TRUST, RISK AND ELECTRONIC COMMERCE: NINETEENTH CENTURY LESSONS FOR THE TWENTY-FIRST CENTURY

Karen Clay and Robert Strauss*

A Paper to be Presented at the
93rd Annual Conference on Taxation
National Tax Association
Session on Taxation and Ecommerce

November 9, 2000
1:30-3:00 PM
El Dorado Hotel
Santa Fe, New Mexico

*H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213-3890; Email: kclay@andrew.cmu.edu, rs9f@andrew.cmu.edu. This paper is the sole responsibility of the authors.

1. INTRODUCTION

The growth of remote commerce, notably business to consumer (B2C) electronic commerce, has begun to slow. For instance, for the key holiday season, Internet sales tripled from 1997 to1998 and doubled from 1998 to 1999. This year, however, Jupiter estimates that sales will increase only 66 percent. Sixty-six percent or even more optimistic estimates of 100 percent by Forrester may seem large, but these increases still represent a very small fraction of total sales through physical channels.[1]

B2C is, however, almost certainly in its infancy. At the moment, it is being held back both by technical barriers and by issues of trust and risk. On the technical side, the barriers are bandwidth and delivery. Bandwidth restrictions coupled with graphics laden pages make many merchants' web pages frustratingly slow to view at standard modem speeds. And if a customer does place an order, gratification is typically very delayed – standard delivery often takes a week or more. Several vendors have been experimenting with standard same day or 24-hour delivery in urban areas like New York City. Technical improvements in the optimization of warehouse locations, order processing, integration with delivery companies, and increased density on delivery routes, should eventually lead to standard 24-hour delivery for a large fraction of the population, making gratification more immediate.

When surveyed, customers and increasingly merchants regularly identify issues of trust and risk as important barriers to electronic commerce. Concerns to consumers about remote merchant conduct include: the risk of merchant opportunism where goods or services are not ever delivered, or, when delivered, are of lower quality than represented;

[1] Web Retailers' Growth Spurt May Be Ebbing, Boston Globe, Sept. 18, 2000.

the risk of misuse of personal information (privacy violations) by merchants either opportunistically or accidentally or by third parties seeking this information to engage in credit card fraud. The primary concern for merchants about remote consumers' conduct involves credit card fraud, particularly for information goods. Firms engaged in B2C, alone or with the help of governments, have strong incentives to mitigate these problems. We believe they will successfully resolve these problems.

Once the technical barriers and issues of trust and risk have been resolved, remote commerce will begin to have real tax implications for states under the current tax regime. If, as we argue below, use of remote commerce is correlated with the opportunity cost of time and therefore income, some states will be harder hit than others. Specifically, affluent states such as California or New York, that have relatively high proportions of their population in the top quartile or decile of the national income distribution, will be harder hit than poorer states. They will be harder hit for two reasons unless *Bella Hess* and *Qull* are overturned and/or federal legislation is enacted which obligate remote vendors without domestic nexus to collect and remit to the consumer's state of residence: individuals will not pay sales tax on most remote commerce and remote commerce will cause a partial crowding out of local commerce, further reducing tax revenues. Our purpose here is not to provide numerical estimates of the extent to which these will occur, but rather to describe, through comparative analysis, the circumstances under which they are likely to occur.[2]

[2] There is a wide range of estimates of current and near term revenue consequences to the state and local sector of ecommerce on sales and use tax collections. See Cline and Neubig(1999), Fox and Bruce (2000), and Mcphillips (2000) for (respectively) small, large and very large estimates of revenue losses to the state and local sector of ecommerce. Also see GAO(2000) for other estimates.

The remainder of this paper is organized as follows. First, we lay out an informal model of the factors that lead to opportunism in either goods or personal information. Then we discuss problems that arose in the 19th century with the development of remote commerce, the effect of the rise of universal credit cards and the fall in data transmission costs during the mid-20th century, and the impact of the development of the internet at the end of the 20th century. With a clearer understanding of the problems that we face today in remote B2C commerce, we outline some possible solutions to the key problems of trust and risk. Finally, we discuss the implication of a dramatic increase in remote B2C for states.

2. TRUST AND RISK FROM THE 19TH CENTURY THROUGH THE MID 20TH CENTURY

Consider a merchant and customer engaging in remote commerce.[3] Customers are concerned about the risk of merchant opportunism, i.e., that the consumer would send money, and the merchant would either not send anything or send a good of lower quality than described in the printed catalog. To mitigate this problem, the merchant sends the good in return for partial payment, thereby extending credit to the customer. As long as the merchant is making a profit and the customer gains something beyond what can be had from a local merchant, both parties benefit from any transaction. This benefit plus the link between past behavior and future interaction through reputation gives both merchants and customers incentives to be honest. Merchants have an incentive to send goods of the appropriate quality and customers have an incentive to repay the merchant, because the gain from cheating is small relative to the value of future interactions.

[3] This paragraph describes a standard two sided moral hazard problem. There may also be elements of adverse selection, to the extent that there is heterogeneity across merchants or across customers.

