ETAILING: NEW OPPORTUNITIES FOR CRIME, NEW OPPORTUNITIES FOR PREVENTION

Graeme Newman
(The University at Albany, New York)

and

Ronald V. Clarke
(Rutgers, The State University of New Jersey)

PRODUCED FOR THE Foresight CRIME PREVENTION PANEL

BY THE JILL DANDO INSTITUTE of CRIME SCIENCE, UCL.

February 2002

© Crown copyright 2002

Published on behalf of the Department of Trade and Industry (DTI) Office of Science and Technology (Foresight Directorate). Applications to reproduce copyright protected material in this publication should be submitted in writing to: HMSO, Copyright Unit, St Clements House, 2-16 Colegate, Norwich NR3 1BQ. Fax: 01693 72300. e-mail: mailto:copyright@hmso.gov.uk

The views expressed in this publication should not be taken to represent those of the Department of Trade and Industry

Contents

Executive Summary and Recommendations

Introduction
Part One: The Opportunity Structure for Etailing Crimes
Crimes of the Computing Environment
Costs of crime in the etailing environment
Information as a Hot Product
The Information System as a Hot Service
The Etailing Environment
The Etailing Value Chain
Part Two: Etailing Transactions and their Vulnerabilities
Online Credit Card Payment
Benefits of the transaction
Vulnerabilities of the transaction
Digital Cash
Auctions
Benefits of online auctions
EXECUTIVE SUMMARY AND RECOMMENDATIONS

This paper places e-tailing in the context of the information society of the 21st century. It identifies the new opportunities afforded criminals to target the core of e-tailing and the information society generally: information and the systems in which this information resides. Using the perspective of situational crime prevention, it then systematically explores ways of reducing these new opportunities for crime.

Information on the Internet and other networks is analysed using the CRAVED criteria that the situational approach has applied to "hot products" of the 20th century, such as mobile phones and other electronic goods. Information rates highly on all attributes: it is easily Concealable and Removable, always Available, immensely Valuable, Enjoyable to hackers and fraudsters, and Disposable in a variety of ways over the Internet. In fact, information may become the hottest product of the 21st century.

Whereas traditional retailing requires physical handling of products by manufacturers, wholesalers and shippers, the business-to-consumer model of e-tailing depends almost entirely on information systems - that conglomeration of computers, networks, switches, software, wiring and microwaves. Information systems allow for the tracking of products through the supply chain and the collection of detailed information from customers. Merchants therefore construct large databases containing proprietary and extremely valuable information concerning their customers and products. They sometimes misuse these and invade customers' privacy, but the greater threat arises from criminal attacks on the databases. These attacks are likely to increase as the value of the databases becomes more widely recognised.

The efforts of criminals are assisted by the criminogenic attributes of information systems that are summed up by the acronym SCAREM: the Stealth permitted by aliases; the Challenge to hackers to beat the system; the value of Anonymity; the ease of Reconnoitring for ready targets; ready Escape from the crime scene; and a Multiplicity of further criminal opportunities created by a single crime.

The crime-enhancing environment described by CRAVED and SCAREM provides a setting in which new crimes emerge and old crimes find a new face. Theft, fraud, extortion, harassment, terrorism and vandalism are just a few crimes that thrive in this environment. All these crimes are a serious threat to e-tailing because of the structure (or lack of it) of the Internet itself. Because it is a worldwide network, crimes that occur in one place or even against one small target may easily affect businesses thousands of miles away. When a virus released in a distant place shuts down the web sites of merchants, the damage is as great as when a flood closes down shops in a city street. When merchants depend on the trust of their customers, and crimes of any kind are committed on the Internet, that trust is eroded. And the task of engendering trust and confidence of the customer to use the Internet to purchase goods is the greatest challenge to e-tailing.

A close analysis of the e-tailing value chain - the value of a product or service as it moves through different stages from manufacture to customer - reveals many points of vulnerability to crime. These vulnerabilities have less to do with the physical security of the product itself (though this continues to be important), than with the transactions that occur along the way of bringing the product to the customer.

The first step in focussing crime prevention efforts is to identify the major participants in the transactions making up the various stages in the e-tailing value chain, and those involved generally with the information systems. These participants are: manufacturers, merchants, trade associations, Internet service providers, police, public institutions such as colleges or public libraries, customers and, finally,
governments. The second step is to identify specific opportunities for crime that could be reduced by the four main methods of situational crime prevention: increasing the effort needed to commit the crime, increasing the perceived risks, reducing anticipated rewards, and removing excuses. Using these two dimensions - participants in the etailing process and the four opportunity-reduction methods - a wide range of concrete preventive recommendations are identified. These are summarized immediately below.

The paper concludes that the twin problems of secure etailing - of verifying the identity of customers and of ensuring personal privacy - will emerge as major issues of public policy. It is expected that technology and the markets will go a long way in both solving these issues and forcing the hand of legislators. Businesses are already introducing smart cards and other high-tech authentication procedures. What may soon emerge is the idea of a "commercial identity" that individuals maintain and use for all commercial transactions. Whether these identities will expand to encompass other non-commercial transactions remains to be seen.

Recommendations

For Manufacturers

- Design security into software and operating languages.
- Confine release of information pointing to "bugs" or "holes" in operating programs to a need to know basis.
- Source tag or chip products so that their ownership may be electronically monitored through each stage of the supply chain from production to customer reception to return.

For Merchants

- Make it harder for criminals to break into databases by: maintaining information and information systems in a physically secure location, using firewalls placed between databases and the Internet, maintaining valuable databases off line, disallowing dial up access.
- Control access by using passwords and PINS that provide differentiated access to information systems; refuse sellers with suspect transaction record at online auction sites.
- Use public-key cryptography and other digital identification methods to verify that files have not been intercepted or changed; to authenticate participants in the transaction use digital signatures and certicates.
- Require PINS to be used with credit cards; install biometric card authentication; accept only credit cards as payment, or use trusted third part online payment system.
- Establish audit trails by monitoring transactions; analyse user patterns to detect deviant use; check for "sniffers" and remove or close; encrypt all transmissions.
- Publicise strong security surveillance on web site; assess when surveillance of computing environment may be most needed and act accordingly.
- Include regular employees in security team and train them in correct security procedures; offer incentives for employee vigilance.
- Use customer service to educate consumers
- Establish community watch areas for auction sites; establish and supervise customer feedback files; monitor auction site for illegal sales and fraud.
- Protect intellectual property by abiding by copyright law and copyrighting web pages.
- Repair system damage immediately.
- Quietly announce on web site the security measures in force.
- Publish clear statement of security policy and procedures and the secure transaction protocols in force.
- Emphasise customer education, especially values, e.g., "Copying software is stealing".
- Penalise customers for breaches of security.
- Devise easy backup and restoration for customers' software; make secure transactions convenient and easy; provide ample security information.
- Peer-to-peer: provide legal service for small fee negotiated with music and video industry.

For Trade Associations

- Campaign for use of smart cards; maintain vigilance for copyright violations.
- Publish best practice guides; campaign against Internet "culture", e.g., "Hackers are vandals".
- Publish names and links to trusted online merchants and professionals.
- Provide links to organisations that rate online businesses and survey online fraud.

For Internet Service Providers

- Adopt filtering software.
Monitor illegal use of service.
Enforce responsible use policy.

For Police and Law Enforcement

- Control deception and false advertising.
- Maintain hidden presence on news groups and bulletin boards; make public announcements of fraud investigations.
- Work closely with etailers and auction sites to prosecute all attempts at fraud.
- Consistently enforce law relating to grey market commerce.

For Colleges and Public Libraries

- Enforce rights and responsibilities policy; campaign against Internet culture, e.g., "Hackers hurt innocent people".
- Require all users to acknowledge a responsible use agreement.
- Remove user rights if rules of use are not followed.

For Customers

- Keep computing devices in physically secure location; do not use hand held devices in crowded locations; install software firewall.
- Do not store passwords on computer; only give up credit card information on an authenticated secure etailing site; always query requests for personal information.
- Keep records of all transactions with etailers.
- Do not use public computers (libraries, Internet cafes) to purchase online; do not pay cash for online auction purchases; check out authenticity of web sites when purchasing grey market products.
- Check for rogue files and minimise "cookies".
- Supervise others, such as family members and friends who use the computer.
- Report suspicious emails and requests for information to Internet Service Provider (ISP) and/or etailing source.
- Participate in community watch on auctions and provide customer feedback on transactions.
- Only shop on etailing sites that digitally encrypt transactions; never pay with cash; use trusted third party for auction payments.
- Resist the temptation to become a victim to offers that are too good to be true or web sites that have appearance of authenticity.
- Read and follow customer guidelines.
- Decline to make copies of software for friends or family.
- Insist that merchants acknowledge security errors; report fraudulent activity.

For Governments

- Allow the highest level of cryptography to be used internationally.
- Set standards for secure payment transactions; protection of customer privacy.
- Pass laws requiring interception of cross border transactions in grey market products; establish security standards for ecommerce.
- Hold auction web sites responsible for illegal sales; hold Internet service providers responsible for fraudulent web sites; hold college campuses responsible for hackers.
- Work in partnership with trade associations to identify fraud and educate customers; develop best practices guides.

INTRODUCTION

The economist Peter Drucker has convincingly argued that this will be the century in which knowledge and knowledge professionals dominate the economy and society. [*1] The last decade of the 20th century gave us a brief introduction to a society that will be driven by information and knowledge. At the heart of this revolution is the breathtaking speed at which information is transmitted and at which technology bears down on society, constantly providing new ways of communicating, of preserving and accessing knowledge, and of tracking persons and objects. These changes have brought with them tremendous opportunities to enhance older ways of doing business, such as robotic and distributed manufacturing [*2] and - the subject of the present review - etailing or the sale of goods and services through the Internet.

While these changes will revolutionize business, they have also brought with them considerable vulnerabilities, and new opportunities to commit crime. This is to be expected. Thus, in the 20th century the mass production of the automobile spawned the bank robberies and crime sprees of such criminal "heroes" as Bonnie and Clyde. While one may say that a bank robbery is still a bank robbery regardless of
Crime of the information age provides the backdrop to the specific crime vulnerabilities that beset e-tailing. Many crimes have been identified over the past ten years as "typical" of the computing environment. Some of these are old crimes given a new face, but others are completely new. Some directly threaten the e-tailing environment, while others do so indirectly. However, all such crimes affect the e-tailing environment in the same way that crime affects any neighbourhood. There is extensive evidence that if crimes of any kind are allowed to proliferate, their effect on the neighbourhood is to provide an attractive setting for more crimes of a different sort, usually more serious crimes. So too on the Internet. If investment frauds or medical frauds, for example, are allowed to proliferate, they provide a climate for other kinds of crime, and they also affect the public perception of that "neighbourhood".

This review places e-tailing in the context of the information society of the 21st century. In Part One, it analyses the new opportunities afforded criminals to target the core of e-tailing and the information society generally: information and the computing system within which information resides. It argues that information is the "hot product" of the 21st century and that the information system within which the information resides (which for retailing is largely the Internet) also contains special crime inducing properties. There follows a close analysis of the e-tailing value chain - value of a product or service as it moves through different stages from manufacture to customer - which reveals many points of vulnerability to crime. These vulnerabilities have less to do with the physical security of the product itself (though this continues to be important), than with the transactions that occur along the way of bringing the product to the customer.

In Part Two, a detailed analysis is undertaken of the specific vulnerabilities of the main kinds of payment methods (credit cards and digital cash) and of the variety of other transactions involved in bringing the goods or services to the customer. Auctions and peer-to-peer sales are covered as well as standard e-tailing arrangements. The vulnerabilities of the delivery system are addressed, though this topic is covered in much greater detail in the companion paper from Herriot-Watt University.

In Part Three, the review then offers a survey of recommendations for preventing crime in the e-tailing environment. While technological solutions are undoubtedly important in preventing crime in the computing environment, the situational prevention approach provides many other problem solving methods that can be used to reduce criminal opportunities. These methods seek to (1) increase the effort that the criminal must make in order to carry out crime, (2) increase the perceived risk of the crime, (3) reduce the anticipated rewards of the crime, and (4) remove excuses for the criminal. The widely used sixteen opportunity-reducing techniques that have emerged as a result of the now extensive research in the field of situational crime prevention are adapted to the e-tailing environment.

The review concludes with a brief assessment of the two major policy issues that emerge from this analysis of e-tailing and criminal opportunity. The first is the problem of establishing personal identity. The second is the problem of protecting personal identity - that is, the issue of consumer privacy. It is likely that these issues will emerge as major concerns of policy makers, legislatures and the private sector in the years ahead.

---

*1 Drucker, Peter (2001). The Next Society. The Economist. Nov. 3. By now, this is not an especially new observation. It reflects the idea of the "post-industrial society" described by Daniel Bell (1976) The Coming of Post-industrial Society. New York: Basic Books. The idea has been developed by many economists and political scientists of various persuasions to describe these irreversible changes: "... just as machines are the tools of the industrial economy, computing and telecommunications technologies are the tools of a new 'information economy'.


PART ONE: THE OPPORTUNITY STRUCTURE FOR ETAILING CRIMES

This part of the review examines the two environments that contribute to new opportunities for crime: the computing environment and the e-tailing environment. The former identifies a range of crimes, some of which are new in the sense that the computing environment has made them possible, but many of which are old crimes taking advantage of new opportunities. The latter identifies the shifts in value in the supply chain of e-tailing compared to the traditional model of retailing, with a view to exposing the shifts in vulnerability and opportunity for crime. This approach necessitates a close examination of the transactions that occur at each point of the e-tailing value chain.

Using the perspective of situational crime prevention it is argued that information is the "hot product" of the 21st century, and that its crime inducing properties can be analysed in much the same way as these properties have been identified in regular consumer products. It is further shown that the information system within which information resides (which for e-tailing is largely the Internet) also contains special crime inducing properties, and these are systematically identified.
The E-Crime Strategy Task Force *5 has identified computers as providing both a target and tool for crime. Computers are targets for crime because they perform two major functions: (a) they store large masses of information that have value to their users and thus to potential criminals, and (b) they are able to transmit large masses of information of many different kinds to other computers and devices at increasingly rapid speed. Criminals may steal or corrupt valuable information by either gaining unauthorized access to the computer that stores the information, or by intercepting any transmission. *6 The fact that the number of people now online has increased tremendously in the last decade, and the number of web sites has increased enormously as well, means that there are obviously more targets of opportunity for criminals. The number of people online has increased from about half a million in 1995 to more than 500 million in 2000. *7 One estimate suggests that the average worldwide loss per online person due to Internet fraud rose from $427 in 2000 to $636 in 2001. *8 It is likely that this figure considerably underestimates the costs of computer related crime because it is limited to scams and cons, and excludes certain types of hacking and vandalism and other types of computer crime that do not have direct monetary effects on specific victims, but whose costs are far broader and non-specific.

Computers may be used as a tool for crime much as automobiles were used to enhance getaways in bank robberies. Drug runners benefit by the enhanced communications provided by cell phones (essentially computers); pornographers use computers for storage and exchange of paedophilic images; money launderers may channel illegal drug proceeds through hidden bank accounts and web store fronts that are easily constructed using the modern tools of electronic and on-line banking and other services of the Internet. The range of crimes made possible by, or enhanced by, the computing environment is vast. Although many such crimes may not be directly related to etailing, depending on the circumstances, they in fact can have a serious impact on etailing. For example, the deliberate infection of the Internet with a virus or worm can wreak havoc with the email systems of companies on the other side of the globe. Companies that depend on email as a means of communication with their customers or business partners will be directly affected, even though the initial release of the virus may not have been intended to infect that particular business. Thus, because of the vast interrelatedness of computers, computer networks, and telecommunications, a seemingly small act of hacking may become a massive act of sabotage.

It would take a major book to review all types of crime committed on the Internet or against computer systems in other venues, though these can be classified into three main groups as in Table 1:

- **Table 1a** lists those crimes that have direct effects on etailing, usually victimizing business (though inevitably this damage trickles down to customers through higher prices). There are two types of crimes included in this category: those that impact directly on specific etailing product types and those whose impact affects all etailing enterprises. Crimes included in the specific product type are telecommunications theft, cloning of cellular phones, video piracy, software piracy and copyright infringement. Those whose impact applies to all etailing are terrorism, electronic funds transfer fraud, hacking, industrial espionage, denial of service, cross border crime, extortion and blackmail, and credit card fraud.

- **Table 1b** lists those crimes that mostly have an indirect effect on etailing (although depending on the circumstances their impact can sometimes be direct). These crimes generally create an ambience of fraud and distrust on the Internet such that they contribute to the customer’s lack of confidence to do business on the Internet. Just as one would not go shopping for an important item of quality in a run down neighbourhood that is ridden with prostitution, drug dealing and pornography, one is also distrustful of shopping at an etailing site if the crimes of this category are widespread on the Internet. These crimes essentially undermine the essential ingredient of good commerce, which is trust. They include: stalking, harassment, money laundering, investment fraud, telemarketing fraud, sale of stolen or illegal goods, and identity theft.

- **Table 1c** lists another group of crimes that create a “frontier climate” by exploiting grey areas of the law. Crimes included here are gambling, tax evasion, criminal conspiracy, and aiding and abetting of crime. Their overall effect is similar to those of Table 1b: to undermine the climate of trust of the etailing neighbourhood.

The crime types in Table 1a-c do not necessarily conform to legal categories *9, nor that they are discrete crimes in themselves. *10 In fact, many criminal events committed within the computing environment probably contain more than one crime type. They are presented rather to provide the detail of the criminal propensities of computing environment within which etailing resides.

---


*6 The task force identified ways in which the computer can also serve to prevent and detect crime, but we will reserve these functions to a later section concerning prevention.

*7 From Grabosky, loc.cit. See also NUA Research at [http://www.nua.org/surveys/how_many_online/index.html](http://www.nua.org/surveys/how_many_online/index.html).


*9 The fact that the number of people now online has increased in the last decade, and the number of web sites has increased enormously as well, means that there are obviously more targets of opportunity for criminals. The number of people online has increased from about half a million in 1995 to more than 500 million in 2000. *7 One estimate suggests that the average worldwide loss per online person due to Internet fraud rose from $427 in 2000 to $636 in 2001. *8 It is likely that this figure considerably underestimates the costs of computer related crime because it is limited to scams and cons, and excludes certain types of hacking and vandalism and other types of computer crime that do not have direct monetary effects on specific victims, but whose costs are far broader and non-specific.

*10 In
Finally, we should note that the target of all computer related crime is not computers but information. In this respect, focusing on misuse of computers may direct our attention away from analysing significant aspects of the information system that attract criminal attention and provide opportunities for computer crime. In fact, consistent with the portrayal of the 21st century as the information society, it is reasonable to target information and the information systems that store and transmit it, as the true source of vulnerability to crime.

