

# **Ex ante risk management by PayPal and other intermediaries: How technologically advanced markets can work even when fraud is “legal”**

**By**

**Edward Stringham**

## 1. INTRODUCTION

In October 1999 a Silicon Valley startup began enabling electronic payments between anyone with an email address. No expensive merchant terminal or revealing personal financial information were required. The service that became PayPal had 1,000 users by November, 10,000 by December, 100,000 by February, and 1 million users by April (Thiel, 2004). Growth was good, but they had not predicted the degree and sophistication of fraud. Annual revenues for 2001 and 2002 were \$14 and \$48 million (Prashanth, 2004, p.5), but by early 2001 fraud was costing PayPal more \$10 million per month (Levchin, 2008, p.6). The schemes against PayPal were many. Some fraudsters would specialize in stealing and selling passwords and others would specialize in exploiting them. In one common scheme, fraudsters would send themselves small sums from multiple accounts, and at the end of the day withdraw the money outside of PayPal. By the time PayPal and the users noticed, the fraudster would be long gone. What to do?

Electronic commerce is not fundamentally different from more traditional forms of trade, but it poses certain challenges. It vastly expands the size of markets, but also exposes people to millions of potential fraudsters around the world. One often has little idea who one is dealing with

---

\* This document is a draft of Chapter 8 of a book that I am writing, *Private Governance* (Oxford University Press). The chapter is in its early stages so I have yet to fully go through the document to fix typos and sentence structure. Comments about content and arguments are most appreciated.

and whether they are who they say they are. Theorists like Douglass North argue that exchange without government is possible but only in small and simple settings. North (1990, p.12) states 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.”

North and others are correct that fraud is potentially profitable and the traditional discipline of repeated dealings offer little constraints in certain contexts. The only problem with North’s theory is that those exact same conditions (large groups, technologically advanced, degrees of anonymity, and interaction across political boundaries,) also make government enforcement more difficult or impossible. As transactions become anonymous, not only are private parties unaware who is swindling them, but so too is government. And even if government can track down a fraudster it may have limited ability to recover assets from them. Suing a fraudster from Nigeria is not that easy. To the swindled, government “solutions” are often too little too late. Government can have as many rules against fraud as they want, but if the less able they can enforce them, the situation is not much different from if fraud were legal.

By now I hope everyone has noticed the theme. Rather than observing a problem and doing nothing about it, PayPal realized their fate was on the line and that they had to take matters of governance into their own hands. PayPal developed a sophisticated fraud system that used human and artificial intelligence to help them prevent fraud before it occurred. Their system would constantly monitor account activity and flag transactions that were more likely to be fraudulent.

Similarly, American Express, Master Card, Visa, and others associated with the payment card industry also face the conditions described by North (large groups, degrees of anonymity,

technologically advanced, and interaction across political boundaries). A merchant can fulfill an order only to find out that the order was placed on a stolen credit card, or cardholder might place an order from fraudster with no intention of filling it, and government's ability to rectify the situation ex post is often close to zero. So rather than setting up a system that depends on government enforcement ex post, intermediaries offer to assume and manage many of the risks of fraud. Financial intermediaries treat risk management like any other economic good, and the better they are at preventing problems ex ante, the less relevant government's inability to deal with problems becomes.

## 2. IT'S NOT SUCH A SIMPLE OR SMALL WORLD, AFTER ALL; WHEN LAWS AGAINST FRAUD ARE IRRELEVANT

Fraud was hitting the new online payment processors hard and led to the downfall of PayPal's competitors eMoneyMail, PayMe, and PayPlace (Jackson, 2004, p.202). PayPal's founder and CEO Peter Thiel started out fairly skeptical of government, so one might expect that his priors were to recognize the ineffectiveness of government enforcement. But as he relayed to me, "I did not appreciate the whole enforcement of fraud problem until after I was at Paypal. The problem is not solvable in any standard government context" (Personal Interview, Palo Alto, October 12, 2004).<sup>1</sup> Using traditional methods of ex post enforcement, if one is defrauded one simply contacts the police who track down the fraudsters, bring them to court, and order them to repay what they have stolen. Yet doing so is easier said than done. The internet (and international trade in general) brings people from all over the globe into one commercial community, but it does not bring everyone under the control of any one government.