The problems faced by merchants and customers in the foregoing description closely match the problems Richard Sears and his customers faced in the late 1880s when he first began to sell mail order watches.[4] Sears would send goods in return for partial payment. If the customer was not happy, he could return the good with no questions asked and receive his money back. If the customer was happy, he would repay the credit over time.[5] Sears and his competitors offered rural customers a compelling value proposition: greater selection, higher quality, and lower prices than were available from local merchants. Sears and a small number of other firms such as Montgomery Ward built national reputations based on this value proposition and quality service. These firms had no incentive to cheat customers, because the value of future transactions was larger than any gains that could be had from not delivering merchandise or otherwise defrauding customers. Customers also had little incentive to cheat Sears. They could, of course, run up a bill at Sears and then not pay. Sears, however, carefully monitored the amount of credit that customers received. Failure to pay, among other things, meant losing the ability to order from Sears, a privilege that most were loath to forgo.

It is worthwhile highlighting a number of institutional features that would later change. After the initial phase in which stores like Sears and Montgomery Ward grew from nothing to be large merchants, the cost of becoming a remote merchant was high. Remote merchants had to print catalogs, maintain warehouses, provide credit and establish a reputation for honesty. Suppose that customers believed that dealing with small remote merchants was riskier, in the sense that those merchants were more likely to not send goods, to not send goods of appropriate quality, or to not accept returns. Then

[4] This paragraph is based on Gordon L. Weil, Sears, Roebuck, U.S.A, 1977.

customers were likely to deal with them only if they offered a specialty product or had significantly better terms than the major catalog companies. Further, customers may have been more likely to accept credit and not pay, because the gains to future interaction were lower. Thus, reputation together with economies of scale and scope may have acted as effective barriers to new remote sellers. Although the exact causes are uncertain, what we currently observe is a fairly small number of large merchants engaged in B2C.

The delay between a customer sending an order and receiving the goods was measured in weeks. First, the order made its way through the post to the company. There a clerk processed the order and then order was assembled, packaged for delivery, and shipped via train and later truck. At the other end, the order was delivered to a post office or catalog store, and the customer was notified that his goods were available for pickup. If the mails were slow or the good was not in stock, the delay could increase from weeks to months.

In this 19th century era of handwritten ledgers and typewriters, data transmission was extremely costly, so privacy was not much of a problem. Some customer information was undoubtedly sold for certain high value purposes; however, it was likely difficulty and expensive to manipulate for profitable use. For instance, very upscale department stores might sell customer lists to dealers that sold exclusive cars. In general, however, the cost of selling lists of customer information was too high to be practicable.

Finally, the incidence of fraud was low, because the costs of getting information were sizeable, the probability of being caught was high, and the gains were typically small. First, the person had to acquire the necessary information, which may have been

[5] Like other merchants of the period, the cost of the credit was included in the price of the good. This made accounting simpler and allowed merchants to avoid state banking and usury laws. [*reference*].

more or less costly than the present. With the information in hand, the person could place an order. Since orders were typically handwritten and merchants kept copies of correspondence, clerks were likely to notice if the handwriting was radically different. Goods sold were physically shipped to customers, who almost always had to sign for their packages at the post office or catalog store.[6] Moreover, the chances were high that person behind the counter knew the person whose name was on the package. So if a fraudulent order were shipped, the person would have to intercept it in transit to or at the post office or catalog store.[7] Overall, the likelihood of being caught was high. Finally, merchants monitored accounts and imposed limits on the amount of credit they would extend, so the magnitude of the gains was limited.

3. TRUST AND RISK IN THE MID TO LATE 20TH CENTURY

Consumer credit continued to be a feature of the retail landscape with local merchants, department stores, and major catalog vendors, among others, continuing to extend credit to customers. The major advance of this period was the development of universal, entertainment oriented, credit cards. The founders of Diners Club, the first universal card, observed that salesmen in New York ate out nearly every night. Their innovation was to recognize that rather than having each restaurant offer accounts to all of their regular customers and having each customer maintain accounts at all of the restaurants in which they regularly ate, it was efficient for both salesmen and restaurants to deal with a single entity. And so, in 1949 the first universal credit card was born. Although merchant to customer credit continued to be important, within a decade, the

[6] One effect of this was to mitigate any incentive a customer would have to claim that the good did not arrive, even if it did.

[7] A person could file a change of address for the person they were impersonating, but this is likely to be difficult in a rural town where post office employees would know if a resident was moving.

number of individuals and merchants that used or accepted universal cards had increased enormously. Expansion in consumer confidence and therefore use was enhanced by passage of legislation in 1970 that limited cardholder liability if the card was used to commit credit card fraud to $50 under most conditions.[8] Table 1 shows the explosion of consumer use of revolving credit, most of which is credit card credit.

Credit card companies could efficiently monitor both individuals and merchants. The fixed costs of monitoring and billing customers could be spread over more transactions than in merchant to customer transactions, thereby diminishing the cost to merchants. Customers got a consolidated bill, and, in the event of a dispute, they may have had more leverage over merchants. For instance, customers through the credit card company could refuse to pay the entire bill, rather just the amount outstanding after the down payment. Moreover, through its initial screening and ongoing dealings with merchants, the credit card company indicated that an unknown vendor was at least minimally reputable.

Because a remote merchant no longer had to provide credit, the cost of entry had fallen.[9] The fall in the cost of entry and other factors such as expanded availability of consumer credit and limitations on consumer liability, the number of remote merchants increased. Their average size was still fairly large, although smaller than before.