Table 1a: Crimes of the computing environment having direct effects on etailing

<table>
<thead>
<tr>
<th>Crime type or incident</th>
<th>Computer as Tool or target</th>
<th>Examples</th>
<th>Estimates of extent or cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of telephone</td>
<td>Target</td>
<td>Obtained employee's access code and software from Internet.</td>
<td>£290 million one incident in 1990. *11</td>
</tr>
<tr>
<td>Services</td>
<td>Hacked into company computer system, and assumed Systems Operator status. See also cell phone cloning, below.</td>
<td>5% of total industry turnover. *12</td>
<td></td>
</tr>
<tr>
<td>Video piracy</td>
<td>Target and tool</td>
<td>Counterfeit copies of movies and video games downloadable from the Internet. Hacker posted on a well-known hacker website (<a href="http://www.2600.org">http://www.2600.org</a>) a program to decode DVDs (DeCSS) and convert them into downloadable files. *14 Video game makers sue Yahoo for selling pirated games at auction. *15</td>
<td>10% of all movies can be downloaded from the Internet illegally, and for free. *16 Piracy drives down prices, occurs in over 65 countries. *17 Industry cost estimated $3.2 billion from piracy in 1998. *18 270,000 Dutch web addresses offer a movie or TV show illegally for sale or most often free. *19</td>
</tr>
<tr>
<td>Software piracy</td>
<td>Target</td>
<td>Easy copying from disks and CDs, obtain protection-free copies from the Internet.</td>
<td>$7.4 billion lost in 1993 according to Software Publishers Association. *20</td>
</tr>
<tr>
<td>Copyright infringement</td>
<td>Tool</td>
<td>Reproduction of copyrighted material on the Internet. Trading in copyrighted songs and recordings via peer-to-peer. Most famous case: Napster music site, used by millions, shut down because of copyright infringement.. *21</td>
<td>Annual costs to industry approx. $15-17 billion annually. *22</td>
</tr>
<tr>
<td>Vandalism</td>
<td>Target</td>
<td>Most infamous example of the &quot;worm&quot; virus released into the Internet causing untold damage within hours infecting 10% of Internet hosts, many out of business for up to two weeks. *23</td>
<td>Trillions of dollars. See hacking and terrorism below.</td>
</tr>
<tr>
<td>Spying, Industrial espionage</td>
<td>Target and Tool</td>
<td>Most famous example: Intruder into Lawrence Berkeley Lab. Computer tracked down and caught. *24</td>
<td>More recently, intruders found &quot;sniffing&quot; in Rome Lab. Griffiss Air force Base Cost: $211,000 plus cost of investigation. *25</td>
</tr>
</tbody>
</table>
**Terrorism**

The US defence department receives some 60-80 hacker attacks a week to its computers. In February 1998, 11 Dept. of Defence computers were broken into. In 1998, a “cracker” cyber terrorist disabled a Chinese satellite to protest western investment in China. *26* It is estimated that there are upwards of 30,000 hacker sites on the Internet which provide tutorials on how to write viruses, choke networks, and announce meeting points for hackers all over the world. *27*

**Electronic funds transfer fraud**

Irrevocable transfer of funds, usually offshore extremely difficult to prevent, especially when perpetrators typically use fictitious identities. *28* Over 50% of banks surveyed report having been victimized by fraud.*29* See also below cross-border crime.

---


*19* Arlen, Gary (2001). Always on: Dutch video piracy preclude to a corporate threat. Broadband Week. April 16. This figure contrasts to the US of 534,668. Clearly the Netherlands figure is disproportionate to the population.


*29* Ibid.

---

**Table 1a: Crimes of the computing environment having direct effects on etailing (continued)**

<table>
<thead>
<tr>
<th>Crime type or incident</th>
<th>Computer as Tool or target</th>
<th>Examples</th>
<th>Estimates of extent or cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking</td>
<td>Target</td>
<td>This is the most well known computer crime. Hackers have broken into banks in Los Angeles, the Los Alamos National Research Centre, the LA Police department, Scotland Yard, Pacific Telephone, <em>30</em> and many more. The most infamous hacker Kevin Mitnick cost hi-tech companies at least $291.8 million. <em>31</em></td>
<td>In 1995 estimated that hackers cost business $800 million. <em>32</em> In 2000 the estimate is $1.6 trillion. <em>33</em></td>
</tr>
</tbody>
</table>
Denial of Service  

The most sophisticated version is distributed denial of service, in which an individual exploits bugs or loopholes in operating systems (usually Windows) to cause a flood of messages to be sent via hundreds of computers to one website which effectively closes it down. *34

It is predicted because of the rapidly increased availability of bandwidth to users, and the more powerful personal computers (especially running Windows XP), that distributed denial of service will increase drastically in coming years. All major ecommerce sites have been victimized. *35

Cross border crime  

Tool  

Boy buys a DVD player on Amazon auction site. Wires money to seller in Moldova. Never receives item. Finds out that many others have been victimized as well. Amazon partially reimburses victim. *36 See also Credit Card fraud below.

Russian in St. Petersburg accesses Citibank’s funds transfer system and deflects payments of $10.7 million to his own account in Russia. *37

Internet ideally suited to cross border crime since the Internet exists beyond national boundaries.

<table>
<thead>
<tr>
<th>Crime type or incident</th>
<th>Computer as Tool or target</th>
<th>Examples</th>
<th>Estimates of extent or cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extortion and blackmail</td>
<td>Tool</td>
<td>Threat to kill Microsoft President Bill Gates, using encrypted messages and images posted on AOL Netgirl Bulletin Board, demanding transfer of $5,246,827.62 to a Luxembourg bank account. Offender caught, tracked to Long Grove, Illinois. *38</td>
<td>Banks have begun to appease online extortionists by paying them off. Gangs have amassed up to £400 million worldwide by issuing threats to destroy computer systems by using information warfare techniques. *39</td>
</tr>
<tr>
<td>Cloning of Cellular Phones, phone cards.</td>
<td>Tool and Target</td>
<td>Buy phones in bulk, clone to other numbers and discard after use. The U.S. DEA numbers were cloned by the Colombia Drug cartel. *40</td>
<td>Estimated in 1996 $1 million to $2 million worth of illegal phone use per day in the United States and Canada. *41</td>
</tr>
<tr>
<td>Credit card fraud</td>
<td>Tool and Target</td>
<td>In an example of cross border crime, two British men in Wales hacked into ecommerce web sites in the USA, U.K., Canada, Thailand and Japan and stole credit card information for 26,000 accounts.</td>
<td>Losses for this crime alone exceeded $3 million. Visa estimates that online credit card fraud accounts for 25-28 cents of every $100 spent, about four times worse than the offline rate of 7 cents per $100. *42</td>
</tr>
</tbody>
</table>


Table 1b: Crimes of the computing environment having indirect effects on e-tailing

<table>
<thead>
<tr>
<th>Crime type or incident</th>
<th>Computer as Tool or target</th>
<th>Examples</th>
<th>Estimates of extent or cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stalking</td>
<td>Tool</td>
<td>Women who register with on-line dating web sites are tracked down by would-be suitors. *43</td>
<td>In 2000, estimated that of worldwide population of users there are 3,000 Internet stalkers. *44</td>
</tr>
<tr>
<td>Harassment</td>
<td>Tool</td>
<td>A man, spurned by a woman, posted on a bulletin board an invitation to her home for a &quot;gang rape fantasy&quot;, giving her address, phone number, and how to bypass her burglar alarm. Eight men showed up. *45</td>
<td>Typical targets are inexperienced users of the Internet, and women. *46</td>
</tr>
<tr>
<td>Money laundering</td>
<td>Tool</td>
<td>Infiltration of banking system by organized crime, use of electronic non-bank transfers and cyber-banking, and many other sophisticated techniques. *47</td>
<td>Estimated that one trillion dollars is laundered every year. *48</td>
</tr>
<tr>
<td>Investment fraud</td>
<td>Tool</td>
<td>Bogus banks set up convincing web sites. Bogus company that promises to turn iron-ore rocks into gold, and many more. *49</td>
<td>Securities scams run by organized crime: 35 companies exposed by FBI in 2000. Frauds cost victims $50 million. *50</td>
</tr>
<tr>
<td>Telemarketing fraud</td>
<td>Tool</td>
<td>The top ten telemarketing frauds of 2000 were (in order of incidence): Prizes/Sweepstakes, Magazine Sales, Credit Card Sales, Work-At-Home, Advance Fee Loans, Telephone Slamming, Credit Card Loss Protection, Buyers Clubs, Telephone Cramming, Travel/Vacations. *51</td>
<td>Estimated cost of $40 billion a year through telemarketing fraud. 92 percent of adults in the United States report receiving fraudulent telephone offers. The FBI estimates that there are 14,000 illegal telephone sales operations at any given time. *52</td>
</tr>
<tr>
<td>Sale of stolen or illegal goods.</td>
<td>Tool</td>
<td>Internet auction sites, bulletin boards, news groups. Man uses aliases to sell pirated Adobe software on Ebay auction site. Indicted by US department of Justice. *53 Four high school boys purchased DXM an hallucinogen on Web auction site. *54</td>
<td>16 million users of auction web sites per month. 87% of fraud cases on-line estimated to be related to auction Web sites. *55 Consumer complaints rose from 1,280 in 1997 to 10,660 in 1999. *56 There are over 1,00 auction sites on the Internet. *57</td>
</tr>
</tbody>
</table>
Identity theft Target and tool A husband/wife team (the "modern Bonnie and Clyde") stole identities and emptied bank accounts of their victims in over six U.S. states. *58

Identity fraud accounted for 96% of Visa’s member bank credit card fraud losses of $407 million in 1997. *59


*52 Ibid.


**Table 1c: “Frontier” crimes of the computing environment having direct and indirect effects on eetailing**

<table>
<thead>
<tr>
<th>Crime type or incident</th>
<th>Computer as Tool or target</th>
<th>Examples</th>
<th>Estimates of extent or cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gambling</td>
<td>Tool</td>
<td>May or may not be illegal in various countries and regions, which is a major part of the problem. *60</td>
<td>Worldwide online gambling revenue has increased from $651 million in 1998 to $2,238 million in 2001. *61</td>
</tr>
<tr>
<td>Tax evasion</td>
<td>Tool</td>
<td>Barnes&amp;Noble.com sued by Amazon.com for not charging sales tax. *62</td>
<td>Sales tax and trade embargoes make otherwise ordinary products &quot;hot&quot;. Cuban cigars are sold widely on the web. *63</td>
</tr>
</tbody>
</table>
Criminal Conspiracy Tool
International networks to trade in pornography, the "Wonderland Club". Organized crime in smuggling, drugs, gambling and prostitution all enhanced by computing environment. *64

Aiding and abetting crime. Tool
How-to news groups: bomb making, lock picking, counterfeiting, encryption fixes, smart card cloning. *66

Alt.hacker news group is one of many in which "newbies" and seasoned hackers exchange information.

Costs of crime in the etailing environment

Examples cited in Table 1, suggest that the costs of these crimes and intrusions into the information systems of etailers are considerable. Although estimates of such costs are always speculative and open to criticism, the chances are that they are underestimates because they represent only those incidents that have been detected. Here are some additional more general estimates of cost: *67

1. $6.7 billion - the cost of the first five days of the "I love you" bug of spring 2000.
2. $125,000 per hour is the estimated cost to businesses for Web outages.
3. $142,000 was the average cost of network security breaches in 1999 according to the FBI.
4. 55% of companies in 1999 experienced at least one breach of computer security in 1999, according to the FBI.
5. On average, 41% of security related losses were the direct result of employees stealing information, and the average cost per incident was $1.8 million.

Information as a Hot Product

If we say that information is always the ultimate target of computer criminals, we must also add that it is very much a moving target. The information that the criminal seeks either to steal or disrupt may be "on the move", and it may be stolen by intercepting it between one computer and another. And with wireless computing becoming more pervasive, this means that information that is on the move truly does exist in space. It is the fleeting existence of information in cyberspace that makes it so efficient to transmit, but it is also its cyber characteristics that cause it to resemble "hot products" that are especially or even inherently prone to criminal attack or misuse. Clarke has identified these products as containing, in varying degrees, six attributes that make them CRAVED by thieves: they are Concealable, Removable, Available, Valuable, Enjoyable, and Disposable. *68 If we examine each of these we find that information in the computing environment fits them almost perfectly.

Concealable. What better way to conceal an item one has stolen than in cyberspace, a vast territory with so many nooks and crannies that one can hide stolen information, and do it so quickly, that one may never be seen carrying it? Thieves may have thought it easy to remove a magazine from a stand in a store and conceal it under their coat. On the Internet it is even easier to steal. In fact, using the Internet, one can steal information without ever having personally to possess it, and can do so from halfway around the world. Not only that, using the standard services and procedures provided by the Internet, users can easily fake or otherwise obfuscate their identities. In fact, in cases where the criminal simply wants the information and does not want to deny it to someone else, the information can be copied and the original left alone. In such cases, there is no trace of the theft. And if so many copies are made of the information, such as, for example in the case of copyright infringement of software and audio files, with so many copies, which one is the original? This is the ultimate in concealment.
Removable. We hardly need to make comment here. The whole raison d'être of the Internet is that information is removable. In fact, it is constantly on the move. It is therefore intrinsically vulnerable to interception and deflection to places that it was not originally intended. As noted in Table 1a, electronic funds transfers between banks can be intercepted and deflected to a criminal's own bank account. Email can be easily intercepted and personal information stolen. Software files can be downloaded which makes the object of the crime - software - removable, yet still leaves the original file in place. While various locks and access controls are used in the computing environment, criminals find ways to break those controls. This is what hackers enjoy doing.

Available. The Internet calls out loud and clear that all information is available. Some argue that the true revolution of the Internet is that it has made all information potentially available to everyone. The revolution has been likened to the invention of the printing press in 1455. Information is displayed on the Internet on all manner of subjects and topics, including information on how to break access codes and obtain information that is available, but ostensibly not removable. One may argue that consumer products are not available as they are on a shelf in a regular store, so that this makes them less "hot" to steal. Clearly, this is true. A book cannot be stolen is such a direct way on the Internet as it can in a bookstore. However, while slightly more complex, one can nevertheless steal a book on the Internet by making a fraudulent credit card purchase, using any number of fraudulent techniques such as pretending non-delivery, using another's credit card. In this case, one does not even have to go to the store to steal the item, rather one can have it delivered right to one's chosen address.

Valuable. In the information society, information is like money (actually, in the case of banks it is money). Companies and individuals are now taking great steps to protect their proprietary information. The paradox is that the ethos of the original Internet was that all information on the Internet should be openly shared, and be free (the "Hacker's Ethic" see Table 2). Thus, criminals are provided with a ready made excuse for attacking protected bodies of information. Since they are placed on the Internet "they ought to be free". There is also much information on the Internet that has immediate value to potential criminals. Because of the masses of personal information now being accumulated on the web as a result of etailing and ecommerce, access to such information by criminals gives them valuable credit card numbers and bank accounts which they can use to commit a wide variety of fraudulent crimes.

Table 2: The Hacker’s Ethic

- Access to computers should be unlimited and total.
- All information should be free.
- Mistrust authority - promote decentralization.
- Hackers should be judged by their hacking not bogus criteria such as degrees, age, race, or position.
- You create art and beauty on a computer,
- Computers can change your life for the better.


Enjoyable. Joyriding was a favourite delinquency when automobiles became all pervasive in the 20th century. The literature on hackers, who are often clever schoolboys (and sometimes mischievous adults), clearly demonstrates the joy that they experience in overcoming the challenge of breaking into protected computer environments. *69 Many appear to do this for the pleasure of the challenge, not for the money - although there are many who also do not mind making money out of their enjoyable enterprise as well. For some computer criminals, especially hackers, much of the enjoyment is obtained by making public the results of their hacking. Enjoyment is especially sought among other hackers, as is clear from even a cursory perusal of hacker web sites and news groups (e.g. alt.hackers). This is somewhat paradoxical, for it often leads to their arrest and prosecution.

Disposable. The Internet provides a ready means to dispose of stolen property. Newsgroups and IRC (Internet Relay Chat - on-line real time communication that is typed into the computer and is less public - can be used to find individuals who are willing to purchase stolen property. However, by far the greatest venue for disposing of stolen property is the on-line auction, such as Ebay and its competitors. This convenient and cheap way of selling goods (one should add that most items are legitimately sold) provides an easy way to advertise and sell any used item, whether "hot" or not. The literature on disposal of stolen goods has suggested that the availability of a fencing operation enhances the chances of particular items being stolen. *70 Thus, the mere existence of on-line auctions provides a ready market for stolen and counterfeit items. Information, this time in the form of matching a buyer to a seller, once again displays its inherently crime prone quality. Depending on the type of information and type of computer crime committed, disposability may or may not be an important attribute of the information. In fact, for many hackers, an important element to the enjoyment of their activity is disposing of their criminal theft - making publicly available the results of their labours. Thus, for example, the individual who cracked the code of DVD protection posted this information on the web (see Table 1a). In this case, the criminal receives public acclaim and recognition for his deeds, rather than financial rewards as he would do if
Perhaps the analogy between Clarke’s hot products and information as a hot product is stretched a little too far? Information, after all, is not a physical product of the same kind as, say, a handgun. Although it may be contained at particular times in a physical product, such as a computer in a particular place on a particular desk, or in a laptop whose small size may make it a hot product it can also exist in many places, especially cyberspace. Information also takes on many different forms and characteristics. It may at one time be intellectual property, at others a list of names and addresses and credit card information, at others encrypted messages, at others a series of instructions to search the Internet, at others a series of instructions to make computers, telephones and networks accomplish particular tasks. Thus, the idea of information as a product is something that is far more complex than one particular consumer item, such as a handgun. What the CRAVED exercise above shows very clearly is that information is inherently vulnerable to criminal attack and misuse. Unfortunately, its complexity and variety, unlike a simple consumer item, makes it especially difficult to suggest specific design changes, such as safety locks on hand guns, that could eliminate or reduce its inherent vulnerability to criminal misuse.

Some changes to the design of information in order to protect it from theft have been developed of course. Encryption is one excellent example, but it is used only in very specific situations or circumstances. It is significant that the majority of successful criminal intrusions into computing systems is made possible by bugs or errors in programming languages which the sophisticated hacker can turn to his advantage. Programming languages such as C, C++, Microsoft’s Visual Basic, and more recently Java all have errors contained in their design. Many of these errors are widely disseminated on the Internet, and in fact there are programs that will scan systems to find such errors or “holes”. Security managers depend on such programs. Unfortunately, hackers can also make use of them. No programming languages have been written with security or defence against intrusion or attack built into their design. *71 Thus, attempts to prevent intrusion have to concentrate on other aspects of the etailing delivery system. This requires an analysis of the situations in which information is used, stored or transmitted. The application of the basic principles of situational crime prevention should be applicable to uncover the opportunities that various information systems make available to potential criminals, and the vulnerabilities that are not only inherent in information itself, but in the system within which the information resides. Furthermore, the characteristics of the system that processes and stores the information are also, perhaps primarily, the target of hackers who are motivated by the elements of the information system itself - i.e. the Internet and its "culture".

---


---

The Information System as a Hot Service

*Turning the Corner* drew a distinction between products and services, suggesting that a different set of crime prone features could be identified in regard to services. These were summed up by the acronym EVADED:

- **E**nduring - once appropriated it can continue to be used and not be terminated by the legitimate supplier;
- **V**aluable;
- **A**vailable - which goes to the heart of the security around such services;
- **D**istributable - will the thief be able to make this service available to others;
- **E**asy to use - the easier the service is to use the more potential recipients there will be;
- **D**esirable - given the range of electronic services in the entertainment sphere, something may be desirable to a thief without necessarily having a high monetary value. (page 8).

