Private, as opposed to legalistic, solutions for mitigating fraud and facilitating online commerce: From PayPal to the blockchain

Very preliminary draft for presentation at NYU April 26, 2016. Typos to be removed and references to be added and I also need to remove repetitive parts in a few spaces. Although the paper is only halfway done, I am looking for your thoughts on the ideas in the paper.

I. Introduction

On Friday February 5, 2016 hackers posing as officials from the Bangladesh Central Bank sent five requests to the Federal Reserve Bank of New York to transfer $950 million out of the Bangladesh Central Bank’s account into private accounts in the Philippines and Sri Lanka. Friday is a weekend day in Bangladesh and Bangladeshi officials only found out after the Federal Reserve Bank of New York had already transferred out $101 million. The Federal Reserve Bank of New York eventually wised up and decided not to transfer the remaining $850 million because “the fact that the money was being wired to personal bank accounts in the Philippines rang alarm bells” but the $101 million was and still is long gone. If two large governmental institutions are unable to recover stolen funds in a case as large as this, imagine if you are a merchant and victim of lots of small scale fraudulent orders. Does anyone actually believe that police and courts will help you get your money back?

Electronic commerce vastly expands a business’s potential customer and partner base, but it also expose it to countless unreliable parties from around the globe. In contrast to a small town brick and mortar business that has the have the ability to know all customers or business partners, online merchants face a potentially unlimited supply of
unscrupulous orders. Fraud against merchants selling online can take the form of unauthorized transactions, hackers using stolen accounts, or the form of “friendly fraud” where a real customer makes an order but later denies it or claims the goods did not arrive. Fraud against merchants doing business with others online can take many forms such as affiliate fraud where one merchant pays commissions for helping sign up customers only to find out that the customers are bogus, or real ones but misled by the affiliate, and later ask for refunds. When a customer disputes an orders, credit card companies typically issue a chargeback and take the money out of the merchant’s account. Lexis Nexis Risk Solutions (2014) estimates the cost of existing card fraud at tens of billions per year, and that does not count the uncountable lost opportunities from trade that never occurred because of the risk of fraud.

What legal recourse do business-to-consumer merchants victimized by online fraud have? A combination of governmental and private mandates (e.g. the United States Federal Reserve’s Regulation Z or many contractually created charge card network rules) say that in cases of card-not-present fraud, merchants, not consumers, have to bear the cost, and, as a practical matter, merchants have almost no options to recover stolen funds. Even when merchants can prove fraud occurred, identifying the fraudsters in the quasi-anonymous settings of the internet is often difficult or impossible. And even when merchants can identify the fraudsters, initiating legal proceedings or recovering money from fraudsters across the world is also not a practical solution. The problem is similar to those faced by all financial institutions when a counterparty intentionally or unintentionally defaults and does not have funds to pay for what it owes. Such a situation can be characterized as a type of large scale prisoners’ dilemma situation where bad transactions spiral out of control.
Martin Boyer (2007, p.481) theorized that when “the proportion of agents that have a low propensity to tell the truth is high” then “resistance to fraud is futile,” and Douglass North (1990) and Richard Epstein (1999) predicted that technologically advanced commerce could not expand without effective laws against fraud.

Despite the continuous threat of fraud and limited legal protections for merchants, electronic commerce not only persists but actually thrives. In the past twenty years, electronic commerce has grown from close to nothing to nearly 10 percent of retail sales in the United States. The value of business to consumer electronic commerce worldwide has also expanded to more than $1.5 trillion per year, an amount higher than the annual gross domestic product of the vast majority of countries. According to Forester Research (2014) the business to business electronic commerce market is four time larger.

How is all that possible? Even though online merchants have limited legal protections against fraud, various online commerce firms have noticed the problem and rather than sitting around and doing nothing about it, they considered solutions as profit opportunities. This article highlights some entrepreneurial, as opposed to legalistic or regulatory, solutions for dealing with potentially bad transactions. The article discusses how online commerce is made possible by firms addressing what could have been considered legal questions as problems of risk management. In contrast to legal solutions that rely on police or courts to address problems ex post, (after they occur), electronic commerce firms have implemented various steps to deal with problems ex ante, (before they occur). One of the first innovators in the early days of the internet was PayPal that developed a system of human augmented artificial intelligence to help predict and turn
down potentially fraudulent orders. Other firms like former software retailer Software.net developed many innovations and refocused itself as the fraud prevention firm CyberSource and was purchased by Visa in 2010.