The time from placement of an order to the arrival of the goods had shortened relative to the previous era. One improvement lay in the increased use of telephones to place orders. Another lay in increased use of airplanes and truck to move packages from

[8] The other big innovation in 1970 was the introduction of standardized magnetic strips on credit cards.
[9] Remote merchants may not have needed to offer credit, if amounts were small and customers are willing to pay cash. This, however, presupposes that a remote merchant was large enough to have a reputation and therefore to be trusted.

warehouses to homes. Other improvements included use of computers to better forecast demand and thereby insure that goods were in stock and optimization of warehouses to decrease the time necessary to fill and pack orders. Delivery of packages to the home rather than a post office or catalog store became the norm. And increasingly delivery was handled by a specialized third party company such as the United Parcel Service or Federal Express.

Another thing that had fallen was the cost of data transmission. Using more sophisticated typewriters and later emerging computer technology, remote merchants and credit cards began to collect personal data and to share it with major credit agencies and other merchants. Consumers were not overly sensitized to privacy issues, perhaps because the primary manifestation, direct mail, was relatively unobtrusive. One dark side to the fall in the cost of data transmission was that more people had access to more data than ever before, making the risk of theft and subsequent credit card fraud by employees or third parties more likely.

More generally, the cost of obtaining the information necessary to commit credit card fraud was probably falling. Waiters, clerks, and anyone else with access to credit cards could copy down numbers or falsify slips. And numbers obtained from face to face or remote transactions were regularly bought and sold on the street. The emergence of markets in stolen credit cards was a reflection of a deeper change in the costs and benefits of credit card fraud.[10]

The probability of being caught had fallen, and the gains to fraud were higher. Remote merchants were larger, so clerks no longer had the personal knowledge of customers and their order patterns necessary to spot suspicious activity. Unlike face to

face transactions, a remote merchant could not see customer X, so it was impossible to make a reasonable judgement about whether X was who he or she claimed to be. At least initially, it was nearly impossible to determine whether a card was valid or stolen within a reasonable period of time. At the same time, urbanization made it less likely that the person behind the counter would know the person picking up the package or notice if a false change of address card had been submitted.

Universal credit cards made it possible for thief to rack up charges much more quickly, because he could hit a large number of physical or remote stores within short period of time. Similar activity within a single store or chain would have been more likely to be noticed either by a clerk or by the person in the back office who processed credit receipts before sending them on to the head office. As noted above, the cost of data transmission had fallen, but initially this was not enough to allow merchants to check credit with the credit card company in real time. Thus, a thief might have had days or even weeks before the credit card company became aware of the fraud and was able to transmit that information back to stores. Even when the information did become available, it was a constant hassle for firms to check the lists to see whether a particular card had been stolen while other customers waited in line.

The result was that the overall incidence of credit card fraud was high. In 1973, fraud represented 1.15 percent of sales. By 1980 industry efforts had driven the rate for universal cards down to 0.52 percent of sales. This was still high, however, relative to current rates of around 0.06 percent of sales for card present (physical retail) transactions. The highest incidence of fraud was in airline travel cards, gas cards, and mail order. The first two reflected the fact that airlines did not issue lists of stolen cards, and gas

[10] Lewis Mandell, The Credit Card Industry: A History, pp. 64-69.

attendants rarely checked cards. The last, mail order, did not require a card at all, only a name and valid card number.

Credit card companies worked assiduously to further lower the incidence of fraud using a combination of education and technology. They mounted education campaigns aimed at merchants to help them identify fraudulent transactions: techniques included checking and comparing signatures and, if necessary, identification through the examination of a driver's license signature and photo in face to face transactions common practice. Similar campaigns aimed at consumers focused on the risks of giving out credit card information over the phone or on non-secure phone lines such as cellular lines and what to do if a card was stolen. On the technology side, credit card companies began to offer telephone verification for large transactions and when it became available real time automated verification for most amounts. The net result was a fall in fraud from 0.52 in 1980 to 0.18 percent of transactions in 1992 to 0.06 percent of transactions in 1998.

Throughout this period, a few customers may have avoided remote commerce altogether because of the risk of opportunistic behavior by merchants or third parties. In general, however, customers could trust merchants to deliver the goods and to be no more likely than average to steal credit card information. The theft or misuse of other types of personal information – invasion of privacy – was not yet a big issue, primarily because of low customer awareness.

4. CREATING TRUST AND REDUCING RISK IN THE 21ST CENTURY

The 19th and 20th centuries saw the rise of remote commerce, first with catalog merchants providing the credit and then with universal credit cards providing the credit as well. In the pre credit card era, merchants posted a bond of good behavior by offering

customers credit for most of the purchase. In both that period and later, the likelihood of future interaction was sufficient to ensure that merchants delivered what they had promised and customers repaid their bills. Over time, changes in transportation, data transmission, and the costs and benefits of fraud affected the risks for both customers and merchants. Despite the risks and delays inherent in remote commerce, it remained an attractive proposition for both merchants and customers.