While these six characteristics do hold merit, taken on their own, they in fact overlap considerably with Clarke’s CRAVED criteria. It is difficult to see how the additional features of EVADED would not also apply to “regular” products. We suspect that the reason for this confusion is that the distinction between "products" and "services" is extremely difficult to delineate, particularly in the information age. A solution to this problem may be to think of all products on the Internet as passing through vulnerable points in an information system that makes up the etailing value chain (see Figure 3 below). Thinking of these points as "situations" makes it possible to apply Clarke’s situational approach *72 which directs attention to analysing the complexity of buying and selling in the computing environment and to identify the situations or points at which opportunities for crime occur. Thus the idea of information as a hot product is extended to *situations* that are also “hot”. That is, while criminals or potential criminals may search for products that are easier to steal or provide greater rewards, they also look for situations that afford greater opportunity to successfully carry out their crimes. The question that should therefore be asked of the computing environment is: What would be the ideal situations or circumstances in which a criminal would prefer to do his or her work? The computing environment - the information system - provides ideal situations that are summed up by the acronym SCAREM. The six features identify not only features of the information system that are “hot” in and of themselves, but also tie these to the known motivations of potential offenders.

*Stealth* (EVADE’s Easy) is certainly a circumstance that makes for carrying out crime. How easy for the thief to just walk...
into a bank, invisible, and remove as much money as he wanted, all the time remaining undetected! Just such a possibility exists on the Internet as clearly outlined by Denning. *73 Criminals use encryption, mimic the actions of a systems operator, obtain passwords, use steganography, and use remote storage on an innocent third party’s computers, to identify just a few techniques. And on news groups, even non-criminals can use assumed identities.

Challenge. (EVADE’s Desirable). The literature on computer criminals who are hackers is replete with one primary motivation: to “beat” the computing system. Many seem unable to stop or even delay their mission to break into a computing system, once they have begun their task. They work very long hours, become obsessed with the challenge and completion of their task. *74 This obsession is not, however, to the detriment of getting caught. Indeed, part of the challenge seems to be to carry out the intrusion virtually under the noses of computer administrators. Depending on the particular situation, the risks of getting caught can be reduced possibly to zero in cases where one can intercept the transmission of information and deflect it to an anonymous account or place. Timing here is of ultimate importance. Messages, such as those containing funds transfer move almost at the speed of light. It follows that the less time necessary to carry out the criminal act, the less chance of being caught. Considerable preparation is needed in order to gain access to these transmissions: one must gain entry into the bank’s or other institution’s computer system. Almost all major break-ins of computing systems have resulted from persistent and stealthy activity by the hacker over long periods of time, from one month to several months. *75

Anonymity. (EVADE’s Easy) These long periods of intrusion are made possible by another important attribute of the online information system, Anonymity, which differs from Stealth. Stealth is sneaky and secretive. Anonymity is a traditional value of regular commerce, though it is fast disappearing. When cash purchases are made at a department store, it is irrelevant who the buyers and sellers are. This is a trusted transaction between two strangers, both of whom protect their identities. Adam Smith marvelled at the market economy that actually thrived on the basis of transactions among strangers. Anonymity and its close sibling, deception, abound on the Internet. Email addresses can be obtained for free in many places on the Internet, with little or no personal data (or if required little or no verification of personal data). Sophisticated hackers can also mimic the IP addresses of others (“spoofing”), *76 making their email extremely difficult to track. This therefore allows such hackers to spend long periods of time online attempting to gain illegal entry into an institution’s information system with little chance of being detected, or if detected little chance of the offence being tracked specifically to the offender.

Reconnaissance. Perhaps the most important element in the rational choices that a criminal makes in carrying out his crime is the choice of a vulnerable victim. The Internet makes it possible to scan thousands of web servers and even millions of personal computers that are connected to the web, looking for “holes” or gaps in security through which the criminal can enter and carry out any aspect of his crime - whether to deposit stolen files on an unsuspecting computer, or to steal passwords or credit card information for use in a later crime, or to intercept funds transfers, and so on. This scanning for victims can also be done automatically, using software easily obtainable on the Internet. Clarke and Cornish *77 have described criminals as demonstrating “limited rational choice” in the process of carrying out their crime. The picture that criminals may have a specific goal in mind, say stealing items from an automobile, but will tend to take the path of least resistance in order to accomplish this crime or something like it. Thus, they may break into cars that are unlocked, or cars that are parked late at night in poorly lit streets. This is a picture of criminals taking advantage of surrounding circumstances of the moment. In contrast, the Internet provides a context in which the informed criminal can take a careful survey of all possible victims, then act accordingly. Much more planning is involved. Rational choice seems less limited than it is enhanced!

Escape. There is little sense in planning and carrying out a crime if it is obvious that the chances of getting caught at the time of the act are very high, or that a trail of evidence is left that will lead inevitably to detection. It is true that some criminals do not think much about the consequences of getting caught when committing their crimes. *78 However it is surely obvious that the crime-inducing aspects of the information system environment of anonymity, deception and stealth all combine to make it extremely difficult for law enforcement to track down the crime to the individual perpetrator, especially when the crime itself may never be detected, even by its victims. In the major case of the US military network break-in, the perpetrator first hacked into the Harvard University computing system, and worked from that address. Thus, he was able to cover up his own location or “true identity”. *79

Multiplicable. (Similar to EVADE’s Enduring). A traditional theft, such as a bank robbery, is a relatively finite act. However, if an offender hacks into a bank’s files, this one crime can be multiplied exponentially, since it makes available to the offender a huge number of new opportunities to commit crime by exploiting access to the bank’s accounts. While it is true that some traditional crimes such as burglary do create the opportunity for additional burglaries of the same premises, these are limited to one or two additional times, and do bring with them substantially increased risk. But hacking into valuable databases makes many more crimes possible and attractive. These are not just confined to theft from bank accounts, but can also involve extorting money from the bank for return of the database.

The CRAVED information and SCAREM of information systems combine to provide a benign setting for the commission of crime on the Internet and other computer networks. It remains now to apply these ideas to etailing. In order to identify the points at which etailing is exposed to CRAVED and SCAREM, it is necessary first to examine the environment of etailing and of ecommerce generally of which etailing is a part.
B2 Clarke, Ronald V. (1997). Situational Crime Prevention: Successful case studies. 2nd. Edition. NY: Harrow and Heston. An accurate application of situational prevention to and understanding of any crime is not bound to a physical location, although the approach certainly has its roots in the idea of analysing physical locations (e.g. CPTED and environmental criminology) for the opportunities they offer potential offenders. Situations may exist in many different forms and ways. They exist in both time and space, but they are certainly not constrained by either. Obscene phone calls, for example, produce situations in which a caller in one physical location harasses another any distance away. A situational solution to that particular crime was provided by call-ID, the exact physical location of which cannot be pinpointed either in time or place, except that the result of it is the appearance of a number at the victim’s telephone appliance. Similarly, the fraudulent use of a credit card in a store at point-of-sale involves many locations and elements of time: the decision to check out the validity of the account of the customer, the checking of a database at a distant location, the interaction of the salesperson and the customer, the validity of the plastic card used by the customer, the identity of the customer, and many more factors that contribute to the apparently simple, but in effect extremely complex situation of a credit card purchase. Applied to the Internet, the complexity of the “situation” of a purchase is even more complex, when the purchaser is many miles away from the “seller” which may not be a person but a computer program. There is no reason, however, to dismiss this interaction as not a “situation” simply because it occurs over a huge distance.

*74 Clough and Mungo, loc.cit.
*76 Ibid. p. 12.

The Etailing Environment

Etailing and retailing. The fact is there is old in the new. The list of crimes in Tables 1a-1c, reveal many crimes that are easily identifiable as crimes that occurred before the online world existed, or before even computers existed (e.g., blackmail, extortion, counterfeiting, vandalism, terrorism, fraud). It is just that the computing environment offers tools and new opportunities to perform many of these crimes more easily. This is clear when we examine the inherent CRAVED features of information in the information society. The same may be said in regard to etailing, for it of course embodies the essential elements of retailing. There are two essential features of all retailing, indeed all of commerce: trust and delivery. The former is an abstract idea that has evolved over hundreds or perhaps thousands of years, clearly identified by Adam Smith, the first to truly understand market economies: “Mankind brought together in a mutual Intercourse of good Offices”. *80 The latter is the practical application of that idea. That is to say, trust assumes that each party will “deliver the goods”.

All commerce, especially retailing, depends on trust between strangers. By “trust” it is meant that, in any exchange, each party to the exchange will reciprocate. In regular retailing, the problem of trust is theoretically reinforced by a face-to-face exchange between the buyer and seller. There are many assumptions of trust in this simple exchange both on the part of the seller and of the buyer. For example, there are assumptions that the product purchased does or is what the seller says it is, that it is “safe”, that the seller in fact is a genuine representative of the retailer, and so on. The buyer guarantees that the money he hands over is not counterfeit. These, and many other assumptions are familiar aspects of retailing. Retailers and manufacturers try their best to overcome the problem of being strangers to their customers, by advertising their products and services, so that they become “household names” and thus can offer trusted products, so that buyers will enter a store they can trust. There are also many ways in which the assumption of trust is abused. Shoplifters will try to acquire an item without paying, often taking advantage of the inviting displays of items shopkeepers use to entice customers. Retailers and manufacturers may use deceptive advertising to create a false sense of familiarity with the product.

Etailing also depends on trust between strangers, though these are strangers of a different kind who never meet “face-to-face”. The exchanges themselves, however, are more complex and are of greater variety. We should also note that the new elements of etailing are not something that suddenly appeared with the computing environment. Many aspects of etailing existed before the computing environment emerged.

Precursors to etailing. The great advantage of a retail store is that the customer can pay for the item and receive it immediately. Other forms of retailing tried to match this great advantage by offering the convenience of shopping from home. Thus, mail order catalogues emerged, often in conjunction with large retail chains (for example, Sears). At around this time large retail stores also allowed customers to pay for an item over a period of time using "lay-away" or "lay-buy" plans, in which the customer chose an item in the store, and it was put away for the customer who paid it off over a period of time.
When it was recognized that the mail order catalogue was an effective means of presenting products to customers, televised shopping channels emerged which exploited the medium of television to enhance and convey details of the products to customers. Ordering by mail and ordering by phone became part of the ordinary retailing marketplace. The advent of credit cards also made this process of payment even easier. It also made it possible for the customer to pay for an item, even though the customer did not, at the specific time of the sale, actually have the money in hand to pay for it. Using a credit card over the phone to pay for an item was a first and very big step towards the online environment. Already, computers were behind the scenes crunching and storing the numbers, though the computers tended to be lodged in one place, and not very accessible or movable. And already, the seemingly simple exchange of money for a product was becoming more complex. Individuals using a credit card could actually purchase an item with someone else's money (the bank's or the merchant's) and pay for the item later (at a higher price, of course, if the customer did not pay off the amount owing on the credit card within a specific period of time). These events laid the groundwork for online retailing.

One other practice also set the stage for online retailing: cross-border shopping. In the United States, where every state and region may have a different rate of sales tax, it is common for customers to drive across a state line in order to purchase items at a lower sales tax rate. In Europe, the same may apply by crossing national borders to purchase items such as liquor, cigarettes or perfume where tax or duty is lower: customers enjoy "tax-free" shopping. As soon as online shopping became available, customers immediately recognized the great advantages of being able to ignore state or national boundaries. Online stores could sell products free of sales tax to those residents who lived outside the state or country from which the store transacted its business. And the US Congress passed a moratorium on taxation of online transactions. Thus, a strong motivation existed for shoppers to gravitate to online shopping. Indeed, as can be seen in Figure 1 the rates of online revenues have increased tremendously in the past decade in the U.K.. Similar increases have occurred in Germany and the USA.

---


---

These increases are remarkable when one considers that in 1998 a survey by Commercenet revealed that the top reasons for consumers not buying on the web were lack of trust and the concerns about the payment mechanism. As will be seen below, etailers have spent much money in establishing reasons to be trusted (encrypted online payment certificates) and in making the payment mechanism as smooth as possible (one-click purchase via credit card or digital cash). The driving force in etailing web design has been to make selling faster, to reach customers more quickly and efficiently, make buying more efficient and easy, and overcome customer concern for security (perhaps the most direct measure of "trust"). Thus "one-click" technology as pioneered by Amazon.com to "assist" customer decisions to buy has dominated web design. Nevertheless, the one disadvantage of online shopping - having to wait for delivery of the item purchased - still dogs the etailing trade. And a great deal of pressure has been put on delivery services such as UPS and FedEx (both of which existed well before the computing environment emerged) to provide efficient and quick delivery systems, and systems that allowed for tracking of purchased goods. It is the delivery of service to the customer that translates the idea of trust into retailing and etailing. Delivery, or the "value chain" concept in retailing has undergone considerable change in the past two decades.
We can see in Figures 2 and 3 the contrasting models of the old supply chain of retailing compared to the model of the 21st century. The delivery systems involved in etailing are diverse and complex. They are sometimes called today the "value chain" or "supply chain" but these systems also contain within themselves specific or identifiable media of exchange. The current preference for the term "value chain" reflects the changes in emphasis on where value is located at particular points in the chain of delivery of product to consumer. We can see in Figures 2 and 3 the contrasting models of the old supply chain of retailing compared to the model of the 21st century. There are several important differences between the old and new models of the value chain:

1. Value lies almost entirely in the customer. The old adage "the customer is always right" seems to reflect this view, but it is given new meaning in the etailing environment. We can see from Figure 3 that a large amount of the activity centres on the POS (point-of-sale), but uses this as a vehicle to collect extensive information on the customer's preferences, credit background including credit card information, and buying habits.
2. Thus, etailing web sites are driven by the four traditional values of retailing, and then some: speed of service (it can never be too fast), convenience (one-stop shopping, one-click shopping, ease and transparency of order entry and fulfiment), personalization (ability to provide the customers with precisely the products they are looking for), and price ("nothing can be too affordable").
3. Large databases of customer information are therefore collected, stored and analysed. They are the first and obvious targets for criminals, as they represent valuable information both for the business that owns the data (and thus could be damaged by any criminal attack on the data base) and for competitors.
4. POS is also used as the point for adjusting inventory on the retail site (if it is even kept any more) and to automatically sending an order to the maker to replace the item just sold. The reduction of inventory reduces the amount of goods that are capable of being stolen by stock room employees, one of the most common forms of theft in retail establishments. Dynamic ordering also reduces the necessity to order a large number of particular items for any one shipment, again reducing the chances of theft out of back door operations (i.e. at the loading dock), since items stolen from a small number are more likely to be noticed than items stolen from a very large number.
5. Final delivery of the product is made by third party delivery companies that now allow close electronic monitoring and tracking of every item. This extra link in the purchasing process adds opportunity for crime. While delivery companies have well-established procedures to maintain security of deliveries, common crimes are those related to traditional credit card fraud such as false delivery addresses and false claims of not having received or ordered the item.
6. Return of merchandise is an important point of information collection from the customer, but it also allows for criminal opportunities, especially in the disposal of stolen goods in conjunction with credit card fraud (goods purchased with a stolen credit card may be returned for cash).
7. The manufacturing end has been in contrast simplified. Large inventories of product are mostly not needed. In fact with distributed manufacturing, inventories of the final product are kept to a minimum because the product is constructed according to requested customer configuration, and the parts are received from the distributed parts makers as the orders are received from the retailer. Alternatively, the manufacturer forms a close partnership with the retailer and provides product only for that outlet. Sears appliances or Marks and Spencer labels, are examples of close partnerships between retailing and manufacturing. Of course, these partnerships existed before the online world, but it is apparent that the new information systems environments considerably enhance these partnerships In fact there are many cases in which the partner company is barely distinguishable from the retailer. For example Federal Express has transformed itself into a full service company for selected companies with whom it has a close partnership. It receives orders, fulfills the orders, and maintains inventory control. In one instance it managed to cut the customer-delivery cycle from four weeks to seven days for one of its clients, National Semiconductor.

Companies that specialize in order fulfilment also provide modern technology in "picking and packing" which reduces the amount of human involvement with inventory and therefore reduces the opportunity of employee theft of inventory.

*82 Information from a variety of reports and texts has been used to construct these figures. However, by far the most detailed and incisive is the UNCTAD E-commerce and development report 2001. For example, UNCTAD summarises succinctly the challenges facing etailing as follows:
* Larger number of small parcels or packages due to a larger number of buyers making direct orders and a larger number of sellers than in traditional trade;
* Large numbers of on-line customers, mostly unknown to the sellers;
* Demand for shipments is more unpredictable and unstable as it originates from many more customers;
* Origins and destinations of shipments are more widely dispersed, given that more buyers place direct orders with producers and
distributors and more sellers access buyers globally;
* Accountability for shipments extends through the entire supply chain, compared with traditional logistics in which accountability is limited to single links of the supply chain;
* Customers have high expectations about quality of services and demand fast delivery of shipments;
* Higher incidence of cargoes returned to the supplier than in traditional trade;
* Greater demand for and availability of information covering transactions over entire supply chain, thus allowing on-line shipment tracking and other supply chain management functions;
* More focus on one-to-one marketing, creating demand for customized delivery and post-transaction services;
* Greater complexity in fulfilling international orders than in traditional trade, thus preventing some retailers and service providers from being involved in international e-commerce;
* The emergence of demand for on-line processing of shipments, including cargo booking, bills of lading/airway bills, freight payment, rate quotation, landed price calculations and tariff management;
* Substantial increase in the volume of small shipments, leading to growth of demand for warehousing, transport and other logistics infrastructure that can handle many more small shipments; (page 174).
* Greater scope for customer self-service.

---

**Figure 2. The traditional retail value chain**

---


84 Kalakota and Robinson, loc. cit. Many of these modern partnerships began as outsourcing, especially in the realm of information technology, which made it possible to "get big" quick.
PART TWO: ETAILING TRANSACTIONS AND THEIR VULNERABILITIES

Etailing transactions are composed of four elements: (1) the method of payment, (2) the type of product or service, (3) the parties involved in the sale or transaction, and (4) the delivery of the product. The opportunities for crime (and the opportunities for commerce) may be variously conditioned by each of these four elements.

Methods of payment online fall into two categories: (1) methods that allow for online payment at the time of the purchase, such as credit cards or various forms of electronic or digital cash, and (2) payment offline after the purchase, such as follow-up with phone call and credit card information, a check, a money order, or COD. Offline payments are more common with other kinds of transactions such as auctions, so discussion of these payment methods will be reserved until discussion of those transaction types. Since credit cards are the most common method of payment for online purchases in a typical transaction between a customer and an etailer, an analysis of this transaction and its benefits and vulnerabilities follows.

Online credit card payment

Figure 3 presented a schematic representation of a typical etailing transaction. This was, however, a very simplified representation. Because of the many known opportunities for fraud exploited by criminals in the use of credit cards (existing long before the modern computing environment) procedures have been introduced to ensure validity of the credit card account, verify the cardholder’s identity, check the card against a list of known stolen cards, and check that the card is not counterfeit. These issues have been dealt with extensively in Home Office studies and do not need to be repeated here. However, it is useful to gain an understanding of the
Table 3: The online credit card transaction

1. If new to the e-tailing web site, the customer enters card number on to secure form, usually provided at "virtual checkout" when the "shopping cart" is reviewed.
2. If a registered customer (i.e. one whose credit information is stored on the etailer's database) customer checks box to give etailer permission to use the credit card information from his personal profile.
3. Depending on local arrangements, the card account may be checked with a third party database to verify authenticity, check against database of stolen credit cards.
4. Etailer sends request to acquiring bank for authorization.
5. The acquiring bank sends a message via the interbank network to the consumer's bank or card issuing institution asking for authorization.
6. Consumer's bank sends message to acquiring bank verifying account status, and debiting amount from consumer's credit line.
7. Acquiring bank notifies etailer that the charge has been approved.
8. The etailer fills the consumer's order. (i.e. a message goes to the etailer's supplier who ships the product to the consumer, or, the consumer receives a key to unlock a file to download, such as software or audio files).
9. The etailer's bank sends a settlement request to the customer's bank.
10. The amount of sale is deducted from the consumer's credit card account and the money placed in an interbank settlement account.
11. The acquiring bank credits the etailer's account for the amount of sale (minus fees paid to the acquiring bank), and withdraws the same amount of money from the interbank settlement account.

