Entrepreneurial, As Opposed to Legalistic, Solutions for Mitigating Fraud and Facilitating Electronic Commerce in the Digital Age: FROM PayPal TO Blockchain

Edward Peter Stringham  
J.R. Clark*

Online merchants have limited legal protection against fraudulent orders, but online commerce thrives nevertheless. Relying on corporate literature and interviews with market participants, the article describes how merchants and financial intermediaries address fraud as an issue of risk management rather than a legal issue. Innovations such as predictive analytics help mitigate what might otherwise be an intractable problem and help vastly expand the scope of commerce. (Keywords: Innovation, Fraud Prevention, Payment Processing, Credit Cards, Predictive Analytics, Blockchain Smart Contracts)

On Friday, February 5, 2016, hackers posing as officials from Bangladesh’s central bank sent thirty-five requests to the Federal Reserve Bank of New York to transfer $951 million out of the Bangladesh central bank’s account and into private accounts in the Philippines and Sri Lanka. In Bangladesh, Friday falls on the weekend and officials only found out what had happened 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wired to personal bank accounts in the Philippines rang alarm bells,” but the money already sent to the Philippines was withdrawn and spent on difficult to track down casino chips.¹ If two large governmental institutions are unable to recover stolen funds in a case as large as this one, imagine being an online merchant and victim of lots of small, fraudulent orders. Getting money back from quasi-anonymous hackers is easier said than done.

Electronic commerce vastly expands a business’s potential customer and partner base, but it also exposes it to countless unreliable parties from around the globe. In contrast to a small-town brick-and-mortar business that can know all of its customers or business partners or at least check the identification of credit card users, electronic commerce firms face a potentially unlimited supply of unscrupulous customers. Fraud against merchants can take the form of unauthorized transactions from stolen accounts / identity theft; “friendly fraud,” where a customer places an order but later denies it or claims the goods did not arrive; fraudulent requests for returns or refunds; or lost or stolen merchandise. Figure 1

¹ The authors appreciate the helpful comments and suggestions from Denis Schweizer, Douglas Cumming, Sofia Johan, H.R. Rao, Amy Fontinelle, participants at New York University’s Colloquium on Market Institutions & Economic Processes, and participants at Concordia University’s Conference on Entrepreneurship, the Internet, and Fraud.
compares losses incurred by physical point-of-sale merchants (brick and mortar stores) with those incurred by electronic merchants for each of these categories. While physical point-of-sale merchants lose the most money from lost or stolen merchandise (e.g., shoplifting and employee theft), that category is the least important for electronic commerce firms who instead see 79 percent of fraud losses stemming from friendly fraud, fraudulent requests for returns or refunds, and unauthorized transactions.

Merchants can also be defrauded by affiliates who are paid to refer customers but end up sending fake ones or real ones who are misled by the affiliate and later want their money back. When a customer disputes an order, credit card companies typically issue a chargeback, crediting the customer for the order amount and debiting it from the merchant’s account. Risk management company LexisNexis Risk Solutions estimates the cost of existing card fraud at more than $10 billion per year, and that figure does not include the uncountable lost opportunities from trade that never occurred because of the risk of fraud. Electronic commerce firm Riskified writes, “While every chargeback incurred is painfully noticeable, falsely declined orders mostly go unnoticed and unreported.” It refers to orders that do not take place but should have as an “invisible problem.”

What legal recourse do merchants victimized by fraud have? A combination of governmental and private mandates (e.g., the United States Federal Reserve’s Regulation Z or contractually created credit-card network rules) say merchants or banks—not consumers—have to bear the cost of card-not-present fraud, and as a practical matter, merchants have almost no options to recover stolen funds. Even when merchants can prove that fraud occurred, identifying the fraudsters in the quasi-anonymous Internet is often difficult or impossible. And even when merchants can identify the fraudsters, initiating legal proceedings or recovering money from criminals 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 the funds to pay for what it owes. Such a situation can be characterized as a type of large-scale sequential prisoners’ dilemma, where bad transactions can spiral out of control and prevent good transactions from taking place at all. Finance professor Martin Boyer theorized that when “the proportion of agents that have a low propensity to tell the truth is high,” then “resistance to fraud is futile.” Economics Nobel laureate Douglass North and law and economics scholar Richard Epstein 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. Figure 2 shows that the annual sales of nonstore retailers (a figure that includes catalogues, door to door sales, and electronic commerce) in the United States have increased over the past two decades, mainly from the growth of electronic commerce. Research firm eMarketer estimates the worldwide volume of business from consumer electronic commerce at $1.5 trillion per year, with the size of those markets by region as follows:

- Asia-Pacific, $525 billion
• North America, $483 billion
• Western Europe, $347 billion
• Central and Eastern Europe, $58 billion
• Latin America, $58 billion
• Middle East and Africa, $34 billion.