In addition to these more established payment networks, many startups and large banks are investing in technology associated with cryptocurrencies to potentially reduce fraud and assure payment. Blockchain technology offers the potential for prereconciliation of trade, and computer evaluated “smart contracts” offers various opportunities for verification of delivery of service and payment. Still in their infancy, online platforms and marketplaces like Ethereum and OpenBazaar are designed to let others build as many levels of verification and escrow into the system as users want. Digital Asset Holdings CEO, and former J.P. Morgan vice president, Blythe Masters suggests “Blockchain should be taken as seriously as Internet in early 1990s.” The better intermediaries are at privately reducing problems with contracts that go sour, the more attractive commerce becomes.

Although most consumers do not notice it, firms like PayPal or Visa help process tens of billions of card-not-present credit transactions per year. Imagine if businesses had to go to court for even a small percentage of these transactions: one percent could add a billion cases to the court system per year. Would even the most mostly wildly optimistic believer in the efficacy of government courts think that courts could handle such volume? Although the potential for fraud will, unfortunately, always exist, and attempts at fraud will continue to become more sophisticated, companies that live and die with the success of online commerce will continue to provide existing and look for new solutions. Online
commerce is made possible because of private solutions, private governance, not because of ineffective police and courts.

II. **Two paradigms of how firms should deal with online fraud: Ex post legal enforcement versus ex ante prevention**

a. **Ex post enforcement in theory and practice**

Most academic theories of how people should deal with fraud seem to be influenced by the structure of our legal system that attempts to deal with problems after they occur. Without such enforcement, cheating will prevail. This view of the problem and solution to fraud can be portrayed as a prisoners’ dilemma where government needs to step in to provide negative incentives for cheating. If something bad happens, one calls law enforcement and they rectify the situation, and that deters future wrong doing as well. In the simple game tree in Figure 1 if the payoffs to cheating exceed the payoffs to legitimate behavior, the government steps in to make sure that crime does not pay.

To theorists writing in this tradition, markets themselves and especially technologically advanced markets cannot exist without government oversight. Nobel Laureate Douglass North(1990, p.12), for example, argues that “realizing the economic potential of the gains from trade in a high technology world of enormous specialization and division of labor characterized by impersonal exchange is extremely rare, because one does not necessarily have repeated dealings, nor know the other party, nor deal with a small number of other people.” North (1990, p.35) writes, “The returns on opportunism, cheating, and shirking rise in complex societies. A coercive third party is essential.”
Government officials have expressed similar sentiment since the early days of the internet. In 2000, U.S. Attorney General Janet Reno recognized that government enforcement against cybercrime was ineffective. She states that for government to be able to stop online fraud, it must have the following technological and legal capabilities: (1) "A round-the-clock network of federal, state, and local law enforcement officials with expertise in, and responsibility for, investigating and prosecuting cybercrime"; (2) "Computer forensic capabilities, which are so essential in computer crime investigations"; (3) "Adequate legal tools to locate, identify, and prosecute cybercriminals, and procedural tools to allow state authorities to more easily gather evidence located outside their jurisdictions"; and (4) "Effective partnerships with other nations to encourage them to enact laws that adequately address cybercrime and to provide assistance in cybercrime investigations."

Kubic (2001) of the Federal Bureau of Investigation came up with a very similar list: “The Internet presents new and significant investigatory challenges for law enforcement at all levels...These challenges include: the need to track down sophisticated users who commit unlawful acts on the internet while hiding their identities; the need for close coordination among law enforcement agencies; and the need for trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases.”