Benefits of the transaction

Swift authorization. In the 1970s, the time taken for a typical charge card authorization was around a minute, and in that period, only charges above a threshold of typically $50 were checked. Today, the time for authorization is less than five seconds. One can see that a wait of over a minute during an online transaction would eliminate many customers. Swift authorization procedures that make it possible for 100% verification of all charge amounts have helped reduced credit card fraud considerably over the past decade. *89

Swift and reliable payment. Compared to other means of payment, most merchants appear to prefer credit card payments because they represent, generally, virtual immediate payment for the item directly into their bank accounts. In contrast, cash may be counterfeit and checks often bounce. As well there is an established accounting trail that can be followed to identify a bogus transaction. Typically, also, the acquiring banks are those that foot the bill in the case of a fraudulent transaction. It is well known, of course, that the consumer is only liable for a maximum of $50 on any fraudulent transaction. In fact, many card issuing banks do not even charge their customers that amount.

Persons eliminated from transaction. Online transactions eliminate a person to person contact between the sales clerk and the customer. The opportunity for clerk-customer collusion to defraud the merchant is therefore almost eliminated. In order for collusion to occur, more elaborate arrangements would have to be made between an employee of the etailer's web site and accounting section and a customer/hacker.

CRAVED products no longer available. There is no physical contact between the customer and the product to be purchased. Thus, it cannot be, in principle, concealed on his person and stolen from the store, as a shoplifter can do typically in a department store.
Computer as sentinel. The Foresight ecommerce task force noted that an important function of computers in ecommerce is to serve as a sentinel. *90 to monitor activities and flag events or patterns of behaviour that deviate from established profiles. This approach has been used effectively to flag deviant spending patterns on credit card accounts, thus warning of potential fraudulent use. *91 The collection of detailed information from customers in the value chain of etailing should make the use of such databases even more effective.

Vulnerabilities of the transaction

Many points of interception. Table 3 demonstrates clearly that there are many points of interception for a hacker to find in order to deflect payment. Although information moves with great speed from point to point, nevertheless in a network environment, the more points of passage, the more the opportunity for interception.

Proximity to the Internet. While there is, in theory, no need to link the etailer’s web site to the banking network, there remains the possibility that this may happen when the etailer transmits information concerning a transaction to the etailer’s bank. The interbank network is not part of the Internet, but it is an “intranet” - a network of computers closed to outsiders and dedicated only to the service of its members. In these days of interconnectivity, however, it cannot be guaranteed that such a connection will not be made by any etailer for reasons of convenience and to speed up the process even more. It requires only one link to be made between the etailer on the Internet and a banking network, and this is enough to provide a door into the entire system. Thus, every effort should be made to maintain valuable databases and important messaging systems physically separate from the Internet. Ways to do this are discussed in the section below on Prevention.

Dial-up vulnerability. Even if the interbank network is physically separated from the Internet, there still remains the vulnerability of transmissions between the different bank computers that are certainly open to attack. In fact many of the serious intrusions into bank computing systems have been made using means that did not require the open architecture of the Internet. Rather, all the sophisticated hacker needs do is find a way into the closed network: either through a telephone dial up which almost all closed networks or intranets have or through a complicit employee.

Employee vulnerability. If the intranet does not have a dial up entry into its system, there is one other way to obtain entry: through insider information from an employee or by a rogue employee. Thus, it is essential that security procedures be adopted within the network itself to prevent attacks from within, just as much as to prevent attacks from outside. (In fact we have already reported some evidence from the FBI that major portions of losses occur as much from internal threats as from those of outside hackers.) *92 These procedures are outlined later, since most of them apply to all situations in etailing as well as online purchasing.

Attractive databases. A more serious vulnerability is that these etailing web sites, as a part of their efficient value chain, collect extensive information concerning their customers - their web site behaviour, their personal information including credit information and even sometimes their bank accounts. By placing such high value on this aspect of etailing, they have created a most attractive target and a potentially lucrative one. Given that the online environment of retailing has closed off some avenues for theft as mentioned above, one may speculate that a special form of displacement may emerge in which the target becomes the databases of etailers, instead of the actual products that they sell. These databases can be used for a number of criminal activities: credit card information can be used to make fraudulent purchases, the credit card databases can be sold to other criminals for their use, or perhaps worse, the database can be used to extort money from the etailer. At least one major incident of this type has already occurred. *93

The above vulnerabilities clearly reflect the problems of the SCAREM information systems environment. There are other vulnerabilities in the online transaction, but these also apply equally to other kinds of online transactions that will now be considered. It should be added that these vulnerabilities are only those relevant to online payments. There are many other difficulties incurred in using credit cards for payment in the traditional POS situation. Various Home Office reports have carefully examined these issues and recommended many successful solutions for prevention of credit card fraud. *94

*89 This applies especially to the UK where special efforts to speed up verification procedures were recently put in place. See: Clarke and Newman loc. cit.
*93 In 1999 for example, a hacker working from Eastern Europe stole 300,000 card numbers from on-line music store eUniverse, and posted 25,000 of them on the Internet. He demanded a ransom of $1 million or else he would publish the rest of the names. See: Kutler, J (2000). A Lucky Break-in? Institutional Investor. 34(2): 22.
Digital Cash

For those who do not wish to use credit cards, there are various forms of Internet online payment services available, which are known as "digital cash" (or sometimes "electronic cash"). The procedure for establishing digital cash requires usually three steps:

1. Enrolment, in which the consumer establishes an account with a payment system. This may require giving a bank account number for automatic debit or credit of bank account by the digital cash agent, or simply that the consumer place into the particular account a certain amount of money to keep it operative.
2. The purchase, in which the vendor (who is usually registered with the payment system) must agree to accept the digital cash payment.
3. Settlement. The vendor deposits the amount in his bank account. Again, the bank must agree to accept these payments, and is usually registered with the payment system to receive the amount.

The advantages claimed for these forms of payment are:

1. Reduced transaction costs (credit card payments cost anything from 25 to 75 cents per transaction).
2. Because of low cost, suitability for multiple small transactions, such as small fees charged by online databases for downloading of information or articles.
3. Anonymity: as we have seen, credit card payments require the consumer to give up considerable personal information online, which makes their personal information vulnerable to attack. Some merchants also think that they could increase sales if consumers were not required to give out this information;
4. Extension of the market to those not eligible for credit cards (although given the competition among issuing institutions, one doubts that there would be many people these days who could not obtain one).

Typical systems include: PayPal, *95 Cybercash, *96 Digicash (now defunct), *97 and various systems requiring passwords, such as Virtual PIN. *98 Depending on the payment system, the features offered may include:

1. Guaranteed anonymity, in which it is "mathematically impossible" for the bank or merchant to learn the consumer’s identity. One can recognize that this feature is almost identical to a simple cash sale in any store. This transaction occurs usually between two strangers (the sales clerk and the customer). Online, the transaction occurs in even greater anonymity where there is no face-to-face recognition of either party involved.
2. Guaranteed privacy in which the merchant does not know the identity of the consumer but the information is available within the organization that operates the payment system.
3. Individuals, as well as businesses, once enrolled in these services can accept online payment.

None of these methods of online payment, however, solves the problem of the SCAREM information systems environment. Committed intruders can break into any of these systems. Fortunately, computer experts have been especially sensitive to this problem and have devoted much time and money to its solution. Businesses and governments have also worked together through Commercenet *99 to collect information and work towards an industry standard for electronic payment procedures. At bottom is the issue not only of stopping criminal abuse of the online environment, but also the challenge to develop an online payment system that consumers feel they can trust. Industry efforts appear to assume that advanced technology can solve both problems: achieve actual secure electronic payment systems and engender trust among its users. Electronic payment technology is discussed in more detail under the Prevention section.

Auctions

Digital payment systems have also turned out to be extremely useful and popular in another type of sales transaction that occurs on the Internet, that of online auctions.

Strictly speaking, auctions are not e-tailing in the sense that there is no value chain as described above, because the merchant does not acquire goods from manufacturers in order to sell them to customers. Rather, the merchant in this instance acts as a trusted third party who provides a service that matches buyers to sellers. This type of ecommerce is included here because it has over the last five years assumed a place in online transactions that has been extremely popular, and has also brought with it extensive amounts of fraud, by some measures accounting for the greatest amount of fraud that occurs on the Internet. It has also been an extremely successful business model. Ebay, the largest auction site, has been the most successful company on the Internet, having turned a profit every year since its inception in 1995, which is quite an accomplishment compared to the majority of dot.coms that have operated in the red, most of them, even the more successful, yet to turn a profit. Ebay promotes itself as "the leading online marketplace for the sale of goods and services". It has 37.6 million registered users world wide, and transacted more than $5 billion worth of sales in 2000. Its mission, Ebay says without modesty, is "to help practically anyone trade practically anything on earth". *100
Ebay is not strictly speaking an auction, although it provides online access to live auctions. Rather, it provides a marketplace in which buyers and sellers can meet. Ebay provides the organization, listing, the venue for sellers to show their products and services, and also provides a secure way for money to change hands between buyers and sellers. The online transaction for a typical auction works as shown in Table 4.

*95 Unlike other attempts at online payment services, this company has proved very popular. See: https://www.paypal.com/ and the Paypal information centre: http://www.pay-pal-infocenter.com/
*96 Cybercash has recently been taken over by Verisign (https://www.verisign.com) a widely respected company that offers verification procedures (PKI) for credit cards. For a detailed account of how Cybercash works for credit cards see: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1898.html.
*97 Stalder, Felix (1998). DigiCash: Learning from Failure. Telepolis. 11.11.1998. It is of particular interest that DigiCash refused to allow accountless operation, thus guaranteeing anonymity of users, and this has been identified as one reason for its failure. See: http://www.echeque.com/kong/digicash.htm.
*98 Details on how First Virtual works can be found at: http://www.virtualschool.edu/mon/ElectronicProperty/klamond/Fvpymnt.htm. However, this company's web page (http://www.firstvirtual.com/) is no longer accessible in the USA.
*99 http://www.commerce.net

Table 4: Online auction transaction

1. Seller registers certain personal details with Ebay such as a credit card account and address attached to that credit card account.
2. Once registered, seller places item on Ebay’s list of items according to selected categories, and also includes information about the product, the minimum amount and bid accepted, and how long the auction will last (usually 5 to 7 days), and payment options.
3. Buyer searches database for item he/she wants to buy.
4. Once the item has been located, buyer checks out the comments of seller’s previous transactions, especially to check on shipment, honesty, previous customer satisfaction with the seller.
5. Buyer places bid, or in some instances, if seller has included a specific price acceptable for an immediate sale, buyer may offer to buy.
7. Seller checks out buyer’s payment history in the feedback file.
8. Ebay also notifies by email each party of the successful completion of the sale.
9. Seller contacts buyer within prescribed time (usually 3 days), either by email or by phone to arrange payment.
10. Payment options initially are money order or check (product shipped when check is cleared or when money order is received). Obviously, this is a high risk situation since there is no guarantee that the seller will ship the product (it is rare that the shipper ships a product without having received a payment). This is why buyers and sellers leave feedback concerning their satisfaction with the transaction in the Ebay feedback file. Buyers and sellers are urged by Ebay to check out this information which, presumably is assumed to provide a kind of informal self-policing of the "Ebay community".
11. Seller may register with Ebay’s credit card processing service (Billpoint) so that the seller can accept credit cards as payment. This involves the seller providing additional information to Ebay’s Billpoint service, in particular a bank account number as well as the credit card number. Other third party services such as PayPal offer similar services. In either case, the processing of the credit card payment of the buyer is processed in the same way as any other online credit card payment (see above). The difference is that Ebay acts as both the buyer’s and seller’s agent, and charges a small fee for the service.
12. When payment is settled, item is shipped by seller according to shipping instructions included in the original notice of sale.
13. Upon receipt of the product, buyer posts comments concerning satisfaction with the transaction on Ebay’s feedback file. Seller does likewise for the buyer.

Benefits of online auctions

The obvious benefit of this variation on etailing is the business model of bringing buyers and sellers together in a trusted environment. There are different kinds of models within this basic idea. The Ebay model allows almost a “free-for-all” in which buyers and sellers deal
with each other with minimal interference of the third party. The third party makes money by charging a small fee to the seller for listing the product. In other models, the third party plays a heavier role. Half.com, for example, requests the seller to set a specific price (usually following guidelines suggested by Half.com) and lists the item description that it has itself assembled. The only input of the seller is to check off the condition of the product. Half.com therefore sells the item as if it were a regular catalogue retailing transaction, charging shipping, then pays the seller after the transaction is settled. Registration is required of both seller and buyer, and Half.com therefore takes responsibility of seeing through the transaction to the end, although actual delivery of the product is left to the seller. Another variation is that adopted by Crossmarket.com, which requires sellers to sign legally binding agreements that they will ship their products to the highest bidders. In this case, Crossmarket takes full fiduciary responsibility for all transactions. *101 Utrade.com also takes stronger charge of the transaction, requiring buyers to send their money to utrade.com, which then transmits the payment to the seller once it has verified that all requirements of the transaction have been met.

An obvious advantage to this business model is the sheer mass of buyers and sellers that are brought together. As noted above, there are over 37 million registered users on Ebay throughout the world, which makes it possible for sellers to sell just about anything. There is always someone somewhere who wants or needs something that the seller has to sell. And because of the sheer mass, the small amounts that the auction sites charge for listing a product makes them even more popular. It must be the cheapest venue of advertising a product ever invented. For a few dollars, one can reach millions of potential customers.

**Vulnerabilities of online auctions**

Unfortunately, with the great benefits of this business model of etailing, come extensive opportunities for fraud and vulnerability to attack. These include enhancement of opportunities that already existed before online auctions, as well as new ways to commit fraud because of the online environment. We should first note that the online auctions account for by far the greatest portion of online fraud. In 2001, 63% of online frauds were at auctions, followed by the next highest of 11% for general merchandise sales, although the average loss per person was higher for general merchandise sales ($845) compared to auctions ($478). *102 In terms of overall amounts lost in the U.S. $4,371,724 were lost by consumers to online fraud in 2001, an increase of some 30% over the previous year. The opportunities for fraud in the online auction may be summarized as follows:

1. **Bid shilling.** A seller or seller’s associate may assume a false identity and bid up the price of the item. Variations of this could, of course occur in a regular offline auction. However, the ability to create multiple identities to bid in an online auction is extremely easy, and difficult if not impossible to detect.
2. **Bid shielding.** A buyer and his partner make a ridiculously high bid, thereby scaring other bidders away. At the last moment, the high bidder withdraws his bid, and his associate wins the auction with a low bid.
3. **Non delivery.** Seller receives payment and does not deliver the merchandise, or delivers a cheaper product than that advertised. This accounts for some 90% of all frauds on online auctions. As can be seen in Figure 4, the problem here is reflected in the method of payment. When buyers send the seller a money order, cashier check or personal check, there is virtually no recourse.
4. **Non payment.** Bidder does not honour the bid, and does not send payment. While the cost is minimal (the seller will have to list his item again) nevertheless the cost in terms of loss of trust in the process is considerable. In fact, every time someone is victimized in online trading, whether it is the seller or the buyer, it is the business itself - commerce itself as we noted earlier in this paper - that is undermined.

*102 Internet Fraud Watch. http://www.fraud.org/internet/2001stats10mnt.htm. Internet Fraud watch works with the FTC to maintain a database of consumer complaints against Internet fraud.

---

Figure 4. Online auction frauds by method of payment (Jan-Oct. 2001)
All of the above are transaction related frauds. Of course, one obvious opportunity created by this wonderful business model is that it can be used most easily as a venue for disposing of stolen goods. Indeed, the online auction, with its millions of registered subscribers (many registered with identities that are not immediately traceable) is a perfect place to sell counterfeit copies of software, videos, music, and many other "name brand" consumer products. While counterfeit versions of name brand products are commonly found on auction, by far the most extensive counterfeit and black-market trade is conducted in software. While much of this trade is conducted by organized gangs, the fact is that there are many willing buyers. Also, much of this software is indistinguishable from its original, and much may be "graymarket" - legitimate software marketed by special agreement to specific markets, such as educational markets. This makes for considerable difficulty in identifying what software is counterfeit or illegal and what is not. The wide availability of low price CD burners also makes it very easy to produce copies of software and music (and soon videos) that can be sold at auction sites.


Peer-to-Peer Transactions

Selling copies of music that have made on a personal computer with a CD burner is in fact not likely at auction. This is because one can get music at no cost illegally from web sites that operate under a different etailing model. Actually, it is not altogether clear whether such a model should be included as "etailing" or not, although since businesses do make money out of these trading sites, it is reasonable to include a brief note concerning these business models. They also represent what is likely to be one of the more significant changes in online Internet models of computing, one that exploits the major strength of the Internet - its decentralized architecture. We speak here of peer-to-peer transactions.

Peer-to-peer transactions occur as a result of software solutions that make it possible for millions of users to be directly connected with each other via software that they download from a particular web site that hosts the peer-to-peer transactions. The most well known example of this arrangement was Napster which made it possible for millions of its software users to directly exchange songs and music
supercomputers could be run easily using peer-to-peer computing. This may be because (a) there is no money changing hands and (b) the model fits closely with the deeply entrenched "ethic" on the Internet that everything should be free lends strong cultural support for this kind of peer-to-peer model. Napster was certainly held up as the "hero" in defending little people from the large corporations in the lawsuit that eventually put it out of business. At its height, it had 38 million file-sharing adherents and it was at that time when the chairman of the huge conglomerate publisher Bertelsmann made an offer of partnership. When one considers that this massive customer following was accomplished in the space of less than three years, it is a sobering fact indeed to contemplate whether there is any way to counteract such a powerful force. The chairman of Bertelsmann obviously saw that it would be better to co-opt it if he could. As discussed below, there is some hope that technology may provide a solution.

Napster and its successors demonstrate the highly fluid nature of cyberspace trading, and point to a possible direction for the future. One might also expect that a computing environment (architecture) that allows strangers to access directly the personal computers of other strangers is fraught with opportunities for fraud. To date, no examples have emerged of any hacking or fraud that has been perpetrated in this environment. This may be because (a) there is no money changing hands and (b) the model fits closely with the hackers' ethic itself - that everything on the Internet should be free. On the other hand, businesses have begun to experiment with peer-to-peer architecture among businesses or within a large corporation because it offers advantages of security: a network of computers can be arranged so that all valuable data and programs are not stored in one or two central locations or computers ("servers") but may be distributed over a wide range of computers. This is looked on especially as a useful safeguard against a catastrophic attack such as the September 11 attack on the World Trade Centre that destroyed many valuable databases that were stored in one place. While it is true that copies of such databases and sites were kept in backup locations, the restoration of those databases took several days. In the online marketing and telecommunications world, being down for several days can be enormously costly. With peer-to-peer architectures, the databases are spread over many computers and if one computer or more go down, others automatically takes their place. One can also see that, given the number and increasing power of desktop computers, the potential in terms of rapidity of access to data and the amount of data that could be stored is close to limitless. Applications that once required supercomputers could be run easily using peer-to-peer computing. The downside, though, is that if many computers are involved in peer-to-peer computing, they offer many more points of entry for hackers.