Figure 3 shows growth estimates of current and future electronic commerce sales as a percentage of all retail sales by country, with China and the United Kingdom having the highest percentages.

[Insert Figure 2 about here]

[Insert Figure 3 about here]

How is all that possible when online merchants have limited legal protections against fraud? Various 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 fraudulent transactions. It 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 solve problems ex post (after they occur), electronic commerce firms have implemented various steps to deal with problems ex ante (before they occur).

**Two Paradigms of How Firms Should Deal with Online Fraud: Ex Post Legal Enforcement versus Ex Ante Prevention**

An important innovator in the early days of the Internet was PayPal, which developed a system of human-augmented artificial intelligence named Igor to help predict and turn down fraudulent transactions. Other firms innovated and adapted to market changes. One example is former software retailer Software.net, which refocused itself as a fraud prevention firm, CyberSource, and was purchased by Visa in 2010.

In addition to these more established payment networks, many start-ups and large banks are investing in technology associated with cryptocurrencies to potentially reduce fraud and expedite payment settlement. Blockchain technology, a distributed database that keeps records of who owns and protocol for transferring ownership, offers the potential for prereconciliation of trade, and computer-evaluated and enforced "smart contracts" offer various opportunities ensure delivery of service and payment. Still in their infancy, online platforms and marketplaces including Digital Asset Modeling Language, 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 JPMorgan vice president Blythe Masters suggests that the blockchain should be taken as seriously as the development of the Internet in early 1990s. The better that intermediaries are at privately reducing problems with contracts that sour, the more attractive commerce becomes.

The number of noncash payment transactions currently exceeds 100 billion per year, and the sky would be the limit for bad transactions if payment processors lacked fraud prevention efforts. But imagine if businesses had to go to court for even 1 percent of these
transactions: it could add a billion cases to the court system per year. The potential for fraud will always exist, and attempts at it will almost certainly continue to become more sophisticated. Yet companies that live and die with the success of online commerce will continue to look for better solutions for reducing fraud. Online commerce is possible because of private solutions that prevent fraud from occurring.

**Ex Post Enforcement in Theory**

Most academic theories of how people should deal with online fraud seem to be influenced by the structure of our legal system, which attempts to deal with problems after they occur. If something bad happens, the victim calls upon law enforcement to rectify the situation. In the standard law and economics framework, the threat of punishment from law enforcement also deters future wrongdoing as well. If the payoffs from cheating exceed the payoffs from legitimate behavior, the government steps in to increase the likelihood or severity of punishment 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 enforcing laws against fraud. North, 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 writes, “The returns on opportunism, cheating, and shirking rise in complex societies. A coercive third party is essential.”

Brooks and Button advocate the creation of a nationalized police response to online fraud and worry about the trend where “fraud is seen as a private matter.” They conclude that without the police dealing with online fraud, “This could also create a vacuum where organisations have no need of the police.”

Government officials have expressed similar sentiment since the early days of the Internet. In 2000, U.S. Attorney General Janet Reno argued that government enforcement against cybercrime needed to be more effective. She stated 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.”

Thomas Kubic, former deputy assistant director of the Federal Bureau of Investigation, came up with a 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.”

**Ex Post Enforcement in Practice**
In theory, each of these conditions could be met, but as a practical matter, government may be unable to meet them. Consider the experience of PayPal, an early facilitator of online commerce and an early victim of online fraud. Founded in December 1998, PayPal had 1,000 users by November 1999, 10,000 by December 1999, 100,000 by February 2000, and 1 million by April 2000. But PayPal had not predicted the amount and degree of sophistication of the fraudulent schemes against it. Some fraudsters specialized in stealing and selling passwords, and others specialized in making use of them. In 2001 and 2002, revenue averaged $1.2 million and $4 million per month, but by early 2001, fraud was costing PayPal more than $10 million per month. PayPal approached various law enforcement agencies, sometimes with evidence showing the wrongdoings of the exact culprit, but the government was ill-equipped, from both a technological and legal point of view, to solve PayPal’s problems. In an interview, PayPal founder Peter Thiel recounted to Stringham, “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.”