Sears offered a compelling value proposition; it was a trusted merchant that offered variety and price not available from local merchants together with high levels of service. Sears has two quite different electronic commerce successors – Amazon and Ebay. Amazon offers some additional variety and perhaps marginally lower price than is available from local merchants, packaged with high levels of customer service. The compelling value proposition for many of its customers, however, is convenience – the ability to shop from a trusted merchant at any time and receive delivery within a week. Ebay offers much greater variety and lower prices than can be found in nearly any conceivable venue. This is a variant on Sears initial value proposition. Unlike Sears, however, Ebay is not the vendor, only the marketplace. The fact that Ebay specializes in consumer to consumer, or more realistically small business to consumer, means that there are significant issues of trust and risk to be resolved.[11]

What is holding electronic commerce back? As we mentioned in the introduction, bandwidth and transportation are key bottlenecks. Early predictions that catalog vendors such as L.L. Bean or Lands End would significantly reduce the number of paper catalogs

[11] We will return to these issues below.

they produce or cease publishing them altogether have been unfounded.[12] The reason is fairly simple, looking at most catalogs online is tedious, even for people like the authors who have DSL or better. In response, electronic-commerce-only sites are beginning to issue paper catalogs as an adjunct to their sites.[13] Currently only 10 percent of households have broadband (always on, ISDN, DSL, or cable). And by 2003, only 33-37 percent of households are predicted to have broadband.[14] Slow penetration is attributable to limited availability and high prices due to labor-intensive installation and limited competition.[15] As wireless, satellite, DSL, and cable, are each able to offer service to nearly all households, prices are expected to drop significantly. Table 2 shows the expected numbers of subscribers for each type of broadband from 2000 to 2005.

Within the transportation arena, there are a number of separate technological problems that have to be resolved before 24-hour delivery can become a reality. The first piece is reducing the time from the shelf to the truck that will do the final delivery. Improvements in warehouse location, supply chain management, and integration with delivery companies will reduce the time spent in this part of the process. The next piece is from truck to house. Route density is the driving factor here, because density is what will enable twice-daily or more frequent delivery for most households. A number of companies want to solve the last mile problem, including Webvan and Federal Express, possibly in partnership with the United States Postal Service. Once the truck reaches the

[12] "We saw some major consumer catalogers cut back their mailings and watched their sales dramatically decline." Your New Customer, Catalog Age, July 2000.
[13] For instance, Internet-only Garden.com launched its first catalog in Nov. 1999. There are likely to be behavioral issues as well. For instance, people read catalogs in bed or in the bathroom, places that are not conducive to online shopping. And a person on the telephone can answer questions about the product, something that web-based order forms cannot do, at least not as readily.
[14] Statistics cited by Cisco: http://www.cisco.com/warp/public/779/govtaff/factsNStats/broadband.html
[15] On the cost and difficulty of going the DSL route, see http://www.business2.com/content/magazine/breakthrough/2000/10/16/21257

house, the other key – and as yet unresolved problem – is that of secure unattended delivery. Households in which all adults work are the households most likely to use remote commerce, yet they are precisely those for whom delivery is the most problematic. For some households, packages can be left on the front porch, or in urban areas, with a doorman. In these cases, the likelihood of theft may be acceptably low. For remaining households, there are two options: creation of a secure delivery site such as a drop box or garage with keypad or extended delivery hours to ensure that someone will be home.[16]

The other key issues are those of trust and risk. What has changed from the late 20th century to make remote commerce more risky? Four things have changed, all as a result of advances in data transmission: i) the costs of becoming a merchant have fallen dramatically, ii) the cost of data transmission has fallen, iii) the form of some goods has changed from physical to digital, and iv) the probability of credit card fraud being caught has fallen.

First, the fixed and marginal costs of becoming a remote merchant have fallen dramatically with the rise of the Internet. For many goods, economies of scale remain important on and off line. Indeed, in commodity markets such as books, music, and computer equipment, we have seen a fairly rapid consolidation of web-based vendors, driven largely by economies of scale. For specialty sellers, however, the web has made it possible for them to reach large audiences much more cheaply than has been possible in the past. Expensive paper catalogs are not necessary, and problems of inventory management are diminished, because web-based catalogs can show actual holdings.

[16] We are assuming that most people will find it inconvenient to have large quantities of goods delivered to their workplace.

Thus, large numbers of sellers have been able to use the web to initiate or expand remote sales. In the limit, the rise of marketplaces such as Ebay has made it feasible for individuals and small businesses to sell to one another quite profitably.

If the propensity for opportunistic behavior is correlated with size, then the rise of large numbers of small vendors has implications for the incidence of fraud in equilibrium. Fraud does seem to have risen, most of it associated with smaller vendors. Some partial solutions have arisen to address this problem. Examples include the rise of Bizrate, Gomez, Deja, and other organizations that pool customer experiences, making reputation more important for these small firms than it otherwise might be. Ebay – probably the largest single marketplace for small vendors – explicitly incorporates reputation. Buyers can view feedback from previous buyers on their experience with a seller and vice versa. Even with these mechanisms, fraud remains persistent.[17]

Second, the fall in data transmission costs means that the risks associated with transmitting personal information are higher than ever before. It is useful to think of this in terms of the ubiquitous waiter example. People routinely hand credit cards to waiters without concern for fraud, even though the waiter could steal the number and then make fraudulent use of it. The analogy goes on to say that using the Internet is as safe as handing your card to a waiter. One problem with this story is that the waiter probably will not give your name and card number out to 10,000 people. Thus the new risk is not

[17] It is particularly problematic on Ebay, because many small vendors do not take credit cards. This forces customers to pay by check or some other cash equivalent payment system. Unless a customer explicitly chooses to use escrow, he has no recourse if the merchant acts opportunistically. For a list of Federal Trade Commission Internet Auction Fraud cases, see http://www.ftc.gov/bcp/reports/int-auction.pdf

theft but transmission. And intentional and unintentional transmissions appear to be frequent.[18] Thus the risk of using the Internet are perceived to be high.[19]