Napster and other online "swap" web sites are examples of variations in etailing that occur directly as a result of the type of product traded. Exchanging and swapping songs among friends has been a popular pastime ever since recordings of songs was made possible in mid 20th century. Napster and its successors, through the medium of the connected personal computers simply made this popular pastime possible not only among friends but among strangers via the Internet. There are other products that are sold in specific selling environments on the Internet. The argument mirrored arguments made by the recording industry when cassette tape decks were introduced: that sales of cassettes and records would decrease. Instead, sales of records and cassettes increased considerably. The opponents of Napster have yet to empirically demonstrate that the exchange of music on Napster and like web sites affects regular sales. See: King, Brad (2000). Napster: Music's friend or foe? Wired News. June14. http://www.wired.com/news/ visited 12/10/2001.

Web sites include KaZa and Morpheus and Gnutella.


For example, one company claims to have invented a technology that can embed CD tracks with "road bumps" that will stop uploading or copying ("ripping") of the songs. See: Staff (2001). Sunncomm introduces Napster-proof technology.. CD Computing News. June, Vol.15, Issue 6, pp.1-2.


The idea of specific types of selling environments for specific products is not new. For example, the sale of cigarettes in vending machines is ubiquitous. One of the great advantages of such vending machines is that they make small items, easily concealed by a shoplifter, inaccessible yet at the same time increase the item's visibility and availability. The same may be said of all vending machines, many of which are now also "online" so that their inventory may be monitored and replenished as needed. While one can purchase a range of items on a vending machine, they tend to be limited to small, everyday consumer products such as soft drinks, travel items, cigarettes, sweets and ice cream.

In regard to Internet etailing, almost every type of product is represented on the web. Most are sold on legitimate web sites that began as specialist web sites (e.g. Amazon.com which began selling books, but expanded to electronics and many other products). However, other products commonly attract specific kinds of frauds either due to the special nature of the product or service, or to the kind of transactions involved in selling or administrating that service. A number of computer related crimes such as telemarketing fraud, phone cloning, telecommunications fraud, and pornography have been described briefly in Table 1b and 1c. In what follows, a brief account of two of the more common product specific Internet frauds is provided: (a) fraudulent medical services/products and (b) financial services fraud. Both these types of fraud are not new by any means. There are centuries old scams attached to both of these products. However, as noted often throughout this paper, the Internet makes it much easier and more effective to carry out frauds related to these products. All the advantages of SCAREM offer an enticing environment for fraud. There are also additional advantages:

1. Start-up costs are minimal. One can set up a bogus "storefront" on the web using excellent quality software that will make a web site look as good as any professional and legitimate site. The price of web design software and obtaining an Internet service provider (ISP) are minimal. Thus, individuals with little capital can undertake major investment scams that were previously the province of organized crime.
2. The Internet gives the fraudster instant access to millions of potential victims. In a second, one email solicitation can be sent to millions.
3. Costs of maintaining the bogus operation are also low. Expensive printing of fancy brochures and expensive mailing of them is not required (though some do follow up with these, especially in the case of travel scams). All this can be implemented on the Internet.
4. All the services and power of the web are at the fraudster’s disposal: email for distribution, web sites for deceptive advertising, electronic newsletters to obtain subscribers, and bulletin boards for manipulation of opinion.
5. With minimal knowledge, a fraudster can mimic legitimate techniques of web page operations and con the victim into sending personal information. For example, a fraudster can monitor activity on your computer when you are visiting a web site. Should you enter a credit card number or other personal information, even if encrypted, the fraudster can program a legitimate looking window to pop up and say something like "the card number you entered did not match the record we have in our database. Please re-enter the information". The unsuspecting user dutifully enters in the credit card information, which is then retrieved by the fraudster. This is a case in which all the encryption of keyboard entry does nothing to prevent theft of valuable information.

Financial services fraud

There are two main types of fraud operated in the financial services arena. The first is the kind that applies across the board to many different types of products: the operation of a bogus company (web site), offering services or products that are either non-existent or not what they appear to be. They always involve offers that are too good to be true, and of course they are not! The U.S. Securities and Exchange Commission on its web site gives an extensive description of the many different kinds of bogus investment scams currently being promoted on the web. These include:

1. Online investment newsletters identify false "hot stocks" that they have paid stockbrokers to tout. When readers of the newsletter bid up the stock, the fraudsters unload theirs at a higher price. One convicted fraudster sold 42 million shares in a bogus stock and issued false press releases touting the company.
2. Bulletin boards on which fraudsters collaborate and invent multiple aliases to join the bulletin boards (extremely easy to do), pump up the stock, and again unload them at a higher price ("pump and dump").
3. E-mail "spams" sent to millions pushing worthless stock. For example, one convicted fraudster built bogus web
The second type of financial services fraud involves the manipulation by fraudsters of the transmission of funds from one bank account to another. This can take too forms: the hi-tech form and the low-tech. The high-tech form involves sophisticated hacking into funds transmissions, as was the case described in Table 1a, in which a Russian diverted international transfer funds from Citibank in New York to his own accounts in Russia. However, something similar can be achieved by decidedly low-tech procedures. For example, at the inception of the new online bank X.com, customers opening new accounts could open it in any name and then nominate a bank account from which they wanted to transfer funds to begin the new account. The bank allowed this transaction to take place completely on their Web site, but unfortunately did not bother to verify that the customer owned the rights to the transfer funds bank account. Thus, it was possible for individuals to transfer money into their own accounts, needing to know simply the name and number of someone else's bank account - not an especially difficult piece of information to obtain. The serious implication of this fraud was that the bank Automated Clearinghouse (ACH) system depends on the integrity of its member banks to make accurate requests. Thus, this breach in security threatened the entire basis of the online banking industry. *116

A case using both hi-tech and traditional security lapses, fortunately uncovered before it was completed, was that of a Mafia attempt to "clone" an online branch of the Banco di Sicilia. Using computer technology and the assistance of bank employees, they stole files, codes and passwords from the bank and set up their own operating clone of the bank’s online system. The plan was to steal 264 billion lire (CHECK) by, at an agreed time, switching off the bank’s computing system and substituting the Mafia’s clone. The money, once stolen would be transmitted electronically to overseas bank accounts. The operation was discovered only because of informants. Subsequently an undercover police officer posing as a crooked bank director was able to expose the whole operation. *117

Finally, brief mention should be made of money laundering as it operates in the financial services sector. As noted in Table 1a, approximately $1 trillion are laundered every year. These criminal funds are typically proceeds of drug trafficking and the smuggling of human beings and guns. The typical problem for the launderer is the preponderance of cash that has to be turned into respectable money without bringing notice of bank officials. In fact many countries have regulatory agencies whose job it is to monitor suspicious use of accounts and movement of money. The OECD Financial Action Task Force, for example, maintains a register of "suspicious activity" which is continuously updated. *118 The difficulty that the launderer faces is that banks and other agencies are attuned to watch for unusual patterns in trading, deposits and withdrawals. Thus, launderers devise schemes to make their banking transactions seem legitimate. One of the most typical features of crimes producing lots of cash is that they tend to be crimes that involve crossing borders. Since the Internet operates without restriction of national borders, it is therefore the ideal place for disposing of money in ways that ignore national borders. Although there appears to be no case on record as yet in which the Internet itself was used to launder money (though there are many using banks and electronic bank transfers *119 ) the OECD Financial Action Task Force has outlined ways in which it anticipates criminals may do so. One scenario would be for the criminal to set up a bogus Internet company, (such as, for example, an Internet Café), use the services of this company as if he himself were the customer, charge the costs of these services to "legitimate credit cards" (obtained using fake IDs) then receiving the proceeds from the credit card acquiring bank.

This case is significant because it points once again to the complex transactions that take place between buyers and sellers of services and products on the Internet and the ways in which the Internet’s qualities, such as the ease of setting up a presence, and the ease of using false identities match nicely the qualities valued by a money launderer. In this case, none of the legitimate companies involved: the Internet Service Provider, the credit card issuing bank, or the credit card acquiring bank would have any reason for suspicion. While money laundering does not impact directly on the regular business of etailing, it most certainly could affect or even poison the regular transactions that are involved in everyday etailing.


Medical services/products fraud

Traditional medical fraud is perfectly suited to the Internet where quacks can ply their false medicines and cures using all the
advantages the web has to offer: cheap set-up, anonymity, easy construction of deceptive advertising and web sites, instant access to millions of potential dupes. However, modern health care offers many more opportunities for fraud. In 1998, 22.3 million adults in the U. S. sought medical information on the Internet and this was predicted to rise to 30 million by 2001. Seventy percent of those seeking information on the Internet did so just before visiting their doctor. Types of medical services and health care fraud online include: making false statements, kickbacks and self referrals, unauthorized distribution of drugs and medical devices, violation of privacy laws relating to personal health information, deceptive trade practices in submitting claims to health care plans, and violating rules set down for health care providers that receive reimbursement from federal or national health programs. Of these, online pharmacies are the most relevant to this paper.

Online pharmacies have blossomed in recent years. It is estimated that legitimate sales in online pharmacies will reach $15 billion by 2004. There are over 300 web sites selling healthcare products, and one study revealed that there were at least 86 web sites selling Viagra, the anti-impotence drug, without a doctor’s prescription. These pharmacies have developed a large following of customers even though they operate in what seems to be a confused edge or grey area of the law. The first reason why any etailer is popular is that the merchant is providing a product or service that customers want. And the benefits that online pharmacies offer customers are:

1. Generally cheaper drugs. Bulk purchases by pharmacies can produce savings, but also different regulatory laws governing the pricing of drugs in different countries can create a large difference in price for the same or similar prescription drugs between one country and another. For example, many Canadian pharmacies (online and off line) sell to US customers because their prices are close to half those in the U.S. The FDA estimates that some two million parcels containing prescription drugs enter the US from other countries each year.

2. Privacy. Customers may purchase drugs from the privacy of their own homes.

3. Convenience. Those who are house bound because of infirmity are able to easily purchase prescription drugs they need. Online pharmacies are also available 24 hours a day, 7 days a week.

4. Easier access to written product and other medical information.

5. Easier comparative shopping for preferred prices and products.

The points of vulnerability and opportunities for crime in the online pharmacy transaction (see Table 5) can be identified as follows:

1. Customers’ personal information, especially if they fill in forms concerning health insurance and health history, not to mention credit card information, is collected and stored on the online pharmacy’s web site. This information, as noted several times throughout this paper, creates an attractive database to hackers who can make use out of the information by either selling it or by extortion.

2. The obvious "legal frontier" of these pharmacies, especially those that sell across national borders, makes for even greater opportunity for fraudsters to operate and avoid legal responsibility for their acts. It provides them with an easy avenue of escape should they be caught. And of course, in a grey area of law, it is difficult to be sure just what it is that the online pharmacy is being "caught" doing.

3. There is ample room for deception on the part of fraudsters to pose as legitimate customers, but who in fact seek to purchase prescription drugs in order to resell them on the illegal drug market, or for own drug abuse. Because of the anonymity afforded by the Internet, it is relatively easy for customers to invent identities, and for them also to invent doctors who call in or email prescriptions.

4. If pharmacies are not registered with the State or licensed in some way, there is no way to guarantee the quality of the product purchased. For example, in the mid 1980s, 2 million bogus birth control pills flooded the U.S. market. Because of the CRAVED features of the Internet and SCAREM information system described above, unregulated web sites dispensing drugs could easily become the outlets for counterfeit and otherwise illegally obtained drugs.

5. There is ample room and temptation for professionals (pharmacists and medical profession) to collude with each other in order to exploit the obvious very strong demand of the public to purchase many of these prescription drugs online. The fact that the U.S. Congress has not yet managed to pass the various bills to control online pharmacies is strong evidence of this public demand.

6. When collusion occurs among different personnel and organizations of the health care system, the privacy policy on the part of the online pharmacy is put at risk, and arguably it is health information that is considered by the public as a most important aspect of health care that must be protected.


*121 Ibid.


*125 Ibid. For a Canadian online pharmacy see http://www.canadadrugs.com.
*126 As an aside, it is worth noting that items that are of an intimate nature are the most often stolen from regular drug stores, so there is some possibility that the shifting to online purchasing of these items could decrease their rate of theft.
*128 Richards, Asha (2001). Downfall of the online pharmacy: the legal climate for online drug sales. Internet Law Journal. April 16. The House held a hearing on "Drugstores on the Net" which was followed by the Internet Pharmacy Consumer Protection Act, that initially failed to make it to the house floor. When a version of it subsequently did reach the House, it passed 324 to 101, but legislative analysts believe that it will probably not make it through the Senate. See: Carey, Benedict and Linda Marsas (2001). Bill on online drug sales raises hope, fears. Los Angeles Times. July 16. However, the Pharmaceutical Freedom Act of 2000 did validate the online sale of prescription drugs, requiring that sites post accurate information, and offer medical consultations, the names of consulting doctors and other background information concerning licensing.

Table 5: Online pharmacy transaction *129

1. In the U.S. online pharmacy obtains licenses to sell prescription drugs from the state in which it operates and from states to which it sells. Different rules may apply in different countries. Pharmacies outside U.S. appear not to be covered by these rules.
2. Customers open an account with the pharmacy, submitting credit card, insurance information.
3. Customer submits a valid prescription. This can occur in a number of ways. Customer's doctor may call in, fax or email the prescription. Or, the online pharmacy provides a doctor online to write the prescription, usually based on the customer filling out a patient history form online. Again, different rules apply in different countries, so it is not clear whether in fact this stage is legally required in all countries, or if it is, how enforceable it is by countries outside the customer's domicile.
4. Some sites provide possibility for the customer to ask questions of the pharmacist concerning the product. In the U.S. the customer should be directed or otherwise asked to read the online pharmacy's privacy policy. This rule may not apply in other countries, or even in different states in the U.S.
5. Customer completes purchase, and customer's charge card is submitted for approval, and sale completed appropriately.
6. Order is shipped to customer.

It should be added that there is no strong evidence of actual serious health damage done to customers who purchase prescription drugs online. While there are an estimated 100,000 deaths in the U.S. attributed to adverse drug reactions, there is no research to identify what portion of these resulted from online prescriptions. Furthermore, it is well known that individuals who are committed to obtaining particular prescription drugs are able to "doctor shop" to find a doctor who will write a prescription. Thus it is not at all clear that online prescription writing may be any worse than many obtained from a regular doctor's visit. Only an occasional case has been reported, such as a male adult with a history of heart problems, who purchased Viagra after filling out an online medical questionnaire and subsequently died of a heart attack. *130 And of course, there is the standard problem of Internet retail sales to minors of products that may be controlled by various regulations. One case was reported of a 16 year old who purchased the diet drugs Meridia and Viagra online using his mother's credit card. *131

Opposition to legislation to control online pharmacies in the U.S. has also been voiced by those who claim that there are plenty of laws and regulations already existing to control their practices. In the U.S. primary control of health care systems is left to the States who license health care professionals and pharmacies. However, certain federal agencies such as the FDA, FTC, and the Federal Food Drug and Cosmetic Act provide considerable opportunity for law enforcement. Thus, because of the myriad of jurisdictions, prosecution has been difficult. However there have been some major cases in which online pharmacies have been shut down, even those operating outside the state that brought the charge. *132 And in February 2000, the US Department of Justice announced that it had conducted 134 investigations into health care fraud, 54 of which involved online pharmacies. In addition, 17 convictions had been achieved as a result of FDA actions against illegal sale of drugs (not necessarily by pharmacies) or medical products over the Internet. The best the U.S. law enforcement has been able to do in regard to foreign based online pharmacies is to send them a warning letter. *

Delivering the Product

The modern value chain of etailing was described earlier in Figure 3, and contrasted to the traditional version of retailing in Figure 2. In the traditional version, it was shown how goods are shipped more often (from manufacturer, to wholesaler, to retailer, to retailer’s branch store). This amount of movement of the product opens up well known opportunities for theft of the traditional kind: pilfering during shipment, but especially theft by employees on their own or in collusion with shipping personnel during the stage of loading or unloading goods to and from the truck. Where there is so much human handling of product the risk of theft naturally increases. There is no need to outline these opportunities here since they are well known and reviewed in a number of traditional security texts. Furthermore, they involve physical locations and environments much of which can be dealt with by established security principles.

In contrast, the movement of product in the etailing value chain is reduced considerably. With the middleman (wholesaler) excluded, shipping of the product is direct to the retailer. However, in the etailing environment, even the retailer may be excluded, and the product shipped direct to the customer. Thus, the opportunity for theft is minimized considerably by this simplification of shipping procedure. It also allows for close monitoring of each and every item shipped, especially when conducted in collaboration with the shipping companies that now provide bar coded systems that track every single package to its destination. Thus, even theft during the movement of the item from the manufacturing floor (or, in the case of a large online warehouse such as that of Amazon.com, a computerized picking and packing procedure) there is almost 100% accounting of product to shipper. In addition there is a final check on the shipment of the product: Did the customer receive it? If he did not, an inquiry ensues to track down what went wrong. If the product had been stolen at the point of shipment from the merchant or manufacturer, this would most certainly be revealed by a simple investigation.  

Thus, the obvious vulnerability of the product delivered as a result of the etailing value chain is at the final destination, the customer’s place of residence or designated location for delivery. UPS and FEDEX for example publish their security standards on their web sites. The advantages that these shippers offer over the regular postal services offered by government agencies in all countries (though the exact manner in which they serve governments varies, as many have been partly “privatised”) is that the large majority of parcels shipped are picked up by the shippers, and require name, address and other information of both shipper and recipient. All items are bar-coded and tracked electronically. Indeed, individuals can log on to the web sites of these shippers and determine the progress of the shipment. Furthermore, the security standards encourage shippers to inform their customers or addressees that they have shipped the item, so that the recipient can be on the look-out for the parcel, and thus reduce the obvious point of vulnerability in this delivery system - the possibility that the item may be left at a location that is unattended (if the customer is not at home and the shipper has not checked the preference to require a recipient signature). This arrangement works well in some localities rather than others, depending on the visibility and availability of parcels left of doorsteps. In crowded inner city apartment buildings without a doorman or entry, parcels are obviously more available to theft. In these circumstances, senders have the option of requesting that the recipient sign for receipt of the package, which costs a little more. Thus, the risk of theft is shifted to the sender, who decides whether reducing the risk is worth the price or not.

An additional method of controlling delivery used by some online stores that also have local stores, is to have the item shipped for customer pick-up at the local store. While this eliminates the risk of theft from the customer’s home if it is unattended, it may increase the risk of theft at the location of the local store in its stock room. There are no comparative data concerning this issue.

Another method of shipment also includes with it a method of payment, which is cash on delivery (COD). This option is offered by most independent shipping companies, and provides an increased guarantee for the recipient that he be satisfied with the condition of the product shipped before paying. However, it does increase the opportunity for theft since cash (and it is always cash that is required as is the payment medium, since individuals who choose this option have spurned any other form of online payment, including credit cards), must be handled in a situation, usually the customer’s location that lacks control from the point of view of the seller. However, to the writers’ knowledge there exist no data concerning the rates of loss either of cash on COD or of items left at unattended locations.