Did government meet the conditions that Reno said government needs to have? Stringham presented Reno’s conditions to Thiel and he said, “Every single one taken by itself seems extremely farfetched. If that’s the threshold, it’s no wonder it doesn’t work.” Thiel described how PayPal initially attempted to report problems to law enforcement, but, he said, “The level of incompetence we dealt with was amazing. At the time, he said 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, they were of little help. Thiel said:

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?’

Stringham heard a similar story when he interviewed another founder, Jeff Berwick, of a 1990s firm doing business online who told him what happened when hackers broke into his system and were potentially ruining his company. He said that after his initial call to the police, they sent an officer to do a report. When the police officer asked what happened, the founder reported, “Someone broke into my computers.” The police officer then asked to view the room with the computers and began looking around at the room’s windows and doors, then asked, “Where did they break in from?” The entrepreneur stated, “From the Internet.” The police officer then stated, “What’s the Internet?”

Although law enforcement professionals are more knowledgeable about the Internet now than they were in the years when online commerce emerged, that does not mean they now have the ability or interested in helping online merchants. Brooks and Button are two scholars who believe government should deal with online fraud rather than using a “system of backdoor ‘privatisation.’” Yet even they recognize that cases from the United Kingdom’s Serious Fraud Office, the only police entity for combating fraud, dealt with a total of thirteen cases for all of 2009–2010. Many of those cases dealt with nonpayment of taxes as opposed
to fraud against merchants, and only one involved a civil recovery order. They report the police declining to investigate a £100,000 fraud case because "the investigation of fraud is extremely expensive in terms of hours spent obtaining statements and preparing a prosecution case."\footnote{15}

A survey of Financial Times Stock Exchange 100 companies (the largest companies listed on the London Stock Exchange) about their experience dealing with police indicates similar findings. Companies report:

- The police are particularly unresponsive and uncooperative.
- Police not interested in frauds of less than £100K!! Poor response generally!
- Police do not appear to take cases of ‘minor’ fraud seriously. You have to prepare the case for the police, ie evidence, etc, without this, they [the police] are not too interested in a minor offence.
- Anecdotal evidence suggests a low likelihood of police involvement in fraud below £100K in the UK. Crown Prosecution Service adds another layer that may still lead to no prosecution.
- The Police will not undertake major fraud on our behalf. They require the evidence to be provided to them once we have undertaken our own investigations.
- [Our company] operates across the world … in many third world countries there is no fraud investigation capability by the local police. Corruption is so rife we are often compelled to apply preventive measures and then take no further action.\footnote{16}

If government will not investigate cases of fraud of less than £100,000, consider the plight of merchants who are victims of small scale fraud. In a process known as carding, for example, fraudsters place low-dollar-amount orders to verify that a stolen card is still active before using the card or selling it to others for higher valued fraud. Merchants that offer low-priced trial offers for online services are common victims of such schemes. Even if one wished for more police action against fraudsters, merchants hit with many small fraudulent orders cannot rely on the police to get their money back. That means merchants can either suffer losses and potentially be bankrupted from online fraud or take private steps to solve it.

**The Alternative of Ex Ante Prevention of Fraud: Entrepreneurial Solutions from PayPal**

Fraud was an increasingly important problem for PayPal, and it led to the demise of PayPal’s competitors eMoneyMail, PayPlace, and PayMe.\footnote{17} PayMe, for example, tried to put the burden of fraud on its users by requiring “buyers to agree that all payments were final and not reversible,” but that made the product unattractive to users.\footnote{18} PayPal recognized the value of having many users and realized it needed to provide assurances to them. Yet with little legal recourse, PayPal realized it had to come up with an entrepreneurial solution to online fraud. Thiel told Stringham in an interview, “The government approach assumes that you can solve everything after a problem occurs. It might have worked in a small-town
setting, where everyone knows everyone else, but it clearly does not work in the current world.” Thiel summarized the issue and its solution by saying, “There are two ways of dealing with fraud: predictive versus backward looking.”

PayPal first expanded its private security team to two dozen employees, but it soon noticed that these individuals could only effectively monitor a fraction of the company’s transactions. That realization led to PayPal’s important solution: programming a fraud monitoring and prevention system that would spot potentially fraudulent transactions and stop them from being authorized. PayPal co-founder and chief technology officer Max Levchin stated, “We mine millions and millions of transactions in real time,” PayPal’s system looked for suspicious 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. For example, a person who usually makes small payments among friends in the Bay Area is not likely to suddenly make a large payment to someone in Nigeria and the system would notice this is likely an unauthorized transaction. PayPal cofounder and chief technology officer Max Levchin said, “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.”