Most major merchants have implemented security to prevent third party interception of information in transit or from the site. Standard security includes encrypted data transmission and firewalls to protect data that the company maintains. Most sites store credit card information, raising the risk of third party attack. In some cases, such as AOL, credit card information is stored even if the account has been cancelled. Firewalls are not a panacea for keeping out intruders, as the recent security breech at Microsoft suggests. The biggest threat, however, is often internal. Without adequate controls, employees can access, use, or sell credit card information stored on site.[20]

Related to this is the fact that customers are much more concerned about merchant opportunism with respect to data (personal information) than previously.[21] Heightened awareness seems in part a result of the fact that the process is more transparent – entering personal data on a web page can almost immediately result in high levels of junk mail. And meta-databases such as that proposed by Double Click can offer unprecedented levels of detail about customer behavior.[22] For instance, a recent survey found that 67 percent of consumers are 'very concerned' about misuse of personal

[18] Weekly media reports of compromised data probably only represent a small fraction of the true incidence. See, for instance, Web Retailers' Growth Spurt May be Ebbing, Boston Globe, Sept. 18, 2000 on recent breeches at Eve.com, Western Union, and AOL.
[19] Exactly consumers are afraid of is unclear given that liability is limited to $50. It may be that costly outcomes such as identity theft are more common in the Internet channel than in physical channels.
[20] Little E-Shop of Horrors: Don't be Afraid to Buy Online, but Take Precautions --- and Never Use a Debit Card., The Atlanta Journal-Constitution, July 9, 2000.
[21] E-Commerce (A Special Report): Revamping the Model – Choice and Trust, Wall Street Journal, April 17, 2000.
[22] Privacy Online: Fair Information Practice in the Electronic Marketplace, A Report to Congress. Federal Trade Commission, May 2000 [Hereafter FTC]. FTC, p. 21. The FTC survey indicates that more than half

information online and another 25 percent are 'concerned.' This has a real economic impact. One study estimated foregone sales in the Internet channel of $2.8 billion in 1999. Without intervention, this could rise to $18 billion in 2002, nearly half of projected sales of $40 billion.[23] Although these numbers need to be viewed skeptically, they do suggest that the privacy problems have a real impact on the Internet channel.[24]

Third, technology has made it more efficient to deliver some previously physical goods in digital form. Examples include words, pictures, video, software and music. This change exposes a problem for merchants in the way remote commerce is currently conducted. As remote commerce with credit cards migrated from paper form to telephone orders, merchants no longer had physical signatures for orders. As long as physical goods were delivered, the signature on delivery prevented customers from accepting delivery and then claiming that the good was never delivered. If the goods are delivered in digital form, there is no longer a signature. So, customers can and do regularly accept digital goods and then claim that they were never ordered or delivered. It is also much easier to commit credit card fraud for digital goods, because the awkward issues of physical delivery are obviated. At the moment, rates of fraud are as high as 30 percent in these segments, particularly pornography. [25] The problem is so severe that American Express no longer serves merchants whose primary business is the sale of

---

of all sites permit third party (e.g. Doubleclick) placement of cookies and less than half of those tell consumers that third parties may be placing cookies.

[23] FTC, p. 2

[24] The overall impact is less clear in the sense that those same purchases may be occurring in the physical channel. American Express is tapping this market with its disposable credit card numbers good for a single transaction. American Express Credit Cards to Offer Disposable Numbers for Web Shopping. Wall Street Journal, Sept. 8, 2000.

[25] See Credit Card Fraud Bedevils Web http://www.wirednews.com/news/business/0,1367,18904,00.html and Merchants and Issuers Must Address Internet Credit Card Fraud, Card News, Sept. 6, 2000.

pornography, and Visa and Mastercard are imposing ever-stiffer penalties on sites with high levels of charge backs (one indication of fraud).[26]

Fourth, the probability of catching fraud in physical goods on the Internet is low. In telephone based mail order, the customer representative may be able to make some determination, however imperfect, of the likely validity of the order. And written mail order has a much longer lag time and therefore a higher likelihood of discovery. Thus, Internet based ordering probably represents yet another decline in the probability of being caught. This is reflected in the percentage of transactions that are charged back The largest credit card processor in the United States finds that charge backs are 0.14 percent for retail, 0.33 percent for catalogs, and 1.25 percent for the Internet. Gartner found similar differences for large retailers 1.24 percent for offline retail and 2.64 percent for online retailers.[27]

To combat this problem, merchants employ sophisticated algorithms to detect transactions that are likely to be fraudulent, such as those with different billing and ship to addresses. Even with active screening, charge backs are typically around 2 percent.[28] The problem is that these algorithms over screen, rejecting large numbers (20-40 percent) of valid transactions along with some fraudulent ones.[29] Thus, merchants are actively limiting B2C, because of problems with fraud.

5. Addressing Problems of Trust and Risk on the Internet

[26] At War Over Merchant Risk, Credit Card Management, July 2000.
[27] Credit-Card Scams Bedevil E-Stores – With No Signatures to Prove Who Placed Orders, Sites Are Left Footing the Bills, Wall Street Journal, Sept. 19, 2000. See also, Putting Your Family Heirlooms Up for Bids May Make You a Target for Credit Card Fraud, New York Times, Aug. 3, 2000.
[28] Credit-Card Scams Bedevil E-Stores – With No Signatures to Prove Who Placed Orders, Sites Are Left Footing the Bills, Wall Street Journal, Sept. 19, 2000
[29] Will e-commerce reverse card fraud trend? ABA Banking Journal, April 2000.