---

<sup>1</sup> Unless otherwise noted, quotes from Thiel are from this main interview although I have had the opportunity to talk with Thiel multiple times.

In a more technologically advanced world characterized with impersonal, often anonymous, interaction, problems of government enforcement are often particularly pronounced. At the height of PayPal's initial ascent, U.S. Attorney General Janet Reno (2000) recognized that government enforcement against cybercrime was ineffective. 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." (4) "Effective partnerships with other nations to encourage them to enact laws that adequately address cybercrime and to provide assistance in cybercrime investigations."<sup>2</sup> If the government is deficient in any of these ways, government can lack the ability to effectively enforce laws against fraud.

I presented this list to Peter Thiel and he responded, "Every single one taken by itself seems extremely farfetched. If that's the threshold, it's no wonder it doesn't work." How expert were the government officials? 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 did internal investigation and figured out that a man named Mr. Yagolnitsler was defrauding the company of money. After reporting the culprit to the authorities, was law enforcement any 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. Yagolnitsler is

---

<sup>2</sup> Kubic (2001) of the Federal Bureau of Investigation expressed a similar sentiment: "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."

not going to go to the police, but maybe we can go to the police and report Mr. Yagolnitsler. 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?'

The assumption that technologically advanced markets depend on government seems wildly unrealistic. Another employee of a Silicon Valley security firm, he told me, "In my view, government is ten years behind what's going on" (Personal interview, San Jose, California. June 30, 2004).

In addition to government being unable to identify who was doing what they lacked the ability to enforce laws around the globe. Peter Thiel said, "Anything that was outside the US was just hopeless." Thiel (2004) also recounted, "There was a jurisdictional dispute between the FBI office in San Jose and San Francisco over which of them had jurisdiction over Kazakhstan, and which could handle it. So there were some very serious sorts of problems." When interaction takes place across political boundaries then government often lacks the ability to enforce the rules (President's Working Group on Unlawful Conduct on the Internet, 2000, p.40).

So conditions that theorists like North assert make private enforcement "impossible," can also make government enforcement impossible. 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." These problems are pronounced with electronic commerce, but they can even be present with what appear to be the simplest face-to-face transactions. In a particularly absurd example, when I lived in San Francisco my friend's sister decided to buy two laptop computers from a street person who showed her the box with a computer chord coming out of it. She gave him \$40, and when she got home she saw that her two laptops were actually two phone books! If a city is big enough calling the cops and getting an unknown street person arraigned to recover \$40 is not that feasible. The lesson was not, "Rely on more effective government enforcement mechanisms next time," but instead "Be more

careful and practice better due diligence next time.” If only there were a service to help people like Julie.

In settings with high degrees of anonymity, advanced technology, and interaction across political boundaries, private parties must look elsewhere than government. As Thiel (2004) 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.” The work goes on behind the scenes so much of what they do is underappreciated aspects of markets.

At the end of the day users just need to know they are safe transacting over a network, in much the same way that car owners need not know everything that went into building the engine. To assure to the customer their car worked, PayPal assumed many of the risks of fraud.<sup>3</sup> Becoming the residual claimant for fraud reduction efforts, they had incentives to minimize problems just as carmakers offering warranties have incentives to make cars more reliable.

PayPal started with many innovations that have now become commonplace. Cofounder Max Levchin helped create the Gausebeck-Levchin test, one of the first commercial implementation of Captcha where users are asked to retype distorted text that programs have difficulty recognizing. They also took other measures to verify legitimacy of each account, like depositing a few cents into customers’ checking account and asking them to verify those amounts, but with each new safeguard came new types of fraudulent schemes. Consider just one example that Peter Thiel described to me of a would-be-fraudster taking payments to ship a video game console when it was released in two