The key to ex ante fraud prevention is to develop ways of predicting whether a transaction is likely to be good or bad. For example, suppose fraudsters transferred $5 out of many people’s accounts in the middle of the night and withdrew the money from the system in the morning. Although PayPal would have a difficult time recovering those losses, it could program its system to look out for and stop similar schemes in the future. When the system saw potentially fraudulent activity, it could take steps such as requiring extra verification for transactions, turning down transfers, freezing accounts, or flagging 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 newly compromised accounts. And because fraudsters adapt and create new schemes, PayPal had to program its system to be adaptive, to learn, and to look for new patterns over time. The detection system had to be much more sophisticated than one that simply looked for fraudulent $5 transfers in the middle of the night because the fraudsters could change their scheme to any amount at any time.

In face-to-face interactions, one can assess the reliability of the counterparty by dealing with friends or by trusting based on past experience, reputation, or visible signals of potential reliability. But how can businesses decide whom to trust when they have not met the other party and when the other party might be a compromised account? PayPal used technology to scale up well beyond close-knit groups to manage the ubiquitous dilemma of whom to trust. The solutions led to a rapidly expanding set of users.

Before PayPal was introduced to the public in late 1999, more than 90 percent of eBay auctions were paid for using checks, and within one and a half years, more than 1 million daily auctions on eBay were advertising PayPal as a method of payment. Thiel stated to Stringham, “If we had left things to the ex post method, the whole thing would have not worked.” He added, “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.” Purchased by eBay for $1.5 billion in 2002, PayPal now has 173 million accounts, processes more than
$200 billion in transactions per year, and has an industry-leading fraud loss rate of 0.5 percent. Spun off from eBay in 2015, PayPal (as of June 2016) has a market capitalization of $45 billion—$15 billion more than the market capitalization of eBay and not far from the $50 billion or $60 billion market capitalizations of long-established firms such as Morgan Stanley, American Express, and Goldman Sachs.

**Entrepreneurial Solutions from Firms Associated with Credit Cards**

Other companies have adopted practices similar to those of PayPal and have come up with important innovations, too. Even without a comprehensive fraud monitoring system like PayPal’s Igor, a company can still use technology to estimate the probability of fraud for any given transaction. In 1995, an early online software reseller called Software.net was increasingly hit by fraudulent orders and realized that unauthorized transactions were pushing it toward bankruptcy. In response, the company developed “one of the first real-time identity verification systems using a unique, automated ‘profiling’ algorithm” and eventually began marketing it to others. Simple algorithms can compare shipping and billing addresses or see if a consumer’s phone area code matches the zip code.

Its fraud prevention subsidiary, CyberSource, eventually became the core of the business, and its algorithms have become more advanced over time. Purchased by Visa for $2 billion in 2010, CyberSource analyzes the 60 billion annual transactions on the Visa network and utilizes “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 fraudulent. Figure 4 shows the amount of online commerce and fraud loss ratios per year (the amount of losses associated with fraud as a percent of revenue). As the market has expanded, so too has the amount of fraud, but the fraud loss ratio has decreased.

[Insert Figure 4 about here]

Figure 5 shows Visa’s visual representation of the choices of merchants or their agents, the payment processors, when deciding whether to proceed with an order. Visa recommends that merchants create a positive database with known valuable customers put on a white list, and a negative database that puts individuals or devices with past problems, such as bad addresses or names, on a graylist or blacklist. Orders from good customers need not go through the same levels of scrutiny as orders from new customers, while customers on a graylist may have their orders turned down or put through extra steps before being processed. For example, the Verified by Visa program requires a purchaser to provide an additional password to help authenticate a transaction, so a hacker with just a stolen credit card number will be out of luck.

[Insert Figure 5 about here]

Payment processor FirstData helps firms answer the following questions to identify potential fraud before processing an order:

- Do the billing and shipping addresses match?
• Is this an average order amount?
• Did the buyer select rush shipping?
• Is the order for an unusual number of the same item?
• Is the order for a large number of a best-selling item?
• Is the order for very high value items?
• Is the shopper using a free, web-based email address?
• Is the computing device from which the transaction originates located in a high-risk region?
• Is the computing device from which the transaction originates associated with past fraudulent transactions?
• Does the shopper’s phone number have a valid area code?
• Does the shopper’s area code match their billing address?