In theory each of these conditions could be met, but as a practical matter government may not be able to. I presented Reno’s conditions to Peter Thiel and he stated: “Every single one taken by itself seems extremely farfetched. If that’s the threshold, it’s no wonder it doesn’t work.” Thiel describes how they initially had attempted to report problems to law enforcement but quickly realized the law would be of little assistance. The government officials were hardly experts. He stated, “The level of incompetence we dealt
with was amazing.” At the time he stated that the FBI did not “even have a working email system.” In one case PayPal conducted an internal investigation and determined that a man named Mr. Yagolnitser was defrauding the company of money. After reporting the culprit to the authorities, the law enforcement was of little help. Thiel (2004) stated:

The positive place where [government] failed was in providing security. The natural thinking was that when people are defrauding you, you can go to the police. Maybe Mr. Yagolnitser is not going to go to the police, but maybe we can go to the police and report Mr. Yagolnitser. We proceeded to do that. The FBI showed up at his home and concluded he was totally innocent. We’d given them Web pages. They were asking us, ‘What’s a banner ad?’

I interviewed another founder of an internet firm from the 1990s who told me what happened when hackers broke into his system and were potentially ruining his multimillion dollar company. He reports that after his initial call to the police, they sent an officer to do a report. When the police officer asked what happened, he reported, “Someone broke into my computers.” The police officer then asked to look at the room with the computers and he began looking around the room’s windows and doors and asked “Where did they break in from?” and the entrepreneur stated, ”From the internet.” The police officer then stated, “What’s the internet?” (Personal interview, March 14, 2016). Although most police officers today know what the internet is, we cannot attribute the existence of online commerce to something they learned about well after it emerged.

b. The alternative of ex ante prevention of fraud

PayPal had 1,000 users by November 1999, 10,000 by December, 100,000 by February, and 1 million by April 2000 (Thiel, 2004). But PayPal had not predicted the amount and degree of sophistication of fraudulent schemes against it. Some fraudsters would specialize in stealing and selling passwords and others would specialize in making
use of them. In 2001 and 2002 annual revenues were $14 and $48 million (Prashanth, 2004, p.5), but by early 2001 fraud was costing PayPal more than $10 million per month (Levchin, 2008, p.6). They approached various law enforcement agencies, sometimes with evidence showing wrongdoings of the exact culprit, but found the government was ill equipped, from both a technological and legal point of view, to solve PayPal's problems. Peter Thiel recounted to me: “It turns out that if you deal with someone bad, you will be completely out of luck, regardless of whether there is a theoretical legal system to help you.” Thiel stated, “The government approach assumes that you can solve everything after. It might have worked in a small town setting, where everyone knows everyone else, but it clearly does not work in the current world.” At the time online fraud led to the demise of many of PayPal’s competitors eMoneyMail, PayMe, and PayPlace (Jackson, 2004, p.202). To deal with their growing problems, PayPal developed a sophisticated fraud prevention system that relied on a combination of artificial and human intelligence. Thiel summarized the issue, “There are two ways of dealing with fraud: Predictive versus backward looking.”

The key in this perspective is to develop ways of predicting whether a transaction is likely to be good or bad. In person, one can assess the likelihood that a counterparty will follow through with his side of the bargain based on the potential for repeat dealings or reputation. Based on whether you know the person or think you can trust him for any reason. Online none of the options are available because even if a business thinks it is dealing with a trusted customer or business partner, the one of the other end might be a hacker in a stolen account. For example, suppose in the past a fraudster had in middle of the night successfully transferred $5 out of many people’s accounts and PayPal only found out about this after the fact.
Although PayPal would have a difficult time recovering past losses, they would program their system to look for similar patterns or new ones in the future. When the system saw potentially fraudulent activity it would take steps such as requiring extra verification for transactions, turn down an order, freeze an account or accounts, or flag a set of orders or accounts for manual review. PayPal had an important challenge because fraudsters were often in control of many accounts, and without a system to look for patterns, a fraudster could simply continue similar schemes from new compromised accounts. As the old saying goes, fool me once, shame on you. Fool me twice shame on me. And because fraudsters adapt and create new schemes, they had to program their system to be adaptive, learn, and look for new patterns over time. The detection system had to be much more complicated than “We suffered losses from many $5 transfers in the middle of the night. Therefore look for fraudulent $5 transfers in the middle of the night” when the fraudster could change their scheme to any amount and at any time.