---

<sup>3</sup> Although certain laws like the Electronic Fund Transfer Act officially regulate how PayPal deals with victims of fraud, even if the laws did not exist I see little reason why exposing consumers to fraud would have been a profitable business model. Many of the regulations only apply to individuals and not merchants, yet PayPal offers fraud protection to all parties. Similarly the credit card industry has limits on holding individual cardholders liable for fraudulent charges, but even though regulations do not apply to business accounts, merchants are offered many assurances. Merchants also can purchase insurance against chargebacks indicating that paying others to assume risks is market phenomenon rather than a product of regulations.

months. A promise of “We will send you the XBox videogame console by Christmas,” allowed the fraudster to collect the money now and have weeks to plan his getaway. The fraudster had already taken in \$800,000 from customers and was in the process of transferring \$100,000 to a bank outside PayPal when they noticed something potentially going wrong. PayPal’s interest was different from intellectual puzzle solving in a detective novel, because PayPal knew they would be on the hook for money lost. Thiel summarized the issue, “There are two ways of dealing with fraud: Predictive versus backward looking.” *Business Week* described PayPal’s work as that of a “‘pre-crime’ detective” (Black, 2002). In the case of the bogus Xbox shipments, PayPal noticed the fraudulent scheme as it was happening and was able to freeze the fraudsters account before much money was lost.

PayPal was expanding their private security team to a couple dozen when they noticed that they could only effectively monitor a fraction of the transactions. As a solution, cofounder Max Levchin led the development a fraud monitoring and prevention system that would spot potentially fraudulent transactions and alert their team of suspicious patterns of behavior (Levchin, 2008, 11). Levchin stated, “We mine millions and millions of transactions in real time” (quoted in Schwartz, 2001). Their system would look for patterns like 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). They looked at past behavior but the system was also programmed to learn and look for new types of fraud over time. If the transactions were likely fraudulent PayPal would not process them or freeze an account. If the transactions were indeed legitimate, they could ask customers to take additional steps to confirm they were making the transaction.

Early on, they recognized that the success of PayPal hinged on how well they assessed and managed risk of fraud. Levchin said:

I think a good way to describe PayPal is: a security company pretending to be a financial services company. What PayPal does is judge the risk of a transaction and occasionally actually

take the risk on. You don't really know the money's good; you just sort of assess the riskiness of both parties. (2008, p.10)

The key was to assess risk, and weigh Type I and Type II errors. Losing from a fraudulent order is not a good thing, but neither is turning down all orders with a miniscule probability of fraud. PayPal had an incentive deal with risks in a reasonable way in contrast to government officials who lack feedback about whether they are being too lax or too zealous (for example, did it make sense to spend tens of millions of tax dollars to prosecute a baseball player for potentially not being forthright about using performance-enhancing drugs?).

By reformulating questions from, "How can we rely on government after a problem occurs?" to "What can we do to make sure that problems do not occur?" they eliminated the "need" to rely on government enforcement. To Thiel the reasoning was clear: "There is nothing unique to government about being able to predict things....There is no reason to believe that government is better at predicting than the private sector...In fact government is so bad at it."

PayPal solved an important problem and they were rewarded for that fact. Before PayPal arrived in late 1999, over 90 percent of eBay auctions were paid using checks (Schwartz, 2001), and only a half year later more than 1 million daily auctions eBay were advertising PayPal. Purchased by eBay for \$1.5 billion in 2002, PayPal now has 109.8 million accounts and processes more than \$118 billion in transactions per year (Sengupta, 2012). Their fraud loss rate is an industry leading 0.5 percent (PayPal, 2012).

PayPal's innovations also were matched with innovation from their more traditional competitors. Firms associated with the payment card industry like American Express, MasterCard, and Visa also have taken many steps to deal with and reduce the problem of fraud. For example, the payment processor and risk management firm CyberSource was originally a software reseller that realized that "online customers were reluctant to purchase unless their buying experience felt completely secure, simple, and seamless." They created "one of the first real-time identity

verification systems using a unique, automated ‘profiling’ algorithm” and eventually began marketing to others (CyberSource, 2012b). Purchased by Visa for \$2 billion in 2010, CyberSource analyzes the 60 billion annual transactions on the Visa network in their efforts to reduce the problem of fraud. Predictive analytics, probabilistic risk assessment, and scoring systems help estimate whether a transaction is likely to be bad.