Simple algorithms to highlight when key variables do not match or when other parts of an order are unusual help merchants assess whether to approve or turn down an order.

**Entrepreneurial Solutions from High-Risk Payment Processors and Fraud-Management Systems**

Firms like PayPal and CyberSource offer important solutions to most merchants, but certain merchants need other solutions. Merchants in lines of business with higher chances of chargebacks, which includes fortune-telling, gambling, and adult websites, often find themselves unwelcome on traditional payment processing networks like PayPal. Digital goods merchants such as sellers of software, gift cards, printable event tickets, or digital content also have fewer ways to prove that the content was delivered to the legitimate buyer. If more than 1 percent of a merchant’s transactions result in chargebacks, MasterCard and Visa will add the merchant to their chargeback monitoring list and require the merchant to pay fees, provide reports, and cut down on chargebacks or be kicked out the network.

But merchants in high-risk lines of business have their own high-risk payment processors that have been successfully experimenting with ways to mitigate fraud. Most high-risk payment processors simply pass the cost of bad transactions on to the high-risk merchant. If the expected rate of chargebacks is high, a high-risk payment processor may require the merchant to have a “rolling reserve,” a portion of the merchant’s revenue that the payment processor sets aside and draws from when the merchant gets chargebacks. The payment processor may set aside 5 percent or 10 percent of gross sales and release extra funds from the reserve after 180 days.24

Stringham interviewed Maria Sparagis, the founder of DirectPayNet, a firm that helps high-risk merchants process payments and reduce problematic ones.25 Here, too, the firm emphasizes preventing problems from occurring. For example, DirectPayNet advises merchants to monitor sources of orders and create velocity rules that limit the number of orders from a particular set of Internet protocol addresses in any given period. The potential cost would be limiting valid orders from, say, a college campus, where many people have related IP addresses, but the potential benefit would be frustrating hackers who program computers to place many fraudulent orders. Merchants can also choose to not accept orders
from entire countries that are frequent sources of fraud or from computers whose locations are masked.

Another option is to opt in to more expensive and more comprehensive fraud mitigation systems that look out for all types of fraud, including affiliate fraud. One example is Kount, Inc.’s risk inquiry and scoring system. Among other variables, Kount’s database keeps track of customer credit cards, email addresses, and shipping addresses, and it pays attention to factors such as whether an order is placed from a big or large town or a company, library, prison, school, or satellite network. Analysts have found, for example, fraudulent orders are less likely to come from company networks (it could look bad to one’s boss) or from small towns. The system helps merchants get a more accurate assessment of whether an order is or is not fraudulent, and with a better assessment, merchants may be able to accept more orders rather than turning too many down for fear of fraud.

Kount works directly with 16,500 merchants, and also has partnerships with JP Morgan Chase to help merchants accept money through Chase. Consider, for example, the case of online music platform Spotify, which came out with an e-card product that allowed users to buy gift subscriptions for friends. Spotify reports that it was heavily hit with online fraud and that "even with new fraud prevention processes in place, fraud attacks spiked in February 2013. Our chargeback rate hit 10% and we were paying thousands each month in fines. We were forced to take down the e-card product once again." After having to pay $145,000 per month in chargebacks for e-cards, Spotify subscribed to Kount’s service and the result was that “we went from a 10% chargeback rate on e-card transactions to 0.1%–0.2%. It’s a tremendous achievement, we were amazed by the results.”

Going one step further, merchants can hire a company to assume and manage their fraud risk. At a basic level, a merchant can purchase chargeback insurance, but without reducing costs associated with fraud, the merchant ultimately would pay for fraud anyway through insurance premiums. Firms such as Riskified offer a more comprehensive solution and decide on the merchant’s behalf what orders to process, then assume the cost of orders that go bad. When a merchant pays an intermediary to assume the cost of fraud, the intermediary has an incentive to reduce such costs. At the same time, Riskified cannot err on the side of turning down too many orders, as that harms the merchant in another way.

**Treating the Problem of Fraud As a Problem of Risk Management**

The importance of ex ante solutions to online fraud is appreciated by a few academics, but the importance of using technology to prevent fraud is widely recognized by industry experts, and the amount of corporate writing on this topic is large. Rather than processing all orders and then going to law enforcement for transactions that go bad, merchants or their agents in the payment processing system assign a probability that a trade will go well or poorly and then weigh 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 firm must decide how much risk it is willing to assume and such a decision must always be a balancing act. Firms must weigh the costs of type I and type II errors: the costs of accepting bad orders versus turning down good orders.