With face-to-face interaction, parties have various options of assessing whether they believe their counterparty is reliable like dealing with friends and family or trusting others based on past experience, reputation, or visible signals of potential reliability. Face-to-face is also often repeated and any party can end it if the other ends up being unreliable. But how can businesses decide who to trust when they have not met the other party and the other party might be a compromised account? PayPal had expanded its private security team to two dozen employees when the team noticed that they could only effectively monitor a fraction of the transactions. That led to the development of a fraud monitoring and prevention system that could spot potentially fraudulent transactions and alert the team to suspicious patterns of behavior (Levchin, 2008, p.11). Levchin stated, “We mine millions and millions of
transactions in real time” (quoted in Schwartz, 2001). PayPal’s system looked for patterns, such as many accounts suddenly transferring small sums into one account, sudden increases in account activity, high dollar payments, or payments to certain regions of the world (Schwartz, 2001).

PayPal used technology to scale up, well beyond close knit groups, the age old dilemma for businesses of whom to trust. The solutions led to a rapidly expanding set of users. Before PayPal was introduced in late 1999, more than 90 percent of eBay auctions were paid using checks (Schwartz, 2001), and within one and a half years, more than 1 million daily auctions on eBay were advertising PayPal as a method of payment. Purchased by eBay for $1.5 billion in 2002, PayPal now has 173 million accounts and processes more than $200 billion in transactions per year and has an industry-leading fraud loss rate of 0.5 percent. Levchin later stated, “I think a good way to describe PayPal is: a security company pretending to be a financial services company.” Business Week described PayPal’s work as that of a “pre-crime’ detective” (Black, 2002). Thiel states, “If we had left things to the ex post method, the whole thing would have not worked.” As Thiel stated, “On the positive side, if we had not come up with a technology solution to fraud, we would have simply gone out of business. [Government] might have arrested various low level people, but we would never have gotten the money back.”

Other companies have adopted many similar practices and have come up with other important innovations too. In 1995 an early online software reseller Software.net was also increasingly hit by fraudulent orders and realized that unauthorized transactions were pushing them toward bankruptcy. In response, they developed “one of the first real-time
identity verification systems using a unique, automated ‘profiling’ algorithm” and eventually began marketing to others (CyberSource, 2012b). Its fraud prevention subsidiary, CyberSource, eventually became the core of the business. Purchased by Visa for $2 billion in 2010, CyberSource analyzes the 60 billion annual transactions on the Visa network and utilize “260 validation tests—all correlated in about one second— to help boost detection accuracy.” Predictive analytics, probabilistic risk assessment, and scoring systems help estimate whether a transaction is likely to be bad.

We can represent the choice of merchants or their agents, the payment processors, using a simple decision tree. Rather than processing all orders and then going to law enforcement for transactions that go bad, a payment processor like PayPal assigns a probability that a trade will go well or poorly and then weighs the costs and benefits of processing or turning down the order. By turning what could have been a legal issue into an economic choice, the merchant or payment processor must decide how much risk it is willing to assume and such a decision must always be a balancing act. One does not want to accept all orders including fraudulent ones, but also does not want to turn down all orders including good ones. Firms must weigh the costs of a Type I and Type II errors, the costs of accepting bad versus turning down good orders.

Although few academics document and discuss such a perspective, such thinking is widely held among industry experts and market participants and the amount of corporate writing on this topic is large. For example, the fraud mitigation firm, Verifi, discusses the importance of protecting against online fraud and advocates layers of protection. But at the
same time they stress the cost of overprotection and state that one should not be too vigilant.

While employing every single fraud prevention tool available is neither feasible nor necessary, merchants should be aware of the types of solutions available and employ each as needed. In the end, merchants need to evaluate the cost of fraud prevention against the benefits. It’s easy to fall into the trap of “turning on” all fraud prevention measures to ensure that nothing seeps through the cracks; however, there is such a thing as being too aggressive. Having a 0.00% chargeback ratio is not a desired outcome if you are turning away 10% of your good customers in the process. A balance needs to exist between what you are turning away and what you accept as valid.