These firms view fraud in much more of an economic way than the theorist who assumes transactions cannot occur without government rules against fraud. CyberSource characterizes fraud and efforts to deal with it as profit leaks along a Risk Management Pipeline (See Figure 1) and they offer various levels of fraud management services. They recognize that one must weigh the impact of fraud with the cost of enforcement efforts including “the additional customer experience ‘costs’ of rejecting valid orders, staffing manual review, administration of fraud claims, as well as challenges with scaling fraud management operations as business grows” (CyberSource, 2012a, p.2). Among online merchants, 97 percent use validation services like address verification, and 67 percent use often more advanced “proprietary data/customer history tools” like fraud scoring models which estimate the likelihood that a transaction is valid. A fraud scoring model looks at numerous variables (such as what the order is for, where the order is from, and other the variables summarized in Figure 2) and accepts, rejects, or flags an order for manual review. Each merchant is able to decide how much risk they are willing to bear when accepting or rejecting transactions, and decide how many fraud prevention tools they want to utilize. Among merchants using automated screening, “68% of merchants report using at least 3 tools in their automated screening solution and an average of 4.9 tools overall. Larger merchants processing higher order volumes use an average of 8 tools.” The potential for fraud will always remain, but Figure 3 shows that payment processors have been successful at bringing losses from fraud from 3 percent of revenues in 2001 to roughly 1 percent

today. The better the private sector is at eliminating problems, the less “essential” North’s essential coercive third party really is.



Figure 1: Transaction Risk Management Pipeline as Characterized by CyberSource (2012, p.2)

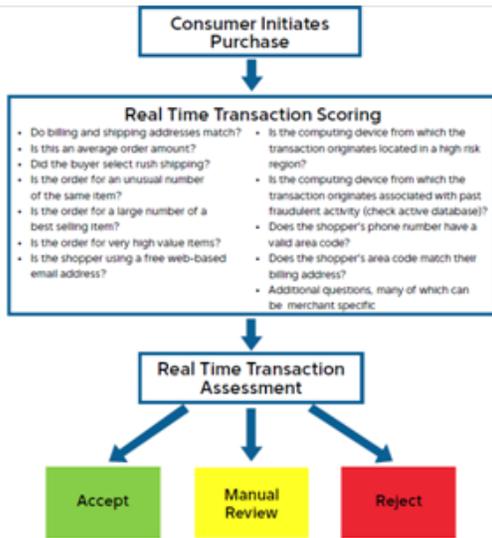


Figure 2 The Transaction Assessment and Acceptance Choice Set (Source: FirstData, 2010, p.7)

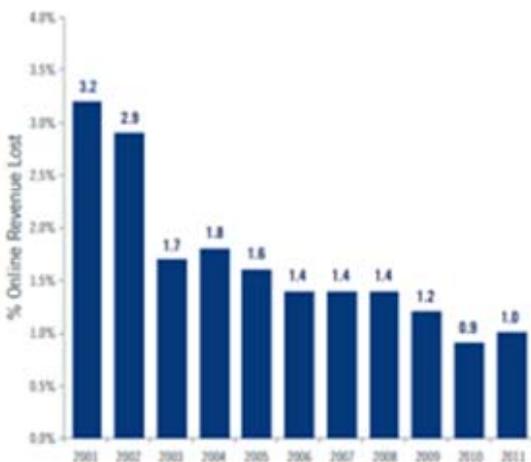


Figure 3 Merchant Losses to Online Fraud (CyberSource, 2012, p.1)

### 3. THE MARKET FOR FRAUD MANAGEMENT

Law and economics scholars usually think about goods at the margin rather than in all or nothing terms, but when it comes to assuring parties make legitimate contracts many abandon their marginalist perspective. For example, Epstein (1999, p. 285) argues one would be a “naïve visionary” to “believe that markets could operate of their own volition without any kind of support from the state.” While discussing laws against fraud Epstein writes, “The rule of law becomes critical to offer a secure framework for these voluntary transactions to take place.” But while legal centralists suggest that the private sector must wait for government to create a secure framework, the private sector treats the problem quite differently. What legal centralists consider enforcement problems are instead treated by the private sector as risk management problems.