A new method of delivery of product has emerged from the modern computing environment, which is the downloading of software for immediate use. There are many software etailing web sites that now offer this option to consumers. This method of delivery avoids all the risks and opportunities for crime of the physical delivery systems, and furthermore offers the customer immediate acquisition of the product, just like in a regular store. In fact, it is better than buying software in a retail store because the product delivery and installation can be directly controlled by the software etailing site, thus avoiding user installation errors. The only opportunity for crime here is for the customer to either break the encryption methods used by the retailer (unlikely) or to have illegally obtained the ID of an individual and purchase the software using that person’s information. There were early difficulties in perfecting the software download delivery procedures, but generally these have been solved. In fact the delivery system is so smooth, and the amount of band width has expanded so much (that is the speed at which an individual can download a file using connections to the Internet that do not require dialling up), that many software companies now offer their software on a subscription basis that automatically updates itself on the user’s own computer each time the computer is switched on and is connected to the Internet. This approach has been adopted for virus detection software where constant updating is necessary to keep up with new viruses. The download delivery is also used by software etailers who offer "shareware" or variations of this, in which customers may download and run a program to "try before they buy".

PART THREE: PREVENTION AND CONTROL

This review has outlined the information environment in which etailing is conducted, the points of vulnerability and opportunity for crime that the etailing environment unwittingly fosters, while providing unparalleled opportunities and benefits to business and customers alike. It has been shown using the situational prevention approach that information in the information society is clearly a "hot product", CRAVED in all respects. And it has been demonstrated that the information systems that make up the etailing environment display crime-inducing features of SCAREM: stealth, challenge, anonymity, reconnaissance, escape and multiplicity. Many different examples of ecrimes were described ranging from those with immediate and direct impact on etailing, to those that had severe though indirect effects. It is now time to turn to the possible ways of preventing ecrime in the etailing environment. This will be accomplished by continuing to apply the approach of situational crime prevention.

Before beginning a survey of preventive possibilities in etailing it is important to mention three aspects of the situational approach that guide this task:

1. Situational crime prevention not confined to physical locations, but concerns itself with all aspects of the transaction between victim and offender. Therefore, situations must be examined in all their complexities, the "virtual elements" such as the relationships among different users of the online environment, and the "physical elements" such as the actual places in which individuals reside and carry out physical actions.

2. The situational approach is not confined by elements of time. When a customer makes an online purchase, he does so within a certain span of time, which may be defined as a "virtual point of sale". But the online sale is a highly complex process as demonstrated in Table 3, and exists only within the context of cyberspace in which various kinds of information move rapidly and long distances. These rapid movements can, however, leave traces or maps of their movement that may be stored. Thus, the "virtual point of sale" can be included as part of a history of tiny fleeting electronic movements of information to become an important focus of inquiry as to what went wrong, in the case of an intrusion or theft. "Situations" therefore can be reconstructed as slices of time in order to identify security weaknesses.

3. The conception of information as a hot product, and the identification of SCAREM attributes of the information system, suggest that there are strong motivations for individuals to commit crime on the Internet. The situational approach has always taken great pains to attend not only to the "physical" elements of a situation but also to the motivations of offenders. The two are, of course, inextricable, as the situational approach has argued and demonstrated many times.

In sum, a particular crime may be composed of any number of situations, some of which may be important in prevention, others less important. The significant situation that will be focused on will depend on the context of the criminal event, which includes both space (virtual and real) and time (moving and static), and the presence (physical or virtual) of motivated offenders.

Sixteen Opportunity-Reducing Techniques for Etailing Crime

In his book *Situational Prevention: Successful Case Studies*, Clarke has outlined four main ways of reducing the opportunities for crime: (1) increasing the perceived effort, (2) increasing the perceived risks, (3) reducing anticipated rewards and (4) removing excuses. Clarke also identified within each of the four elements of crime reduction sixteen what he calls "opportunity-reducing techniques". Suggestions for preventing etailing crimes will be presented below using these sixteen techniques with some minor adaptations to suit the information environment. The main adjustment has been to include suggestions for opportunity reducing techniques from the points of view of the major players in the etailing environment. These are: the merchant, the customer, government regulatory and law enforcement agencies, legislatures, trade associations and public oriented institutions such as colleges, universities and public libraries. Universities are especially important because in those venues students have considerable access to powerful computing facilities, and it is there that major hacking events have often originated. It is also college campuses where the hacker’s ethic of "everything free" is most likely to linger. Furthermore, college students are probably the main customers of the free exchange of music via the peer-to-peer web sites such as KaZaa and Morpheus. Of the players, merchants and customers are the two who are the primary guardians of the target or targets (i.e. the information that each of them owns and transmits). Government, trade associations and colleges are the primary institutions or organizations that are positioned to influence or even implement many of the opportunity reducing techniques.
In making preventive suggestions, reference is made wherever possible to actual attempts that have been made to reduce e-tailing crime. However, there exists no systematic research on the effectiveness of any (let alone situational) crime prevention techniques on the e-tailing environment, although there are a number of well-researched techniques to prevent intrusion into computing systems. Many of those techniques are highly technical. However, in using an overall situational approach one also avoids the trap of imagining that technology will solve the problems of crime prevention in e-tailing. The situational approach requires one to evaluate all aspects of the situations in which the crime occurs, and technology, though important, is only one such factor.

The sixteen opportunity reducing techniques are summarized in Table 6 and discussed in below under the four main situational prevention approaches.

**Increasing perceived effort**

1. **Target hardening.** As noted in Tables 1a-1c, computers (defined broadly to include telephones and other computing devices) may be seen as tools or targets or both depending on the kind of offence. Strictly speaking, in the information environment information is the ultimate target, so measures to protect and harden both are needed.

**Merchants.** Bandit screens introduced to London Post Offices in the 1980s, which reduced robberies by some 40%. "Firewalls" fulfill a similar function in the online environment. Firewalls may be installed as either hardware or software, and their function is to block entry of unauthorized users from another network, usually from the Internet. Because the Internet is such an open system, anyone theoretically can attempt to gain entry into a company’s closed network, or intranet). While merchants may certainly want Internet users to enter their web sites, they certainly do not want the common user to enter their valuable databases. An important function of the firewall is also to control any transmission of information out of the intranet to the Internet. The firewall intercepts all messages and transmissions and checks for their authenticity. There are many different versions and arrangements of firewalls, and many highly technical factors need not concern us here. Suffice it to say that all firewalls intercept all transmissions to and from a company’s private network and the Internet. They intercept email, web browsing, filter unwanted transmissions, check and filter files that are sent back and forth.

Obviously, a major problem is where to locate the merchant’s web site in respect to the firewall, behind it or outside it. A web site is more likely to be attacked than files behind the firewall. Thus, it could be better in front. However, if the web site is attacked, it could result in embarrassment such as happened to the U.S. Department of Justice when its web site was attacked and reconfigured with pornographic images) or valuable down time. On the other hand if the web site is configured behind the firewall, the firewall will have to be carefully configured in order to allow the verified customers to pass through. This itself is very difficult. Some claim that in this situation two firewalls may be needed. In any event, the computer and accompanying network hardware must be maintained in a physically secure location, usually in a locked room, with access limited only to those so authorized. Highly valuable databases such as customer credit information etc. should also be maintained in this secure location, and certainly behind a firewall.

However, problems of security remain with the many workstations and computers in a typical business office, and these workstations may have several different users. Since these workstations are most likely behind the firewall, special security procedures are necessary to make sure that employees do not compromise the system either purposely or inadvertently. This is achieved by various procedures such as: disallow employees to download files without proper authorization, disallow employees to take home work on disks, do not allow, or limit dial up access to intranet. The latter is most important because the most serious intrusions into networks (especially telecommunication and government agencies) have occurred through dial-up entry. The merchant's security manager should constantly review the network for software holes and bugs, since it is well known that all operating system software that makes the Internet and personal computers work, have bugs and errors that can be exploited by sophisticated and even less sophisticated hackers. Finally, screen locks that switch the screen off after a period of inactivity, requiring a password to switch it back on, should be used to avoid unauthorized persons picking up information from the computer screen. It bears repeating that many of the cases of hacking described through this paper have been carried out by those who were not computer sophisticates, but those who obtained necessary information from employees or others inside the merchant’s network.

**Software and Network Companies:*** Many products would be less attractive to criminals if they had been designed differently. For example, the design of credit cards makes them easy to counterfeit and eminently usable by those unauthorized to do so. The introduction of picture ID for credit cards and other design changes has made them much more difficult to use for fraud. When new operating system languages are written, especially those for the Internet (and surely more will be written) they should also be designed to include security concerns from the outset. Unfortunately, because of the structure of computer languages, it is far more difficult, and mostly impossible to rewrite them to correct the errors that cause security holes, although certainly much improvement has occurred over the years, particularly in regard to UNIX, arguably the backbone or the Internet operating languages.

**Customer:** Many of the procedures described for the merchant apply. The user should keep personal computing devices in a physically secure place, and avoid using them in crowded surroundings (cell phones, personal digital assistants or PDAs) and install a software firewall if his computer remains connected to the Internet for long periods.

---

2. Access control. This technique is probably the most widely used and well developed technique in the computing environment. It can be traced to the use of moats and drawbridges of medieval times, and the design of apartment buildings as they relate to "defensible space". Passwords and PINS, of course are the most typical technique for preserving access in the computing environment.

**Merchant:** There are many different kinds of passwords and technical specifications for their implementation. Since the wide adoption of bankcards and debit cards many more people have become used to using PINS to gain access to their accounts and money. Passwords and PINS are now routinely required for access to computing systems. Multi-user workstations in business offices depend on user IDs and passwords to allow different users to log on to the same machine. Because of the valuable (and vulnerable) nature of business databases, different levels of access must be set up, and employees differentiated on the need-to-know basis. All web etailing sites require passwords and user IDs for access to the purchasing step in the shopping program. Because these PINS provide access to vital data, the merchant databases that contain the passwords represent extremely high value to merchants and to customers, and thus make attractive targets. Thus, although passwords are created in order to protect the computing environment, the passwords themselves become targets for criminals. Auction web sites have a special responsibility to refuse to register sellers who have a poor or suspect transaction record (usually available for inspection on an auction's web site). However, in the case of auctions, requiring a user ID and password to register as a seller does not guarantee the identity of the individual who has registered. Some argue that this is the way it should be, since after all this is the way it is at garage sales or even in shops. If one pays cash, one's identity is irrelevant to the purchase.

**Customer:** Customers are probably the most vulnerable and least protected when it comes to access to their personal computing environment. In the customer's own place, the customer should use passwords for access to personal computing devices and computer files, and store passwords in secure places (ideally not on the personal computer). Nor should one open suspicious email or program files sent over the Internet, as these may contain hidden programs that can embed themselves in one's computer. While viruses certainly do damage, more seriously, other programs may search the computer for passwords, bank accounts etc. and send them to a criminal who is connected to the Internet on the other side of the world. Peer-to-peer programs such as those that are downloaded for music exchange (e.g., KaZaa, Morpheus) are especially prone to this. In January 2002, for example, it became known that these and other companies were embedding programs with the download of their software (which is free) on the user's computer, which then monitored the previous two days' web browsing, in order to target the user with advertisements. Finally, the usual security procedures should be taken in regard to credit card use online: one should never give out credit card information unless on a secure etailing site and one should always query requests for personal information.

3. Safeguarding data integrity and origin. It is important to ensure that files have not been moved, changed or deleted while in transit, especially in regard to online transactions. Performing standard verification procedures on file integrity increases the difficulty of those who would either change the files for nefarious purposes, or others to claim that they never did what they did.

**Merchant:** Periodically verify attributes of critical files by using check-sum operations, and comparing them to their originals. To guard against repudiation (when customer claims a transaction never took place), use public-key cryptography and other digital identification methods to verify files (see technique 10, Identifying property).

**Customer:** Keep records of transactions with etailers, including receipts, transaction numbers, etc.

Law enforcement and legislatures: The US government strictly controls the levels of cryptography allowed on products and services whose destination is abroad. This means that the civilian sphere (that is commerce) is far less protected by cryptography than is the military sphere. Governments must allow use of high-level cryptography in the civilian sphere and internationally to guard against terrorism, because terrorism is in fact a commercial threat. Since September 11, there can no longer be a clear distinction between commercial and military spheres when it comes to terrorism. The terrorist act of September 11 had direct and severe impact on the U.S. economy and commerce generally. There are also many cases on record of foreign nationals hacking into commercial networks of the U. S. Furthermore, because commerce now widely uses the Internet, any attack on one part of the Internet must have an effect on commercial activity.

4. Controlling facilitators. The anonymity afforded users of the telephone when electronic switching was introduced in the 1960s facilitated the use of the telephone to make obscene or harassing calls. The introduction of caller-ID in the early 1990s which effectively removed the anonymity of phone calls, was found to reduce the number of obscene and harassing calls. **There are a number of facilitators on the Internet. These include anonymity, deception, and aliases all of which challenge the authentication of identity. The other major facilitator on the Internet is information itself, and it poses a fantastic paradox. On the one hand users on the Internet demand privacy in the extreme to be able to interact not only anonymously but deceptively using "virtual" identities. But on the other, the force of the Internet is to make all knowledge and information accessible and available to all.**

**Merchant:** Some argue that anonymity is an essential element of open markets although it is never stated just how widely this belief is held, nor why it is so essential. Since all agree that it is trust that makes commerce possible, one would have thought that knowing...
those with whom one does business will enhance trust. However, from the etailing merchant’s point of view, it is essential that not only information concerning the customer’s credit information is obtained, but as much information about the customer’s buying habits and online interests as possible. This new approach was outlined in the discussion of the etailing value chain (Figure 3). And it has also been shown that credit card fraud was been reduced considerably as a result of procedures that essentially added significantly to knowledge of the customer’s identity. This trend can only continue as new smart cards are introduced and PINs are required with their use as well. Merchants should install the latest technology to establish customer authentication. Require PINs to be used in conjunction with credit cards. New ways to authenticate the cardholder are also emerging, such as biometric authentication of identity. Thus, merchants are advised to favour only credit cards as payment, because the opportunities for credit card fraud are rapidly decreasing, and the form of payment provides far more information about the customer than any other popular form of payment.

Software manufacturers: It is a paradox that software manufacturers, especially those that sell operating system software, release versions of their software with known and unknown errors in the them. These bugs or "holes" can be exploited by hackers to break though firewall protection. Thus, software manufacturers must convey to security managers and the computing world generally, information concerning known bugs. Indeed, there are also many news groups and bulletin boards on the Internet devoted to disseminating information concerning these holes and how to fix them. Unfortunately, because the Internet is an open system, it is especially difficult to convey this information only to security managers and computing professionals, without also providing opportunities to those who would like to exploit these software errors. At the periodic briefings ("Black Hat Briefings") that Microsoft holds, for example, this information is conveyed, and some have argued that these briefings should not be open to the public because they provide valuable information to hackers. Guidelines for disclosure of such information are badly needed.

Customer: Customers can provide information about their activities in two ways: by failing to maintain proper security procedures with their own personal computer, and using public use computers to make online purchases (such as computers in an Internet Café or public library). Web browsers can be set up to record the history of web ages visited and can also retain passwords and user IDs. Also, participants in auctions should never pay for an item with cash, because by far the highest cause of loss in online auctions is non receipt of items that have been paid for with cash. Credit cards are the most secure form of payment both for the seller and buyer - even though surveys show that the majority of people believe that credit cards are an insecure form of payment online. The truth is that credit cards are far more secure online than off line. Online auctions also provide third party escrow and card acceptance services so that the seller can accept credit card payment via the trusted third party, and the buyer can submit credit card information to a trusted third party without fear of fraud. However, customers must also be constantly vigilant for deceptions that are used by savvy operators who imitate legitimate online retailer web pages and purchase systems, and ask users to input their credit and other personal information. Customers should check out the authenticity of web sites if buying grey market products such as pornography, prescription drugs, investment and tax avoidance services online. It is clear from the earlier review of such sites that deception is more likely at such sites, and this includes as well the utilization and theft of the customer's credit and other personal information.

Law enforcement: Regulatory agencies must constantly search the Internet for bogus web pages, and bogus companies that, through deception, can con users into giving out valuable information or into buying bogus, worthless or non-existent goods (investment and medical fraud). As often noted, the Internet is the perfect environment for deception. In fact it cultivates it. In addition, the appropriate agency should regulate advertising which again is perfectly suited to deceive users of the Internet. Law enforcement should also constantly search for bulletin boards that convey information on how to hack into computer systems, and other knowledge that may be hard to get. As noted, there are many hacker bulletin boards and news groups where such information is exchanged.

*140 Ahuja (1996). Op. cit. p. 164-166. This is a computation that summarizes a number of characteristics of a file, and should be identical to the check-sum performed on the original file.
*142 Adam Smith marvellted that self interest that drove individuals to enter commerce, and that people who were complete strangers benefited from that self interest since they also were able to enter commerce, and buy and sell with others. Smith admired the complexity of the free market system. It could be argued that if we knew those with whom we traded better, and recognized their self interest, we would trust them less. But if free markets work in the way Smith argued, then we do not need to get to know others to find out that they also are motivated by self interest. The fact is that Smith did not take into account the relatively few individuals who would not play by the rules. And why should he when he saw that the free market system worked so well? The difference today is that fewer people not playing by the rules can do much greater damage than in a market of the 17th century, because of the Internet environment where one small act of terror can disable an entire network.
*144 The difficulties of authenticating the identity of individuals should not be understated, especially given the comparatively recent increases in theft of identity. It is speculated that the increase in identity theft is a direct result of the successful steps take in controlling credit card transaction fraud, especially introducing smart cards in the U.K. The only way to overcome smart cards with PINS is to assume the complete identity of an individual which would include knowing the PIN of that individual's card and the password for online bank account etc. Ways to counteract this are also in progress, such as using a biometric device to match the card with the individual. See the research report by Jones and Levi ibid.
Increasing perceived risks

5. Detecting intrusions. In regular retailing, the introduction of merchandise tagging, bar-coding and electronic point of sale has resulted in significant reductions in shoplifting when offenders were detected by alarms triggered by the tags. The equivalent to these systems in the computing environment is the introduction of hardware and software traps that will identify intruders should they manage to break into the system.

*Merchant*: Monitor every keystroke made by customers from entry to website to exit after sale. Monitor the keystrokes of all employee users. The collection of this information provides audit trails that can be analysed for regular patterns and individual profiles. This technique has been used to flag deviant or unusual credit card use, and can also be used to flag any unusual computer use that does not fit with past profiles. Check for "sniffers" which are hidden programs that can record all "packets" of information as they are transmitted through various points of a network or networks. These sniffers are widely available on the Internet along with instructions on how to install them. *147* Those who place the sniffer can collect all passwords and user IDs that pass through the sniffing point. These sniffers exploit weaknesses or errors in operating system languages, as well as the decentralized structure of the Internet itself. Sun operating systems have been the favourite targets. Two fixes are possible: (a) Security managers should frequently run software (made available by Sun) that checks for these error states and can detect possible operation of rogue programs and (b) all transmissions should be encrypted using one of the many systems now available.

*Customer*: Install firewall and virus scan software that detects rogue files and "cookies" - files that web sites place in the user's computer to make the web page operate faster and enable other advanced features to operate. Generally speaking, the less of these the better.


6. Formal surveillance. Clarke notes that visible surveillance by security guards, CCTV and police serve as a deterrent to would-be offenders, and cites a number of studies supporting their effectiveness in such places as parking lots, burglar alarms and random breath testing. Times of day and frequency of patrols may also be significant. In the absence of any research concerning the deterrent effects of formal surveillance on the Internet, it is difficult to suggest possible opportunity reducing techniques of formal surveillance. The reason for this is that one of the attributes identified in hackers is that they are motivated by the challenge (the C in SCAREM) to beat the system. Thus, formal and visible surveillance may have an opposite effect; encouraging the crime rather than deterring it.