Notice the perspective is quite different from the standard legal and regulatory responses that tend to be binary and focused on disallowing bad transactions, and less attuned to letting market participants weighing Type I and Type II errors when assessing options. Many financial regulations, for example, aim to minimize the chance that a loss occurs but do so at the expense of disallowing transactions that might go sour even if the transaction has a positive expected payoffs for all parties involved. In contrast to the legalistic approach, the perspective of risk management lets merchants weigh the costs of accepting bad orders or turning away too good ones.

Figure 3 shows the amount of online commerce per year and the amount of fraud per year. As the market has dramatically expanded, so too has the amount of fraud, but notice that the fraud loss ratio has decreased. With risk management, the objective is never to decrease fraud against oneself to zero: the best way to do that would be to turn down all

---

1 Tabarrok argues that when faced with a choice of allowing a drug that will save many people but kill some of its users, the FDA will turn down the drug because those with negative complications are highly visible whereas those who were never saved are unseen.
orders and do no business at all. Instead, companies weigh the cost of potential fraud with the cost of turning down good orders.

How much risk a firm is willing to assume depends on its industry and risk profile and some firms or parts of the industry are more risk averse than others. Merchants doing business in areas with higher chances of chargebacks such as fortune telling, gambling or adult websites, find themselves unwelcome on traditional payment processing networks. But merchants doing business in the high risk area have their own high risk payment processors that have been successfully experimenting with ways to mitigate fraud. One option is to just deal with high risk payment processor that simply passes the cost of bad transactions to the high risk merchant. Another option is to take additional steps to reduce potential problems. Companies like DirectPayNet advise merchants to implement various rules such as not accepting too many orders from a particular location in any given time period and that can cut down bogus orders coming from a particular hacker's machine. Or a merchant can choose to not accept any orders from a particular location or not accept orders from computers whose locations are masked.

Merchants might adopt precautionary measures involving geolocation services and not accept orders from IP addresses from certain regions or not accept orders from customers using proxy servers. Others might use velocity rules that limit how many orders can be placed from a particular set of internet protocol addresses in any given time period. Others can opt into more expensive and more comprehensive fraud mitigation systems such as Kount Inc.’s risk inquiry and scoring system. High risk merchants also often have to
have a set of reserve funds with the payment processor, which the latter can draw from when transactions go wrong.

DirectPayNet founder Maria Sparagis also advises firms on how to do business with cryptocurrencies like Bitcoin. An advantage to merchants for Bitcoin is they get instant payment and do not have to worry about chargebacks from consumers who later deny the purchase. On the other hand, if an owner of crypocurrency has his account hacked and money, the legitimate former owner has no way to recover funds. But today’s potential problem is tomorrow’s potential solution and many firms are building on the technology to add layers of safety.

New platforms or marketplaces like Ethereum and OpenBazaar are building on aspects of Bitcoin related technology (i.e. blockchain) and are programmed to accommodate use of escrow and multisignature approval for trigger transference of funds and goods. Contracting parties could have as many parties involved with the process as they want, but a standard 2-of-3 contract items are not transferred until two of three signatures are obtained from: the buyer, the seller, and a third party notary or arbitrator. If the buyer and seller sign off on a contract then items are released from escrow, and if one party does not agree an arbitrator is brought in to release certain items out of escrow. Another option includes algorithmically judged “smart contracts” where a platform and contracts are programmed to look for objectively verifiable facts (such as what team won a sporting match for the purposes of settling a bet) and if those conditions are met, then funds or goods are released. It seems these are just the tip of the iceberg for further ways of ensuring payment in the future.
Although parties may want human review and interpretation for many contracts, many contracts can easily be programmed and adjudicated algorithmically using if-then statements. For example, credit default swap contracts currently take the form of: if a bond has a credit event and the International Swaps and Derivatives Association determines the bond is worth x cents on the dollar, then a holder of a credit default swap 100 – x. (For example, a person with a $1 insured bond ends up with a bond in default worth $0.40 would be entitled to $0.60.) Many online contracts can be programmed to allow release of goods and funds when certain objective criterion are met. When observers from two decades from now look at smart contracts from today, they will almost certainly consider these smart contracts much less developed than the standard of the future. They will have a similar perspective of an observer from 2016 looking back at electronic commerce from 1996.

Conclusion

Insert this section in the future

References

Insert this section in the future

Figures

Insert this section in the future