A loss from fraud is quantifiable just like any other loss, and firms will take steps to minimize them just like any other loss. A firm that can reduce losses for itself captures those benefits, and a firm that can help reduce losses for others can market those benefits to others. For example, CyberSource started out as an online store solving their own problems and then it began selling solutions to others. The private sector did not need to look into academic debates about

whether fraud management was a public good. Instead they saw fraud management as a service that can be priced and sold thereby filling in a “missing market” in this realm.

The market for fraud management created by estimating the probability of fraud for various transactions, pricing those risks, and then taking steps to manage them. At the risk of upsetting economists who think human choices cannot be quantified using probabilities because the future is radically uncertain (Lachmann, 1994, p.120), I will mention that lenders have done this since time immemorial when they charge higher interest rates to parties with higher likelihood of default (Rothbard, 1977).<sup>4</sup> Transacting parties must estimate the likelihood that counterparties will have the ability and intention to follow their promises (Dufie and Zhu, 2010) and also what one can expect to recover if a problem occurs. Where certain transacting parties, like mortgage lenders, can foreclose on the assets purchased with a loan, many, like credit card or unsecured debt lenders, are unable to recover significant assets if the other party fails to follow his half of the bargain. Many firms, like those conducting business over the internet, have a very limited ability to recover assets from those who defrauded them.

But herein lies the beauty of the market. 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. This can happen when transacting parties can hire intermediaries to pool and insure risks pricing them into the cost of a transaction. All of this transforms the risk of fraud into a predictable cost of doing business, and it enables parties with various risk profiles to smoothly transact. For example, even if 10 percent of total sales in a particular area go bad, payment processors will still process them if they charge 10 percentage point higher transaction fees.<sup>5</sup> Those

---

<sup>4</sup> Those who believe that human choices cannot be quantified using probabilities should either unwilling to loan to anyone because “the future is radically uncertain” or be just as willing to invest at the same interest rate in junk bonds versus AAA rated debt (good luck with that strategy).

<sup>5</sup> One of the more problematic aspects of price controls on interchange fees in the Dodd Frank Act of 2010 is that it will interfere with payment processors’ ability to price the cost of fraud into transactions.

transacting in higher risk areas can transact using the aptly named high risk payment processors (some charge merchants upwards of 15 percent per transaction), just as more risky borrowers can borrow money by paying higher interest rates. Payment processors constantly collect data on rates of fraud and chargebacks, which are higher with certain product categories like bankruptcy attorneys, consumer electronics, adult content, gambling, and fortune tellers (alas fortune tellers cannot always predict the future perfectly). If a merchant gets too many chargebacks it can get kicked out of its payment processor network meaning that parties are likely to be pooled with others of similar risk levels. The more accurately risks are pooled and priced into the cost of transactions, the less problematic fraud becomes when recovering assets ex post is not an option.

Although insured risks will not cripple any individual making transactions, risk premiums for fraud can still discourage trade at the margin, and if left unchecked, fraud can lead to adverse selection problems with legitimate traders leaving of the market, further pushing up risk premiums. Here payment processors and other financial intermediaries provide their important behind the scenes role. Intermediaries make money by facilitating transactions, and any one that can ceteris paribus lower transaction costs, including lower costs of fraud, will gain. This makes them residual claimants for successful fraud management, and the better they are at keeping fraudsters out, the lower the risk premiums they will have to charge. In the constant game of cat and mouse, firms that find better ways of keeping fraudsters at bay, will gain.

Notice that all of this works even though many potentials for “market failure” exist. First, all of it works even though parties do not have perfect information about the other party or all of the fraudulent schemes that could occur. As long as one hires an intermediary to assume and manage those risks transacting parties just need to trust that one party. Second, all of this works even in the presence of network effects associated with fraud reduction. The value of a payment system certainly depends on how many others want to use it (PayPal recognized this from day one when

they decided to give \$10 to each new user and \$10 more for referring a friend), but, if anything, network effects help explain why fraud management has been done more effectively by the private sector. PayPal alone has more users than almost every country has citizens (China, India, and the United States being the only exceptions), has strong incentives to invest in technologies that increase the value of their network. Your local police department or federal government officials do not have those same incentives. Fraud reduction is often considered a public good, but law enforcement agencies have limited resources and one should not be surprised if officials around the globe do not consider reducing fraud for merchants or consumers among their top priorities (Reno, 2000.) Intermediaries hired to manage fraud, on the other hand, are residual claimants for successful fraud reduction, and they internalize the benefits of their investments.