Three key issues of trust and risk are preventing more rapid expansion of B2C electronic commerce: i) merchant transactional opportunism, ii) merchant data opportunism, and iii) credit card fraud. In plain English, customers need to be able to trust that merchants will not act opportunistically with respect to the transaction or their personal data. And merchants need to be able to trust that customers will pay for the goods.

The first problem, transactional opportunism, is an old problem for remote commerce. Sears solved this problem by posting a bond – sending the good with only partial payment – and through the importance of reputation.[30] Today the same kind of bond is not feasible, because retailers no longer extend credit directly to customers. A similar bond of good behavior could, however, be posted with a trust third party such as Trust-e. In terms of complaints, by far the biggest problems with transactional opportunism to date have arisen with vendors in Internet auctions.[31] In this setting, auctions such as Ebay and Yahoo could permit merchants to post a substantial bond with it or a partner service.[32] The idea would be that reputable vendors would be willing to post the bond and disreputable ones would not. The bonding agency would report numbers of complaints and this would be added to the reputational information that these sites already post. Alternatively, auction sites could bundle escrow into the cost of posting goods of more than a specified value.

Reputation is an important counterpart to bonding in providing merchants with incentives to deal fairly with customers. As we noted, some third party sites such as

[30] in much the same way that reputation ensures good behavior for some large e-commerce sites today.
[31] More than half of all complaints to the Federal Trade Commission thus far have been about transactions arising from internet auctions.

Bizrate maintain information relevant for reputation. It is unclear, however, how widely such sites are used and how representative the information their information is. For reputation to play a larger role, two things are necessary – a centralized site that collects information and the posting of this information on B2C sites. A centralized site has not yet emerged, in part because reputational information is a public good. The issues of whom we trust enters into the equation as well, since some sites offer consulting services that allow participating merchants to increase their scores, diminishing their ability to act as a trusted third party. These problems suggest that a governmental agency might make a better trusted third party than a private sector corporation.

It is not enough to have ratings; the ratings of the centralized trusted third party need to be immediately visible. One possibility would be for merchants to implement this voluntarily. Another possibility is for ratings visibility to be a browser-level option.[33] Alternatively, the government could mandate the posting of ratings in much the same way that the Los Angeles department of public health mandates that restaurants in post their health inspection letter and number grade in the front window.

The second problem, data opportunism, has only recently become a significant issue in the last decade or so. [34] The term data opportunism includes a number of discrete issues including merchant tracking of customers within their site, third party tracking of customers within and across sites, the sale or exchange of customer information, without adequate notice or permission, and data security. The first step in mitigating this issue is

---

[32] The bond would guarantee delivery of a non counterfeit good that closely matched the posted description.

[33] This immediately raises complicated issues of customer preferences and identifying B2C sites. For identification, though, non B2C sites would simply not show any reputational information.

[34] Interestingly, the FTC survey showed that privacy seals have not been widely adopted overall, although 45 percent of the sites in the top 100 had them. Further, having a seal did not guarantee that the site complied with the four principles of fair information.

for sites to prominently post privacy policies that an average user can understand. Voluntary industry wide efforts on this front have had some, quite limited effects. A survey in late 1999 by the Federal Trade Commission suggest that only 20 percent overall and 42 percent of the top 100 web sites comply with the four fair information practice principles of notice, choice, access, and security.[35] Although these numbers represent an improvement over the previous year, compliance remains inadequate. On the data security front, Visa recently announced data security standards that merchants must implement by 2001.

Government intervention on data opportunism seems likely given the problems with the status quo. The form this will take is not yet clear. One possibility is government mandated privacy statements and government enforcement of the contents of these statements. Such intervention would have public support. Indeed in one recent survey, 82 percent of respondents indicated that the government should regulate the use of personal information.[36] Interestingly, unlike other forms of merchant opportunism, namely fraud, reputation mechanisms have not developed to address the problem. With government support along the lines described for fraud, however, reputation could become important. That is, if customers could observe third party ratings of merchants' privacy policies and information on merchants' violations of these policies, then merchants with poor records on privacy would be forced to improve or offer customers something else in return, such as lower prices or better service.

The third problem, credit card fraud, is an old problem that has become much more severe with the rise of universal credit cards and the Internet. Sears addressed the

[35] FTC, pp. 4, 12.
[36] Privacy: E-Firms Just Don't Get It, Los Angeles Times, May 29, 2000.

problem of customers running up debts and not paying by offering superior value and limited the amounts of credit. For most people, the value of future interaction gave them an incentive to pay. Because of the close knit nature of society in the nineteenth and twentieth centuries, fraudulently using other peoples personal information to acquire goods was fairly difficult. Sears used clerks' personal knowledge of customers as a protection against fraud. Merchants today use sophisticated software in much the same was to protect themselves. Major credit card companies are also working to address fraud. For instance, American Express will begin offering disposable credit card numbers. And customers may soon enter passwords that are routed directly to the bank to authenticate transactions or use digital signatures.[37] For digital goods, where the problem of credit card fraud is particularly severe, other steps may be necessary. For instance, merchants may only sell on a cash basis. Third parties could offer cash accounts and bear the risk of fraud. Such third parties could establish a waiting period before the digital cash is available – time for credit card fraud to be identified and checks to clear or charge premiums that reflect the level of risk that they face.

