives of Processors and regulatory agencies to eliminate fraudulent merchants from the market are ultimately in alignment makes the implementation of voluntary guidelines, such as those set forth by the ETA, a superior alternative to the regulators' aggressive law enforcement policies aimed at Processors. Industry self-regulation avoids the additional costs of third-party liability to processors and therefore does not distort the market or reduce competition by driving out important lawful merchants.

---

[49] Kraakman at 78.

[50] Fraud and fraud prevention costs are already passed on to merchants and ultimately consumers. See e.g. Federal Reserve System, *Debit Card Interchange Fees and Routing; Final Rule* (76 FR 43394, July 20, 2011). See also David S. Evans and Joshua D. Wright, "The Effect of the Consumer Financial Protection Agency act of 2009 on Consumer Credit," *Loyola Consumer Law Review* 22 (2009-10) 277-335 at 281 ("Lenders will also pass on the higher costs resulting from federal and state regulation of lending products to consumers in the form of higher interest rates and fees.")

NERA
ECONOMIC CONSULTING
Tel: 1 (212) 345-3000 Fax: 1 (212) 345-4650
www.nera.com