#### 4. SUMMARY AND THOUGHTS.

In a high technology world with relatively anonymous interaction across political boundaries, government's ability to deal with fraud is quite limited. PayPal, and likely most all electronic commerce, would likely not exist had they been depending on government to enforce contracts over the internet. When they realized that could not rely government to rectify occurrences of fraud, PayPal found many ways to minimize problems before they occurred.

The risk management services of electronic payment processors are representative of a much wider phenomenon where firms deal with risks of problems *ex ante* rather than *ex post*. Hiring others to conduct proper due diligence (the accounting firm, the underwriter, or the rating agency) helps certify that an entity is the real deal, and hiring others to assume risks reduce firms' exposure when any one thing goes wrong. Having your car stolen and not getting it back is not the worst thing in the world if you purchased insurance, or having a loan you made defaulted on is not the

worst thing in the world if you purchased a credit default swap.<sup>6</sup> Hiring an exchange to facilitate these transactions further reduces risks. In futures markets, transacting parties hire the Chicago Mercantile Exchange or another exchange assume and manage counterparty default risks. When two parties seemingly make a contract with each other, they are actually each making separate contracts with the futures exchange, so they need not worry about the other party defaulting (Deutsche Borse Group, 2008, p.16). The futures exchange then works to minimize problems with margin, daily settlement, and other trading requirements. By managing risk in the most sophisticated markets the world have ever seen (Chicago Mercantile Exchange Group process billions of transactions per year and the notional value of contracts on all futures exchanges exceeds world GDP [CME Group, 2011]), these intermediaries eliminate the “need” to have billions of contracts enforced in court. Easterbrook and Fischel (1996, p.283) write “a rule against fraud is not an essential or even necessarily an important ingredient of securities markets” and I will add the same is true for all markets.

Hayek (1945) used the world marvel to describe the price system, and I will add that the fraud management system of financial intermediaries is also marvelous. They allow us to make transactions with nearly anyone in the world while keeping problems of fraud to a minimum. Payment processors don’t tax half of our income, and instead provide these crucial services for a just couple percentage points.

### **References being edited by my assistant**

---

<sup>6</sup> For an excellent discussion of the widely misunderstood and, in my opinion, unfairly maligned credit default swaps see Stultz (2010). Stultz points out that even during the financial crisis of 2008 most credit default swaps were still performing and the problematic ones were simply an indicator of economywide problems rather than the cause of them. Although I have a small amount of sympathy when firms like Goldman Sachs practice poor risk management and put too many eggs in one the basket of firm like AIG, which itself did not proper risk management when it issued credit default swaps, I see no reason that taxpayers should have to bailout Goldman Sachs and AIG for their poor risk management. The best way to minimize the future risk of insurers like AIG and customers like Goldman Sachs from practicing poor risk management is to let them pay for their errors rather than shifting these losses to taxpayers.