6. THE COMING EXPLOSION OF B2C, IMPLICATIONS FOR THE STATES

Over the past several years, representatives of state and local government have expressed their growing concern that the explosion of B2C activity over the Internet will fundamentally impact their ability to finance state and local services. While there is widespread disagreement[38] about how much use (as well as sales) tax has been and is currently being lost due to diversion of sales of tangible goods to the Web, and the

[37] Digital signatures (or equivalently fingerprints, retinal scans, or typing) still have unresolved data security issues.

growth in intangible goods sold over the Web, few doubt that the effects could easily be profound. Less appreciated but perhaps more important than the overall issue of revenue loss is the upheaval which will occur in state-local intergovernmental fiscal relations when the effects of diversion impact on particular urban counties. In some parts of California and elsewhere in the US, local sales and use taxes comprise as much as 15% of a jurisdiction's own-source tax revenues. Should these decelerate, or disappear as the states begin to honor their commitment to move to one rate per states, either local property and/or wage or income taxes will have to be raised, or enabled and raised, or the states will be forced to substantially enlarger their revenue sharing programs to municipal governments.

Our historical review of the way 19th century retail commerce evolved reminds us that the states followed suit by modernizing their commercial law institutions to facilitate merchant and customer concerns about risk. According to McBride, Baker and Cole(2000), within the past six months, most of the states have adopted some form of digital signature legislation whose purpose is to provide an improved level of assurance to remote vendors, primarily on the web, that their customers claims are accurate. Outstanding in most states, however, is counterpart legislation which will protect customers on the web from various forms of vendor fraud. It is readily imaginable that state inaction to reduce the risks of B2C commerce for vendors and consumers, through the enactment of either a digital Universal Commercial Code, or a uniform adoption of UCITA, will put off the supposed explosion of B2C commerce, and forestall the adverse revenue consequences which pessimists expect. On the other hand, state action to solve

[38] See Fox and Bruce (2000) and more recently McPhillips (2000) for larger estimates of lost revenues and Cline and Neubig (1999) for more modest estimates; also see GAO(2000) for a discussion of the range of

the commercial law problems facing B2C may be a precursor to achieving some sort of political solution to either convincing Congress that federal legislation is necessary to overcome *Bella Hess* and *Quill*, or finding a cooperative solution that is truly workable. At this point in time, November, 2000, it is evident that a coalition of traditional retailers and an energized state and local sector has stopped Congressional extension of the federal moratorium enacted in 1999. Whether this political ability to block a moratorium is strong enough to obtain positive enactment of federal tax legislation continues to be an issue hotly debated by combatants in the fray.

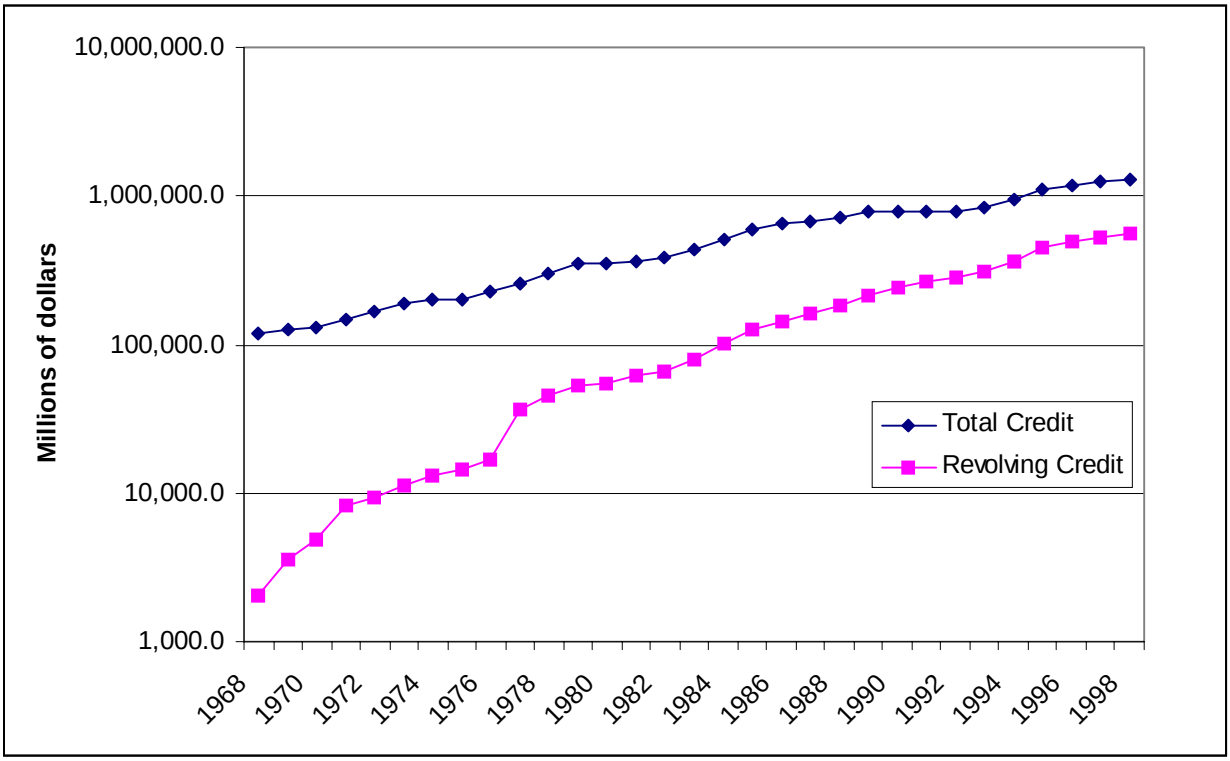
What is clear to us is that meaningful solutions to the collection and remittance of remote use tax problem will require not only vast simplifications and harmonization of extant state sales taxes, which are long overdue, but also a likely role for either the federal government through a federal agency to determine whether each state's version of a reformed sales and use tax adheres to an agreed upon template, or some other credible third party agency which could prove effective to induce both private and public sector compliance with the model statute. To one of this paper's authors, the simplest and most effective solution lies in placing the model statute in the Internal Revenue Code, and enabling the IRS to determine whether any state's sales and use tax comports with this template; however,[39] as McLure(1998) points out, a prominent role for the federal government runs afoul of state (and local) sovereignty concerns.