For example, fraud mitigation firm Verifi discusses the importance of protecting against online fraud and advocates layers of protection, but at the same time, the firm stresses the cost of overprotection and states 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.”

Riskified points out that false declines not only result in lost sales revenue for the transactions turned down, but also lost customer lifetime value, lost growth opportunities, and wasted acquisition costs. Riskified points out, “Merchants who employ overly restrictive fraud measures may have the best intentions, but a false decline can seriously diminish future purchasing revenue: nearly 6 in 10 (58%) declined cardholders report that they either limited or ceased their patronage of the merchant following the decline, and 32% report that they stopped shopping with the merchant entirely.”

The perspective is quite different from the standard legal and regulatory responses that tend to be binary and less attuned to letting market participants balance risks. In their search for profits, firms operating in this space must price the risks of fraud and then seek to manage them. But herein lies the beauty of the system. Even if laws against fraud are ineffective and the possibility of recovering assets from fraudsters is zero, transactions can still take place among even the most risk-averse traders when transacting parties can hire intermediaries to pool or even insure risks, thus pricing them into the cost of a transaction. The process transforms the risk of fraud into a predictable cost of doing business, and it enables parties with various risk profiles to smoothly transact. Those transacting in higher-risk businesses can use high-risk payment processors (some charge merchants upward of 15 percent per transaction), just as riskier borrowers can borrow money by paying higher interest rates.

Once a business quantifies the cost of fraud, the business can attempt to minimize it, like other costs. An advantage of the risk-mitigation approach over a legalistic approach is that firms get constant feedback about their fraud prevention efforts: merchants that process too many bad orders get penalized with chargebacks, while a merchant that turns away good customers loses profits.

Riskified recommends a scientific approach and instructs merchants to develop hypotheses about borderline cases, measure outcomes, and adjust choices over time. If a merchant starts getting too many chargebacks on a particular type of order, the merchant should become more diligent with what orders it accepts. Visa also recommends that merchants should compare the number of likely fraudulent orders that they see but decline with the number of fraudulent orders that go through.

Figure 6 presents CyberSource’s portrayal of the problem of fraud losses and false declines as similar to profit leaks in a pipeline. With risk management, the objective is never to decrease fraud to zero; the best way to do that would be to turn down all orders and do no business at all. Effective risk management encourages firms to reduce bad outcomes and expand good ones.
Entrepreneurial Solutions of the Future: The Potential for Blockchain and Smart Contract Technologies

Attempts at fraud will become more sophisticated over time and merchants will need to come up with more advanced steps to mitigate it. Some high-risk payment processor like DirectPayNet currently advise firms about how to do business with cryptocurrencies like Bitcoin. Bitcoin has many possible advantages to merchants: it enables them to receive instant payment and to not have to worry about chargebacks from consumers who later deny the purchase. On the other hand, Bitcoin has certain risks, because if users have their accounts hacked, former owners have no way to reverse transactions or recover funds.

But today’s potential problems are tomorrow’s potential solutions. New platforms and marketplaces like Digital Asset Modeling Language, Ethereum, and OpenBazaar are building on aspects of blockchain technology and allow others to program many layers of assurance. A recent innovation with a lot of potential is the algorithmically enforced “smart contract,” a term coined by computer scientist Nick Szabo. A smart contract is programmed to be enforced by a machine when certain conditions are met. At the simplest level, think of a vending machine, which is programmed to release a candy bar when a customer inserts a dollar and selects that item. At a more complex level, a smart contract can be linked to money on a blockchain and any number of events. For example, two parties can wager about a sporting match and have an algorithm visit NHL.com to learn the final game’s outcome and release payment to the winner. Digital Asset Holdings explains the objective:

The primary goal of blockchains with inbuilt Smart Contracts was to create self-enforcing agreements that independently control and automate the exchange of value according to predetermined rules based on predefined inputs. As with Bitcoin, Smart Contract platforms like Ethereum were designed to minimize the role of trust and enable actors that did not know each other to enter into software-enforced contractual agreements that are censorship resistant, meaning neither party, nor even governments can tamper with or prevent their execution.