*Merchant*: Advertise clearly on the etailing web site, especially on pages in the purchasing process, that high level encryption is used, that databases are protected by a trusted name-authentication company (e.g., Verisign). Surveillance may be effective at certain times of the day, depending on the etailing site's customers. If the majority of them are during the day, the chances are that attacks on the computing environment from hackers will occur late at night, when few if any systems operators are on duty. Thus, it is necessary to monitor user activity and assess what time of day intrusion attempts are more likely.

*Customer*: Supervise others who use one's computer, such as friends and family.

*Law enforcement Agencies*: Anonymity works well for crooks on the Internet, but is also works for law enforcement. It is an easy matter for law enforcement personnel to maintain a hidden presence on news groups and bulletin boards that exchange crime facilitating information. While maintaining a hidden presence they should at the same time make public announcements of fraud investigations, their frequency and their successful prosecution.

7. Surveillance by employees and customers. Regular employees in various positions such as doormen, park keepers, parking lot attendants and shop assistants, all assume some informal, if not formal responsibility for monitoring conduct in their workplaces. Substantial reductions in crime have been found as a result of enhancing this vigilance. It is a well established principle of retailing security to train employees in security procedures, and even to encourage them to be actually part of the formal security program. *148* It is rare, though, for regular retailers to enlist the help of their customers in identifying theft, even though it is known that substantial theft is carried out by employees in a retail establishment.

*Merchant*: Include regular employees as part of the security team. Train all employees in correct security procedures and habits. Offer incentives for employee vigilance both of each other and customer online behaviour. Use customer service to educate consumers about maintaining vigilance and security procedures.

*Customers*: Report any suspicious emails or web site requests for information to etailing web site or to Internet Service Provider (ISP).

National and international legislation establishes clearly the identity of the consumer to the vendor, but they also establish a clear audit trail. In the case of repudiation, technologically, and have an excellent record for securing payments. Digital signatures also have other important benefits: Not only do they demonstrate that the consumer has a legitimate account with the payment system and is who he says he is. These systems are highly sophisticated and are becoming widely used. Authentication procedures using digital signatures, digital certificates or other software to establish the “identity” of the consumer (that is, verifying ownership) are now widespread. The technology consists of basically two elements: (a) encryption of all transmissions and messages, and (b) special authentication procedures using digital signatures, digital certificates or other software to establish the “identity” of the consumer (that is, verifying ownership). These systems are highly sophisticated technologically, and have an excellent record for securing payments. Digital signatures also have other important benefits: Not only do they establish clearly the identity of the consumer to the vendor, but they also establish a clear audit trail. In the case of repudiation, for example, a situation in which the consumer claims that he did not order a particular item, the digital signature will reveal whether in fact he did so. In other words, it takes the place of the traditional personal handwritten signature. This technology has spawned a flurry of legislative activity that has passed laws (or is in the process of doing so) regulating encryption in the business environment, its use by law enforcement, and defining and giving legal recognition to digital signatures and certificates. National and international legislation has been very active in recent years, much of it based on this technology.

The use of digital certificates in consumer electronic payments is relatively new, but has been extensively researched over the past few years, especially in regard to electronic transactions between businesses, where the amounts or value of the exchange are very high. However, recently there has been an increasing willingness to apply this technology to consumer purchases. Visa International has published extensive information concerning its recommended security standards, with particular reference to PKI infrastructure that uses digital certificates for authentication.

The work of the SEMPER project for the EU, for example, has established a model electronic payment system which also...
electronic signatures the same legal status as a written signature. In the USA, the Electronic Signatures in Global and National Commerce Act (E-SIGN) was signed into law in 2001, and affords electronic signatures the same legal status as a written signature. Digital certificates and signatures offer several advantages over any other method of electronic authentication. While the topic is far too complex to deal with in any depth in this paper, briefly the way this technology works is as follows.

The system is based on a simple principle used by Western Union when it wires money for a client. The client in London gives cash to Western Union and the name or other identifier of the recipient in New York. The client is asked by Western Union to provide a question and its answer that only the recipient could know. The recipient goes to the Western Union desk in New York, gives his name, answers the question correctly, and receives the money. The authentication process depends on both the sender and the receiver knowing the "key" to the message (which "unlocks" the money which is conveyed by a trusted third party). Obviously, this method would be very cumbersome if it were to be used by an online retailer with thousands, perhaps millions of customers. Every customer would have to have a question that only he and the retailer knew. As well, the customer would have to convey somehow either by email or phone what the question was, which would defeat the whole purpose of the exercise! Instead, a complicated system called "Public Key Infrastructure" (PKI) is established.

PKI works by establishing encrypted keys at each end of the transaction. The sender uses one key to encrypt the message, and the other key is used to decrypt the message by the recipient. These keys are mathematically related, but one of the keys can be "public" or shared with others. These keys are used along with a digital signature, a cryptographic mechanism that guarantees sender verification, which provides a unique "fingerprint" of the digital environment from which the message is sent. These signatures can be combined with the message itself and again encrypted so that a unique "fingerprint" of the document itself is produced. Thus, the recipient, using his key can not only verify the authenticity of the sender, but also of the document itself, and can be sure that the message was not intercepted and changed or that it has been sent by an individual who is pretending to be the sender. This very oversimplified description nevertheless demonstrates that this system is highly complex. Estimates are that it costs between $500,000 to $1,000,000 per company to establish. Nevertheless, Visa international has already incorporated aspects of PKI into its verifications procedures for credit card payments and many other major etailing web sites have introduced the system.

It should be noted that the property being marked here is essentially the identity of the user. The problem here is to establish with some certainty that the user really is who he says he is. In an attempt to solve this very difficult problem, a new system for electronic payment is the "smart card". A basic smart card contains a computer chip embedded in the card itself. It may be either exposed so that it may be read on contact with the card reader, or it may be embedded inside the plastic of the card, and read by means of remote electronics (some phone cards are like this). There are several advantages to the smart card over the regular card with a magnetic stripe. First, it actually can process information on the card and can store a record of its use. It is therefore possible for the card to contain several levels of security, to be able to conduct security checks within its own micro-processor, so that, in the more sophisticated cards, they do not need to be constantly checked by a central system that contains a database of the usual information, such as credit limits etc. The card also can require a PIN number to be entered (much as is already required for Bank Cards for ATM's which incidentally have a very low fraud rate), or it may contain its own means of identification using a special messaging algorithm. The smart card has been used in France since the late 1980s, and that country has a very low credit card fraud rate. The smart card have been implemented on many university campuses in the United States, as well as in regions throughout the world, in particular Switzerland and Australia (including the Olympic Games in Sydney), New Zealand, South Africa and Taiwan, all with very promising results in so far as user acceptability is concerned, though there are no measures of fraud available. The United Kingdom began to phase in smart cards with PIN numbers in November of 2000. Experts claim that the level of investment that fraudsters would need to make in order to hack through a smart card (sometimes called a chip card) will far outweigh the reward, and as well, the chips can more easily be updated and changed, making it easier to remain one step ahead of even the most sophisticated fraudster.

The promise of these cards is considerable, since in theory they could be used instead of cash anywhere, provided the POS had the technical equipment to recognize them, and because most importantly, the recognition system does not depend on reference to an online database, thus eliminating a major source of vulnerability. They can also be encrypted with digital certificates and signatures. This does, of course, shift the focus of vulnerability to the person of the user. The only way an intruder could break into the smart card system would be to extort or otherwise trick the user into giving him the PIN. However, when it comes to online payments, the consumer's computer would have to be fitted with an attachment that could read the smart card.

Merchant: Use digital signatures and digital certificates for all online transactions. Design web pages so that they are not duplicable, and therefore forged web sites can be more easily detected. Copyright all web pages. As part of customer service educate consumers about the benefits of digital signatures and certificates.

Customer: Only shop on etailing sites that digitally encrypt transactions. Use password protection and User ID on own computing devices. Question the authenticity of all windows that pop up during web surfing. Never enter personal information unless the site has been thoroughly authenticated.

Trade Associations: Campaign for introduction of smart cards into all digital payment systems. Maintain vigilance for copyright violations.
Legislatures: Design legislation based on digital certificate and encrypted technology. Set standards and requirements of all e-tailing environments for digital encryption for secure payment transactions. Set clear standards for protection of intellectual property. *174

*150 There is a large literature on encryption and its use for data protection. This is partly due to the fact that computer professionals enjoy the challenge of solving difficult puzzles, but it is also due to the fact that encryption has had serious and central implications for what governments perceive as their sovereignty and national security. At the simplest level, the earlier versions of Netscape Navigator included encrypted security levels designed specifically for transmission of such data as credit card information over the Internet during e-tailing transactions. However, those versions of Netscape had two different levels of security: one for internal US use and one for international use. The international security level was much less rigorous than the national level because of the US Federal Government laws that regulated the export of encrypted material (see Garfinkel, op. cit. p.12). The US government, because of market forces, has been forced to gradually liberalize its position on the restriction of export of encrypted information. See: Thomsen, Roszel C.II. and Antoinette D. Paytas (2001). US to EU! The United States amends its export controls of encryption, responding to recent developments in the European Union. Computer law and security report. Vol.17, no.1.


*152 Law enforcement is very involved in encryption technology because of the perceived need for law enforcement to be able to intercept encrypted messages by criminals or enemies of the State. See: Cabinet Office, UK (1999). Encryption and Law enforcement A performance and innovation unit report. May.


*155 Traders in electric power have been the earlier significant users of this technology. Power companies traded more than $30 billion in electric power by 2000. Greenberg, Eric.(2000).Real-World security. PC Magazine. Vol.19, Issue 15, pp.106-109.


*174 See for example the Digital Millenium Copyright act. 1998 (DMCA) which proposes a maximum of $500,000 fine and 5 years prison for copyright violations, among a number of other highly restrictive standards. See: Zielinski, Dave (2001). Stop Thief! The great web copyright crackdown. Presentations. July. http://www.presentations.com

11. Reducing temptation. The mere presence of a weapon, such as a gun, can induce aggression in some people. Cars that are popular for joyriding, if parked on certain streets tempt delinquent joy riders. Failure to deal promptly with minor signs of decay tempts people to commit vandalism. The equivalent to this situation in the computing environment is the Internet itself. As noted throughout this paper, hackers find the mere existence of the Internet a temptation. Indeed, some have even claimed that people can become addicted to surfing the web. The problem e-tailers face, therefore, is how to strike the right balance of demonstrating to potential vandals that all computing systems of the e-tailer are under constant surveillance and intrusions dealt with immediately, and at the same time not
announcing this important information in such a way that it offers a challenge to hackers to overcome the etailer’s security system. This is a job that the etailer cannot do alone.

**Merchant**: Repair system damage immediately, especially if caused by vandalism. Note on web site that the system is closely monitored for intruders and announce this on the purchasing web pages. Citibank’s security statement may be taken as a model. *175 It is displayed without fanfare, but is there for those who want to find it. Use customer service and every chance there is to educate customers about the security systems in place.

**Customer**: Customers on the Internet are constantly bombarded by temptations sent to them in the form of cunningly worded unsolicited emails from fraudsters. In this case, customers need to resist the temptation to become a victim!

**Legislature**: Legislate appropriately severe punishments for etailing crimes, so that it is clear that the punishment outweighs the pleasure of yielding to the temptation to damage or otherwise defraud Internet users.

**Law Enforcement**: Regulate fraudulent advertising and scam web sites, and constantly publicize the effectiveness of security systems in the online environment and effectiveness of law enforcement of catching offenders.

**Internet Service Providers and System administrators**: Install filtering software that removes spam and fraudulent messages from known sources.

12. **Denying benefits**. This technique is similar to reducing temptation. A typical example is the attachment of a PIN to car radios rendering them useless if stolen, unless the PIN is entered. The obvious technique to achieve this on the Internet is to encrypt all databases and messages so that, if stolen, they are rendered useless.

**Merchant**: Encrypt valuable databases and use encryption technology to secure all transmissions.

**Customer**: The obvious benefit to the fraudster is to obtain money from the victim. At least the potential victim can minimize his or her loss by never paying for anything bought on the Internet with cash, thus eliminating the immediate benefit to the fraudster. As already noted, payment by credit card is much more secure. As well, a cardholder’s liability for loss from fraud on a credit card payment is limited to around $50, and many credit card companies do not even charge the user that. While this does not exactly deny the fraudster the benefit, it certainly does delay it, and also offers the greater chance that information regarding the fraudster may be collected, and thus make tracking him down slightly easier. Utilization of a trusted third party to pay for auction items also ensures that the intended fraudster has to produce the goods first, before receiving payment, which also makes clear that he cannot enjoy the benefits unless he fulfills his part of the contract. Thus, it denies the fraudster the benefit of getting something for nothing.

**Law enforcement**: work closely with etailers and auction sites to prosecute all attempts at fraud, and publicize the actions taken.

**Legislatures**: Pass laws that require interception of cross border transactions concerned with grey market products such as pornography, gambling, drugs and investment services. While this idea goes against the popular belief that the Internet recognizes no national borders, recent events suggest that this may be changing. *176

*175 link no longer valid

**Removing excuses**

13. **Rule setting**. If there are no clear, unambiguous standards, rules and procedures, such as for the handling of cash or electronic transactions, or if the rules are unclear or not visibly enforced, individuals will take advantage of the ambiguities. The Internet culture would prefer no rules - paradoxically, considering that computer languages tolerate absolutely no deviation from their grammatical structure. In etailing there is of course the necessity for procedures for implementing secure transactions, and these are quite similar to those that are used in the offline world of retailing. The steps and procedures necessary for secure transactions have already been outlined. However, there are areas of great ambiguity on the Internet where there is no clear way to apply rules or set clear standards. The first of these areas is that of cross-border commerce where the laws of different countries (and in the U.S. different laws of each state) compete for status, and even agencies of enforcement compete with each other for jurisdiction. The second area is the commerce in grey market products and services such as prescription drugs, gambling, and certain tax avoidance schemes in investment services. The application of laws and regulations is often unclear, and also varies from jurisdiction to jurisdiction. The third area concerns intellectual property and the application of copyright law, which, although frequently revisited by legislatures, remains very different from country to country.

**Merchant**: Publish a clear security policy and specific security procedures to be followed by all employees. Adopt secure transaction
online protocol.

**Customer:** Follow customer guidelines for online purchases.

**Law Enforcement:** Disseminate clear and consistent applications of relevant laws and regulations concerning online grey commerce.

**Legislature:** Pass laws establishing security standards for ecommerce.

**International bodies:** Develop international agreements for consistent application of copyright law, grey market commerce and cross-border crime. *177

**Trade Associations:** Publish best practice guides and promote security on web sites.

**Colleges:** Develop a computer use rights and responsibilities policy and educate all users. Require all users to indicate agreement with the policy.


**14. Stimulating conscience and disarming disinhibitors.** This technique combines the 14th and 15th of Clarke’s original techniques. Clarke is not referring to the “general sense of guilt” that individuals may feel when they do something wrong, a sense that derives from a multiplicity of society’s socialization processes. Rather, he is concerned to link conscience to a specific act. The idea of this technique is to stimulate conscience at the specific point at which the offender may be contemplating action. For example, the common sign “shoplifting is stealing” serves to prick the conscience of would-be shoplifters. The main disinhibitors identified by Clarke are drugs and alcohol that remove an individual’s normal inhibitions. However, the battle on the Internet is the battle for conscience that has been “neutralized” by the culture of the Internet. It is the culture of the Internet that acts as the disinhibitor to committing computer crime. The potential offender has to be reminded that the Internet value that “everything should be free” does not make everything free, and to treat others’ property as one’s own is wrong. Nor does it justify damaging information systems since innocent people suffer. Obviously a lot of customer and student education is needed to counteract the hacker’s ethic. It may be that, as commerce gradually takes over the Internet, new generations of computer users will come to see that the Internet cannot be, and perhaps should not be free to all. Campaigns and posters (hard copy and electronic) that display these messages are recommended.

**Merchant:** Customer education. "Copying software is stealing".

**Customers:** Decline to make copies of software for friends or family

**Trade associations:** Campaign against Internet culture, e.g., "Hackers are vandals", "Authors deserve remuneration for their work", "Copying software is punishable by prison".

**Colleges:** "Hackers cause serious personal and financial damage". "Hackers are criminals". "Hacking violates innocent victims". "Hackers violate privacy rights". Also, require all users to acknowledge a responsible use agreement.

**15. Assigning responsibility.** The relationship between law and the Internet is opaque. This is largely because the Internet is popularly thought of as a kind of frontier, something like the mythical Wild West. This idea in turn derives from the Internet’s highly decentralized architecture that is pictured as “anti-law” because there is no central authority that “runs” the network. *178 The next step in this argument, which is questionable, is to argue that it is therefore not possible to assign responsibility to any particular individual or organization for bad things that happen. It is the picture of "every man for himself", a kind of cooperative anarchy. While it may be true that there is no single authority that “runs” the Internet, it is also certainly true that one could direct an attack at certain features of the Internet and almost bring it down - as some hackers have done. However, it is also necessary to recognize that there are very clear rules about how the network operates: rules about the structure of messages (how they are moved from one place to another, how Internet addresses are assigned, how files are recognized) and strict procedures that must be followed in order for individuals to log on to the network. So, lying beneath the apparent chaos of millions of people connected together through different devices and different operating systems, there is a "backbone" of strict rules that keeps the Internet running. Attacks that violate these rules - and most unauthorized intrusions certainly do that - should therefore be viewed harshly, and assigned full individual responsibility for these acts. So also should those organizations be held responsible, which allow hackers to operate through their services. Finally, organizations that allow criminal activity to exploit their otherwise legal services should be held responsible for doing so.

**Merchants:** Penalize customers for breaches of security.
Legislatures and Regulatory Agencies: Hold auction web sites responsible for illegal sales. Hold Internet service providers (ISP) responsible for fraudulent web sites and hold college campuses responsible for hackers who obtain unauthorized entry into other systems by exploiting the college computing system.

Customers: Insist that merchants acknowledge security errors; report fraudulent activity.

Colleges and ISPs: Remove user rights if rules of use are not followed.

*178 This belief that "nobody runs the network" is probably right. The organization that comes closest to "running" the Internet is the Internet Corporation for Assigned Names and Numbers (ICANN). This is the organization left over from the original organization that first started the Internet, financed by the U.S. government. The funding future of this organization is currently uncertain. See: http://www.icann.org. Abolishing the organization, however, would not terminate the Internet. It would probably go unnoticed. However, it does set certain rules, especially address protocols.

16. Facilitating compliance

Merchant: Devise easy backup and restoration for customers’ software. Make sure transactions are convenient and easy to use. Provide ample information to customers about security procedures and provide other information that authenticates the company’s identity and status in the business world.

Trade Associations: Publish names and other information of trusted and authentic online merchants and professionals (e.g., pharmacies, investment services). Provide web sites and links to organizations that publish and rate the online businesses. Provide information and links to organizations that survey the web for fraudulent web sites and other aspects of online fraud.

Peer-to-peer: Provide a legal service for a small fee negotiated with the music and video industry.

Regulatory agencies: Work in partnership with trade associations to identify fraud; develop best practices.