---

estimates.

[39] See Strauss(2000) for the details of this proposal.

Table1: Consumer Credit (Logarithmic Scale)



Notes: TABLE B–75.—Consumer credit outstanding, 1950–99, Economic Report of the President, February, 2000 based on data from the Board of Governors of the Federal Reserve System. Data on revolving credit begin in 1968.

Table 2: Millions of Households Predicted to Have Broadband

	Broadband	DSL	Cable	Wireless	Satellite
2000	3.3	2.4	3.6-5.7		
2001					
2002	16				
2003		9.3			
2004	16.6-25	13.8	24.3		3.9
2005		25	27.6	9	

Notes: Data from Cisco http://www.cisco.com/warp/public/779/govtaff/factsNStats/broadband.html Data are from different sources, so they may not sum to the broadband total.

Bibliography

ABA Banking Journal (2000), "Will e-commerce reverse card fraud trend?," April 2000.

The Atlanta Journal-Constitution (2000), "Little E-Shop of Horrors: Don't be Afraid to Buy Online, but Take Precautions --- and Never Use a Debit Card," July 9, 2000.

Boston Globe, "Web Retailers' Growth Spurt May Be Ebbing" , Sept. 18, 2000.

Card News, Sept. 6, 2000, "Merchants and Issuers Must Address Internet Credit Card Fraud",

Catalog Age, July 2000.

Cisco: http://www.cisco.com/warp/public/779/govtaff/factsNStats/broadband.html

Cline, Robert and Thomas Neubig (1999), "The Sky is Not Falling: Why State and Local Revenues Were Not Significantly Impacted by the Internet in 1998," *State Tax Notes*, July 5, 1999, p 43.-49.

Credit Card Management (2000), "At War Over Merchant Risk, " July 2000..

Duncan, Harley (1999), "State Revenue Losses from E-Commerce Underestimated," *State Tax Notes* 17, 4 (July 26, 1999), 245-246.

Federal Trade Commission (2000), *Privacy Online: Fair Information Practice in the Electronic Marketplace, A Report to Congress*. (Washington, D.C.: May 2000).

Fox, William and David Bruce (2000), "E-Commerce in the Context of Declining State Sales Tax Bases," Cetner for Business and Economic Research at the University of Tennessee (February, 2000), http://cber.bus.utk.edu

General Accounting Office (2000). *Sales Taxes: Electronic Commerce Growth Presents Challenges; Revenue Losses are Uncertain*. (Washington, D.C.: General Accounting Office, June 2000), GA)/GGD/OCE-00-165.

http://www.wirednews.com/news/business/0,1367,18904,00.html "Credit Card Fraud Bedevils Web."

http://www.ftc.gov/bcp/reports/int-auction.pdf

http://www.business2.com/content/magazine/breakthrough/2000/10/16/21257

Los Angeles Times(2000), "Privacy: E-Firms Just Don't Get It", May 29, 2000.

Mandell, Lewis, *The Credit Card Industry: A History*.

McBride, Baker, and Coles(2000), "State Digital Signature Legislation-Legislative Tables," http://www.mbc.com/ecommerce/legislative_1.asp?state=all

McLure, Charles E. Jr. (1998), "Electronic Commerce and the Tax Assignment Problem: Preserving State Sovereignty in a Digital World," *State Tax Notes*, April 13, 1169-73.

McPhillips, Sean (2000), "Sales Taxes and E-Commerce: A Practical Solution," *State Tax Notes*, 19, 13 (September 25, 2000), 835-840.

New York Times (2000), "Putting Your Family Heirlooms Up for Bids May Make You a Target for Credit Card Fraud,", Aug. 3, 2000.

Peha, Jon and Robert P. Strauss (1997), "A Primer on Changing Information Technology and the Fisc," *National Tax Journal*, 50, 3 (September, 1997), 607-621.

Strauss, Robert P. (2000), "Federal Tax Mechanisms to Enable State Taxation of Final Consumption," *Tax Notes*, 87, 12 (June 19, 2000), 1657-1664,.

Wall Street Journal (2000a), "E-Commerce (A Special Report): Revamping the Model – Choice and Trust," April 17, 2000.

Wall Street Journal (2000b), "American Express Credit Cards to Offer Disposable Numbers for Web Shopping," Sept. 8, 2000.

Wall Street Journal (2000c), "Credit-Card Scams Bedevil E-Stores – With No Signatures to Prove Who Placed Orders, Sites Are Left Footing the Bills," Sept. 19, 2000.

Weil , Gordon L (1977). *Sears, Roebuck, U.S.A.*