Although parties may want human review and interpretation for certain contracts, a high percentage can easily be programmed and adjudicated algorithmically using if-then statements. For example, if you place a limit order with your stockbroker, the contract is a set of if-then instructions: if the price of Microsoft stock falls to $45, then buy one share. Or if a bank buys a credit default swap contract, the contract takes the form of: if a bond has a credit event and the International Swaps and Derivatives Association determines that the bond is worth 40 cents on the dollar, then a holder of a credit default swap is entitled to $0.60. Tying such contracts to a blockchain and having them algorithmically executed can ensure that the money is in the other party’s account and the contract is instantly executed. Gone will be the days when a customer can say, “The check is in the mail,” or when either party can neglect to follow through with its half of an arrangement.

A smart contract can be entirely algorithmically enforced or it can be programmed to allow for the possibility of human oversight or escrow. Similar to how corporations typically require multiple signatures on large-value checks, one can create multisignature smart contracts.
contracts. In a 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, but if one party does not agree, an arbitrator is brought in to evaluate the situation and to decide what to do with the items in escrow.

Simply programming a smart contract is not a silver bullet against all fraud. At a simple level, a poorly programmed smart contract that looks for an NHL score on NBA.com will not work, and at a more complex level, an entity might have some well-programmed smart contracts but remain vulnerable to fraud in other ways. An example of a potentially innovative but poorly designed entity relying on smart contracts was an investment fund called The DAO. In June 2016, about a month after it raised the equivalent of $150 million in the cryptocurrency Ether, hackers initiated transactions to take $55 million from it. On the plus side, The DAO’s code specified a 27-day waiting period before funds could be removed, so the sponsors reversed the fraudulent transactions and decided to liquidate the fund and return all the money to its investors. As with any new area, many people will likely underestimate the cunning of fraudsters. Over time, however, firms will likely learn from others’ mistakes and make these new environments more secure.

One of the more professional companies in this space is Digital Asset Holdings, which focuses on creating a secure and not completely public blockchain that established financial institutions can use. Unlike Bitcoin, these private blockchains are distributed on and powered by the servers of various banks, and they require various levels of permission from member banks before transactions are approved. That contrasts with bitcoin, which allows any two parties to transact without a financial intermediary. Now in their early stages, these private blockchains are currently used to exchange stocks, dollars, or other financial instruments, and they help to settle trades much more quickly than the three days that is common with stock transactions today. NASDAQ, for example, is currently experimenting with blockchain technology to keep track of ownership and transactions for certain non-publicly traded stocks. Digital Asset Holdings has investors from many large firms in the financial service industry including Accenture, the Australian Securities Exchange, BNP Paribas, Citi, the Chicago Mercantile Exchange, the Depository Trust and Clearing Corporation, Deutsche Börse, Goldman Sachs, IBM, and JPMorgan Chase.

As of early 2016, JPMorgan was experimenting with blockchain technology to transfer funds for 2,200 clients and had decided to increase its investments in new technology to $9 billion per year. A recent memo states, “As we look ahead to 2016, one of our major priorities will be to aggressively pursue the innovative technologies that we have been making investments in . . . We have also established teams dedicated to areas such as blockchain technology.” The firm’s CEO, Jamie Dimon, stated in his annual letter to shareholders, “Competitors are coming in the payments area. You all have read about Bitcoin, merchants building their own networks, PayPal and PayPal look-alikes . . . Rest assured, we analyze all of our competitors in excruciating detail—so we can learn what they are doing and develop our own strategies accordingly.” Just as past technological improvements from PayPal have been important for enabling electronic commerce, it seems the potential for future technological advances surrounding blockchains and smart contracts is large.

Concluding Thoughts
The expansion of commerce is not just about coming up with more goods to sell, but also about developing improved mechanisms to assure payment in markets other than simple markets where goods and money are exchanged on the spot. From goldsmith banker certificates and letters of credit a few centuries ago to credit cards today, improved financial intermediation provides assurances to reduce counterparty risk and fraud. Modern firms such as PayPal and CyberSource use technology to solve the age-old problem of deciding whom to trust. Even though merchants have a limited ability to track down stolen funds from quasi-anonymous fraudsters around the globe, firms rely on predictive analytics and other mechanisms to prevent fraud.