- Black, Jane (2002) Insert details from: [http://www.businessweek.com/technology/content/oct2002/tc2002101\\_0628.htm](http://www.businessweek.com/technology/content/oct2002/tc2002101_0628.htm) Include date.
- CME Group 2011 <http://www.cmegroup.com/education/files/BIS-OTC-Markets.pdf> As a document authored by a corporation, please list the corporation as the author and please have the reference formatted with the same details as a book or monograph. That means List the corporation is the Author, Year, Title of Document, Location of Corporation, and then list the Corporation again as the Publisher.
- CyberSource 2012b Insert details from: <http://www.cybersource.com/company/history/> As a document authored by a corporation, please list the corporation as the author and please have the reference formatted with the same details as a book or monograph. That means List the corporation is the Author, Year, Title of Document, Location of Corporation, and then list the Corporation again as the Publisher.
- CyberSource 2012a Insert details from: 2012 Online Fraud Report [http://www.jpmmorgan.com/cm/BlobServer/Payments\\_Fraud\\_Information\\_Resources.pdf?blobkey=id&blobnocache=true&blobwhere=1320552298829&blobheader=application%2Fpdf&blobcol=urldata&blobtable=MungoBlobs](http://www.jpmmorgan.com/cm/BlobServer/Payments_Fraud_Information_Resources.pdf?blobkey=id&blobnocache=true&blobwhere=1320552298829&blobheader=application%2Fpdf&blobcol=urldata&blobtable=MungoBlobs) As a document authored by a corporation, please list the corporation as the author and please have the reference formatted with the same details as a book or monograph. That means List the corporation is the Author, Year, Title of Document, Location of Corporation, and then list the Corporation again as the Publisher.
- Deutsche Borse Group, 2008 Insert details from: [http://math.nyu.edu/faculty/avellane/global\\_derivatives\\_market.pdf](http://math.nyu.edu/faculty/avellane/global_derivatives_market.pdf)
- Duffie and Zhu 2010 Insert details from: <http://www.stanford.edu/~duffie/DuffieZhu.pdf>. After searching for the name of this article search on the internet to see if it has been accepted or published and if so insert the name of the journal.
- Easterbrook and Fischel INSERT their first names. 1996 *The Economic Structure of Corporate Law*. Cambridge: Harvard University Press.
- Epstein Richard A., *Hayekian Socialism*, Search internet to find the full reference for this. The abbreviated citation info is: 58 Md. L. Rev. 271 (1999).
- First Data 2010 <http://www.firstdata.com/downloads/thought-leadership/ecommmfraudwp.pdf>
- Hayek 1945 *Use of Knowledge in Society*. Search the internet to find full details.
- Jackson, Eric M. (2004) *The PayPal Wars: Battles with eBay, the Media, the Mafia, and the Rest of Planet Earth*. INSERT CITY AND PUBLISHER DETAILS FROM THE INTERNET.
- Kubic, Thomas T. 2001 Statement for the Record, House Committee on the Judiciary, Subcommittee on Crime, June 12, 2001. This is all the reference information that we need.
- Lachmann Ludwig 1994 *Expectations and the Meaning of Institutions*. London: Routledge.
- Levchin, Max 2008 "Interview between Max Levchin and Jessica Livingston" Pages 1-16 in *Founders at Work: Stories of Startups' Early Days* By Jessica Livingston. Search internet for name of publisher and location.
- North Douglas C, *Institutions, Institutional Change and Economic Performance*, (Cambridge: Cambridge University Press) (1990)
- PayPal 2012 Insert details from: [https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing\\_CommandDriven/bizui/BusinessSecurity-outside](https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing_CommandDriven/bizui/BusinessSecurity-outside) As a document authored by a corporation, please list the corporation as the author and please have the reference formatted with the same details as a book or monograph. That means List the corporation is the Author, Year, Title of Document, Location of Corporation, and then list the Corporation again as the Publisher.
- Prashanth, 2004 insert details from: <http://xa.yimg.com/kq/groups/20452006/112783859/name/Paypal.pdf>

- President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, March 2000.
- Reno Janet, Statement of Janet Reno Attorney General of the United State Before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, and State, "Cybercrime" February 16, 2000.
- Rothbard 1977 Insert details from: <http://www.econlib.org/library/NPDBooks/Fetter/ftCIR0.html> Have this formatted like a chapter in a book edited by someone else.
- Schwartz, Evan (2001) "Digital Cash Payoff: Online Payment Services Like PayPal are Catching On" *MIT Enterprise Technology Review*, December 2001.
- Sengupta (2012) insert details from: <http://www.nytimes.com/2012/04/19/technology/ebay-earnings-surpass-forecasts.html> Include the specific date for all periodical publications.
- Stultz 2010 Insert details from <http://www.cob.ohio-state.edu/fin/faculty/stulz/publishedpapers/jep%2024%201.pdf>
- Thiel, Peter 2004 "Innovation, Entrepreneurship and the Global Marketplace," Presentation at Independent Institute, San Francisco, CA April 21, 2004. This is all we need for that.