Despite the limited legal recourse against fraud, electronic commerce thrives. Relying on an entrepreneurial, rather than a legal or regulatory, approach for preventing online fraud has many advantages. In contrast to regulators, who do not lose profits when they prevent legitimate transactions or fail to recover fraud losses, firms that live or die with the success of commerce have an incentive to eliminate problems. With a market for fraud prevention, payment platforms or financial intermediaries will compete and come up with better solutions for merchants. The better a platform or intermediary is at helping merchants accept good orders and turn down bad orders, the more attractive it becomes. In the constant game of cat and mouse, those that find better ways of preventing fraud will profit by helping commerce to expand.
FIGURE 1. Distribution of Fraud Losses for Electronic versus Physical Point-of-Sale Merchants

[Bar chart showing the distribution of fraud losses for electronic and physical point-of-sale merchants.]

Source: Data from LexisNexis Risk Solutions, 2016 True Cost of Fraud Study (Alpharetta, GA: Reed Elsevier, 2016), p. 12.

FIGURE 2. Annual Sales for U.S. Nonstore Retailers (in $ billions)

[Line chart showing the annual sales for U.S. nonstore retailers from 1992 to 2015.]

**FIGURE 3.** eMarketer’s Projections of Retail Electronic Commerce Sales as a Percent of Total Retail Sales by Country

![Graph showing projections for retail electronic commerce sales by country from 2013 to 2018.]

Source: eMarketer, “Retail Sales Worldwide Will Top $22 Trillion This Year,” eMarketer.com, December 23, 2014.

**FIGURE 4.** Fraud Loss Ratio as a Percent of Revenue and Value of Online Commerce per Year

![Graph showing the fraud loss ratio and value of online commerce from 2001 to 2012.]

**FIGURE 5.** Visa’s Representation of Decision Tree to Process or Decline Orders

FIGURE 6. CyberSource’s Representation of a Risk Management Pipeline


---


3 Riskified, How to Avoid False Declines: Guide for eCommerce Merchants (Tel Aviv: Riskified, 2015), p. 4.

4 Card-not-present transactions are those where a customer does not physically hand the card to merchants or swipe the card in front of the merchant and that includes mail order, telephone, internet, or recurring purchases. For a discussion of the about how merchants or banks must bear the cost of card-not-present fraud, see Kevin V. Tu, “Regulating the New Cashless World,” Alabama Law Review, 65/1 (2013): 77–138, p. 120.


7 eMarketer, “Global B2C Ecommerce Sales to Hit $1.5 Trillion This Year Driven by Growth in Emerging Markets,” eMarketer.com, February 3, 2014.


9 Douglass C. North, op cit., p. 12, p. 35.


An area with a parallel problem and related solutions is investments in start-ups with difficult-to-enforce contracts between investors and founders. In theory, an angel investor or venture capitalist could sue a founder that misuses funds or that represents an investment as better than it really is. We know, however, that three out of four start-ups fail and 30 percent to 40 percent end up with zero assets, and even the best court cannot recover funds in such a case. But even though many firms fail, investors have to weigh the cost of potentially investing in a bad company against the opportunity cost of not investing in a good company. Ahlers, Cumming, Guenther, and Schweizer discuss how start-ups attempting to raise money must signal to investors that they are trustworthy and how the investor must evaluate them when deciding which risks to assume. 


Many financial regulations, for example, aim to minimize the chance that a loss will occur, but do so at the expense of disallowing transactions with positive expected returns. In contrast to the legalistic approach, good risk management entails merchants weighing the costs of accepting bad orders or turning away good ones. 


12 Personal Interview by Edward Peter Stringham, Palo Alto, October 12, 2004. Unless otherwise noted, quotes from Thiel are from this interview, although Stringham has spoken with Thiel multiple times.
14 Personal interview by Edward Peter Stringham, Hartford, March 14, 2016.
22 CyberSource, “Company History,” CyberSource.com
26 Kount, Cutting Chargeback Costs and Expanding Internationally is Music to Spotify’s Ears (Boise: Kount, 2013).
29 Many financial regulations, for example, aim to minimize the chance that a loss will occur, but do so at the expense of disallowing transactions with positive expected returns. In contrast to the legalistic approach, good risk management entails merchants weighing the costs of accepting bad orders or turning away good ones.
31 Riskified, How to Avoid False Declines, op cit., p. 11.
In April 2016, Digital Asset Holdings purchased a Swiss smart contract start-up, Elevence, and its “powerful modeling language capable of expressing any right or obligation, including cash, securities and derivatives, whereby the code defines the considerations between parties, and determines how these contractual relations can evolve over time.” Digital Asset Holdings, “Introducing the Digital Asset Modeling Language: A Powerful Alternative to Smart Contracts for Financial Institutions,” news release, April 20, 2016.