Table 6: Opportunity-reducing techniques in the etailing environment

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Merchant</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- secure physical location</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- firewalls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Software and Network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>companies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- design security into</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>operating languages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Customer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- keep computing devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>in physically secure place</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- avoid using in crowded</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>place (cell phones, PDA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- install software firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Merchant</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- passwords and PINs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- differentiated access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- refuse sellers with</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>suspect transaction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>record (auctions)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Customer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- store passwords in</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>secure places</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- do not open</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>suspicious email or files</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- only give credit card</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>information on</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>secure etailing site</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- always query requests</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for personal information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Merchant</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- check attributes of</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>critical files</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- use public-key</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cryptography and other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>digital identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>methods to verify files</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Customer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- keep records of all</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>transactions with</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>etailingers,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law enforcement and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>legislatures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- allow high level of</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cryptography to be used</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>internationally</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Merchant</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- install latest technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to establish</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- require PINs to be used</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>in with credit cards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- install biometric</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- accept only credit card</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>payments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Software manufacturers</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- control release of</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>information pointing to</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;bugs&quot; or &quot;holes&quot; in</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>operating programs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Customer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- do not use public</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>computers (libraries,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet cafes) to</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>purchase online</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- auctions: no cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>payments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- check out authenticity of</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>web sites when purchasing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>grey market products</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law enforcement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- control deception and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>false advertising</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Increasing perceived risks

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Merchant:</strong></td>
<td><strong>Merchant:</strong></td>
<td><strong>Merchant:</strong></td>
<td><strong>Merchant:</strong></td>
</tr>
<tr>
<td>• establish audit trails</td>
<td>• Publicize strong security surveillance.</td>
<td>• Include regular employees in security team.</td>
<td>• Auction sites establish community watch sites</td>
</tr>
<tr>
<td>• Analyze user patterns to detect deviant use</td>
<td>• Assess when surveillance of computing environment may be most needed.</td>
<td>• Train all employees in correct security procedures</td>
<td>• Supervise customer feedback files</td>
</tr>
<tr>
<td>• check for &quot;sniffers&quot; and remove.</td>
<td>• Customer:</td>
<td>• Offer incentives for employee vigilance</td>
<td>• Monitor for illegal sales</td>
</tr>
<tr>
<td>• encrypt all transmissions.</td>
<td>• Supervise others who use the computer</td>
<td>• Use customer service to educate consumers</td>
<td>• Customer:</td>
</tr>
<tr>
<td>• Check for rogue files</td>
<td><strong>Law enforcement Agencies:</strong></td>
<td>• Report suspicious emails and requests for information to Internet Service Provider (ISP).</td>
<td>• Participate in community watch on auctions;</td>
</tr>
<tr>
<td>• minimize “cookies.”</td>
<td>• Maintain hidden presence on news groups and bulletin boards</td>
<td><strong>Law Enforcement:</strong></td>
<td>• provide customer feedback on transactions.</td>
</tr>
<tr>
<td>• Make public announcements of fraud investigations.</td>
<td></td>
<td>• Utilize natural surveillance for undercover operations.</td>
<td></td>
</tr>
</tbody>
</table>

### Reducing anticipated rewards

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Merchant:</strong></td>
<td><strong>Merchant:</strong></td>
<td><strong>Merchant:</strong></td>
<td><strong>Merchant:</strong></td>
</tr>
<tr>
<td>• valuable databases offline</td>
<td>• digital signatures and certificates</td>
<td>• Repair system damage immediately.</td>
<td>• Encrypt valuable databases.</td>
</tr>
<tr>
<td>• no dial up access.</td>
<td>• Copyright web pages.</td>
<td>• Quietly announce security measures in force.</td>
<td><strong>Customer:</strong></td>
</tr>
<tr>
<td>• refuse auction of stolen, counterfeit or unethical items.</td>
<td>• Customer:</td>
<td>• Resist the temptation to become a victim.</td>
<td>• Never pay with cash.</td>
</tr>
<tr>
<td><strong>Customer:</strong></td>
<td>• Only shop on e-tailing sites that digitally encrypt transactions.</td>
<td><strong>Legislature:</strong></td>
<td>• Use trusted third party for auction payments.</td>
</tr>
<tr>
<td>• Do not store valuable passwords and other information on computer.</td>
<td>• Never enter personal information unless site has been thoroughly authenticated.</td>
<td>• Legislately appropriate severe punishments.</td>
<td><strong>Law enforcement:</strong></td>
</tr>
<tr>
<td>• Do not leave laptop, cell phone or PDA unattended.</td>
<td><strong>Trade Associations:</strong></td>
<td>• Regulate fraudulent advertising and scam web sites.</td>
<td>• work closely with e-tailers and auction sites to prosecute all attempts at fraud.</td>
</tr>
<tr>
<td></td>
<td>• campaign for use of smart cards</td>
<td><strong>Internet Service Providers and System administrators:</strong></td>
<td><strong>Legislatures:</strong></td>
</tr>
<tr>
<td></td>
<td>• Maintain vigilance for copyright violations.</td>
<td>• Adopt filtering software</td>
<td>• Pass laws requiring interception of cross border transactions in grey market products.</td>
</tr>
</tbody>
</table>
This review began by outlining the broad crime-inducing features of the information society, and followed by analysing the detailed transactions that occur in the etailing environment so that points of vulnerability could be identified. This is the approach that is most suited to a situational prevention perspective. It is now appropriate to turn to a broader consideration of the policy issues emerging from this analysis. In fact, there is just one major issue that emerges from this analysis, and that is identity. Within the context of the present paper, this translates into two perplexing problems: (1) the authentication of identity which presents itself mainly to merchants and other officials who need to be assured that their customers are who they say they are, and (2) the protection of consumers’ privacy, since it is impossible to verify one’s identity without obtaining very private information about his or her personal history.

Identity theft appears in Table 1a as a crime of the computing environment. Of course, impersonations and deceptions that are used in traditional frauds and con games have existed long before the information society and the computing environment. However it has been argued that the SCAREM attributes of the information systems of the computing environment throw the whole idea of identity into a quagmire. The Internet allows for - even fosters - deceptions, anonymity, aliases and “virtual identities”. At the same time etailing merchants must try to verify the identities of customers who make purchases from them when they pay by credit card. Furthermore, there is the additional problem of establishing the identities of documents, which can also be changed at various points along the way of an etailing transaction. It is not surprising therefore that the opportunity-reducing techniques of Access Control and Identifying Property receive more extensive coverage than the other techniques. But the problem has much broader implications.

It has been noted that credit card fraud has been reduced considerably in the U.K. by the adoption of several situational preventive techniques, among them improved technology in making the cards, including requiring a PIN number of the user, and the utilization of large databases against which a card can be checked for either fraud or use that deviates from the cardholder’s established pattern of use. However, it is also apparent that there is a good possibility that criminals will shift their attention to other places in the etailing transaction where there may be more value and more vulnerability. Thus, if the card itself cannot be counterfeited easily, a better solution is to assume the identity of the user. Thus etailers’ valuable databases of credit card and other personal information become the target. The Foresight study by Jones and Levi showed that there has been a dramatic increase in recent years in identity theft in the U.K. *179 And in the U.S. it was estimated that there were between 500,000 and 700,000 cases of identity theft in the first six months of 2000. *180 The problem was considered sufficiently severe in the U.S. that President Clinton signed into law the Identity Theft and Assumption Deterrence Act *181 on October 30, 1998. *182
It may seem strange to begin a discussion of such a broad issue of identity in the information society by recounting the criminal aspects of identity theft and acquisition. But it is criminal activity that exploits society's traditions of identity creation and preservation that exposes the significance of this issue. The extensive reports and legislative work conducted concerning privacy have been more often than not motivated by spectacular criminal cases, *183 and spawned a number of interest groups *184 and government agencies that campaign for online privacy rights, such as the Privacy Rights Clearinghouse. *185

Jones and Levi *186 list several reasons for identity change or acquisition:

1. Theft and deception in acquisitive crimes
2. Hiding of unattractive antecedents - crimes and civil embarrassments - bankruptcy.
3. Obtaining information about another for use in blackmail, court proceedings, or press revelations
4. Citizenship and ability to unlawfully remain in the country
5. Legitimate victim and witness protection from violent and determined offenders
6. Legitimate changes of forename following gender re-assignment or change of surname that through the development of slang terms that are unattractive and embarrassing.

The fourth reason for identity acquisition listed above, the issue of citizenship and unlawfully remaining in a country is especially significant for this discussion. After the September 11 terrorist attack on the World Trade Centre, a number of the attackers were found to be travelling with fake passports, and others had obtained drivers' licenses under false pretences. When it became apparent that there were Al-Qaeda cells throughout the U.S. and other countries, the immediate question that arose was, how is this possible? Why can't we identify people more carefully? Why are such people allowed to enter the country and why are they allowed to stay there, unidentified? When the idea of a national identity card was raised, as it has from time to time in the history of both the USA and the U.K. it was briefly debated, but quickly fell from public view. This is of particular interest when one considers that proving one’s identity is so endemic to managing one’s life in modern society. In the United States, drivers' licenses are the surrogate "national ID card" although these are issued by each state. While they now mostly all have picture IDs, it is well known that obtaining fake licenses is not difficult, and also that pictures are generally a poor form of identification. *187

National ID cards are common in European and Asian countries, but there seems to be a visceral opposition to them in the USA and the U.K. The arguments against this idea revolve around the notion of the "free society", (and arguably the Internet is its extreme form), which recognizes the right of people to move about freely without interference and live their lives without the intrusion of outsiders - especially the government. *188 This belief has also been the foundation for the attack on the government's claim on cryptography, a claim that assumes the right of the government, in the last resort, to have the right to snoop on an individual's Internet transactions. It is significant to note that the US Congress considerably loosened the wiretap laws in its antiterrorism legislation passed in the aftermath of the September 11 attack.

Will the information society create the impetus for something like a national ID card? Technology may be creating the groundwork for something similar, though it is impossible to predict just exactly what form this will take. The transformation of credit cards into smart cards in the U.K. is a small but very significant beginning to nailing down an individual's ID on a card. The increasingly widespread introduction of digital certificates and signatures also puts a premium on being able to claim authentication of one's transaction, and with increasing technological progress, the possibility of also being able to attach this authentication process on to a smart card. These cards may be initially introduced only in the field of e-tailing, and e-commerce generally. The present analysis of the e-tailing environment suggests that these forms of authentication are essential to reliable and successful e-tailing transactions. And if the public continues to use the Internet to do more and more of its daily business, then these authentication procedures will become more and more common, and more and more accepted. How many passwords and user IDs do ordinary people have these days compared to just twenty years ago? Identifying ourselves has already become "an integral part of everyday life".*189

The problem that faces us, therefore, is not so much that a National ID card may emerge from these significant changes, but that the ability to verify one's identity will increasingly be attached to those with the means and education to conduct their business using the facilities and convenience offered by the information society. These conveniences are not confined to desk top computers any more, but to telephones and PDAs, devices of mass communication such as television and radio, global positioning systems, and who knows what other devices that will emerge during this technological revolution. It is conceivable that consumers will be unable to exploit these services to the full without establishing their identities to the satisfaction of those who provide these services. And in most cases, those who provide these services will be (and are) private enterprises. Thus, if smart cards become widespread, they will most likely be dominated by a few major corporations, just as is the case with credit cards now. There are also companies that provide "premium" identification, such as Verisign, which guarantees the digital verification of many online transactions conducted on major e-tailing web sites. Thus, it is conceivable that individuals could pay to obtain premium identity smart cards, cards whose authentication is beyond reproach. In contrast, the homeless, or poorly educated and unemployed, or illegal aliens may, in the future, have no acceptable means of authenticating their identities.

---

*183 List several reasons for identity change or acquisition:

1. Theft and deception in acquisitive crimes
2. Hiding of unattractive antecedents - crimes and civil embarrassments - bankruptcy.
3. Obtaining information about another for use in blackmail, court proceedings, or press revelations
4. Citizenship and ability to unlawfully remain in the country
5. Legitimate victim and witness protection from violent and determined offenders
6. Legitimate changes of forename following gender re-assignment or change of surname that through the development of slang terms that are unattractive and embarrassing.

---

*184 The arguments against this idea revolve around the notion of the "free society", (and arguably the Internet is its extreme form), which recognizes the right of people to move about freely without interference and live their lives without the intrusion of outsiders - especially the government. *188 This belief has also been the foundation for the attack on the government's claim on cryptography, a claim that assumes the right of the government, in the last resort, to have the right to snoop on an individual's Internet transactions. It is significant to note that the US Congress considerably loosened the wiretap laws in its antiterrorism legislation passed in the aftermath of the September 11 attack.

---

*185 National ID cards are common in European and Asian countries, but there seems to be a visceral opposition to them in the USA and the U.K. The arguments against this idea revolve around the notion of the "free society", (and arguably the Internet is its extreme form), which recognizes the right of people to move about freely without interference and live their lives without the intrusion of outsiders - especially the government. *188 This belief has also been the foundation for the attack on the government's claim on cryptography, a claim that assumes the right of the government, in the last resort, to have the right to snoop on an individual's Internet transactions. It is significant to note that the US Congress considerably loosened the wiretap laws in its antiterrorism legislation passed in the aftermath of the September 11 attack.

---

*186 Will the information society create the impetus for something like a national ID card? Technology may be creating the groundwork for something similar, though it is impossible to predict just exactly what form this will take. The transformation of credit cards into smart cards in the U.K. is a small but very significant beginning to nailing down an individual's ID on a card. The increasingly widespread introduction of digital certificates and signatures also puts a premium on being able to claim authentication of one's transaction, and with increasing technological progress, the possibility of also being able to attach this authentication process on to a smart card. These cards may be initially introduced only in the field of e-tailing, and e-commerce generally. The present analysis of the e-tailing environment suggests that these forms of authentication are essential to reliable and successful e-tailing transactions. And if the public continues to use the Internet to do more and more of its daily business, then these authentication procedures will become more and more common, and more and more accepted. How many passwords and user IDs do ordinary people have these days compared to just twenty years ago? Identifying ourselves has already become "an integral part of everyday life".*189

---

*187 The problem that faces us, therefore, is not so much that a National ID card may emerge from these significant changes, but that the ability to verify one’s identity will increasingly be attached to those with the means and education to conduct their business using the facilities and convenience offered by the information society. These conveniences are not confined to desk top computers any more, but to telephones and PDAs, devices of mass communication such as television and radio, global positioning systems, and who knows what other devices that will emerge during this technological revolution. It is conceivable that consumers will be unable to exploit these services to the full without establishing their identities to the satisfaction of those who provide these services. And in most cases, those who provide these services will be (and are) private enterprises. Thus, if smart cards become widespread, they will most likely be dominated by a few major corporations, just as is the case with credit cards now. There are also companies that provide "premium" identification, such as Verisign, which guarantees the digital verification of many online transactions conducted on major e-tailing web sites. Thus, it is conceivable that individuals could pay to obtain premium identity smart cards, cards whose authentication is beyond reproach. In contrast, the homeless, or poorly educated and unemployed, or illegal aliens may, in the future, have no acceptable means of authenticating their identities.

---

*188 The fourth reason for identity acquisition listed above, the issue of citizenship and unlawfully remaining in a country is especially significant for this discussion. After the September 11 terrorist attack on the World Trade Centre, a number of the attackers were found to be travelling with fake passports, and others had obtained drivers' licenses under false pretences. When it became apparent that there were Al-Qaeda cells throughout the U.S. and other countries, the immediate question that arose was, how is this possible? Why can't we identify people more carefully? Why are such people allowed to enter the country and why are they allowed to stay there, unidentified? When the idea of a national identity card was raised, as it has from time to time in the history of both the USA and the U.K. it was briefly debated, but quickly fell from public view. This is of particular interest when one considers that proving one’s identity is so endemic to managing one’s life in modern society. In the United States, drivers' licenses are the surrogate "national ID card" although these are issued by each state. While they now mostly all have picture IDs, it is well known that obtaining fake licenses is not difficult, and also that pictures are generally a poor form of identification. *187

---

*189 The problem that faces us, therefore, is not so much that a National ID card may emerge from these significant changes, but that the ability to verify one’s identity will increasingly be attached to those with the means and education to conduct their business using the facilities and convenience offered by the information society. These conveniences are not confined to desk top computers any more, but to telephones and PDAs, devices of mass communication such as television and radio, global positioning systems, and who knows what other devices that will emerge during this technological revolution. It is conceivable that consumers will be unable to exploit these services to the full without establishing their identities to the satisfaction of those who provide these services. And in most cases, those who provide these services will be (and are) private enterprises. Thus, if smart cards become widespread, they will most likely be dominated by a few major corporations, just as is the case with credit cards now. There are also companies that provide "premium" identification, such as Verisign, which guarantees the digital verification of many online transactions conducted on major e-tailing web sites. Thus, it is conceivable that individuals could pay to obtain premium identity smart cards, cards whose authentication is beyond reproach. In contrast, the homeless, or poorly educated and unemployed, or illegal aliens may, in the future, have no acceptable means of authenticating their identities.
One of the main arguments raised against National ID cards is that they are the "primary tool of totalitarian governments" to quote a former U.S. senator, Alan Cranston. He made this statement commenting on a proposed national database to be used for employment verification purposes. The idea of a National ID card, of course, presumes a national database that would contain the personal details of all individuals in the nation. In fact, what is emerging in the 21st century is the existence of multiple databases of personal information. There are web sites that specialize in providing a service of searching through multiple databases to find or discover the identities of missing persons. The "white pages" and "yellow pages" found on many web portals are simple versions of such databases. The US government already maintains many such databases for specific purposes: taxation, handgun licensing, legal residents, naturalized citizens, and social security to name but a few. So also does the U.K. with the notable addition of the national health card. If one adds to that the growing number of databases of personal and credit information such as those of etailers for credit and marketing information and those in the health field for medical services, the amount of information available on any single person in the information society is stunning, to say the least. Is it an advantage that his information is located in different places? This is difficult to evaluate. Having so many databases creates many attractive targets. On the other hand, if all the information about a single person were assembled together in one database, it would become indeed a critical target and a very powerful tool of government.

However, one may argue that identity verification does not have to depend on a database at all. The problem may be solved by smart cards. Here is how it could be done. Identity is composed of two attributes: what we are and who we are. What we are is determined by "accidents" of birth, that is, biology. Who we are is determined by life events. Until recently, all ways of authenticating identity drew upon who we are, not what we are. An exception to this observation is of course, fingerprint files. The recent development of DNA files has begun to add to the biological method of identification. Picture IDs are also attempts to use biological data of identification, though this is a very crude method compared with DNA and other new biometric methods of establishing identity such as voice patterns, retinal scans, hand scans, facial scans, iris scans and many others. These approaches only do half the job, though. They do establish that this is an individual who is unique in certain ways. They do not attach a name or other features to the person: This has to be done by using the person's life event history. These events come from basically four sources: public databases (records of birth, marriage, tax records etc.), commercial databases (energy or telephone bill, mortgage papers), professional and employment history (school or university, educational degrees), and family records (family referees, parents or guardians). A short list of documents deriving from these sources includes:

- Electoral register entries
- Mortgage account information
- Property ownership and leasehold
- Credit account and other financial facilities information
- Insurance policies
- Marriage and financial associations
- Previous addresses
- Telephone numbers - fixed and mobile
- Employment information from applications for financial services
- Library cards and other memberships
- Satisfied court judgments
- E-mail address
- Higher educational qualifications
- Forwarding addresses - re-directions
- Previous address linking
- Previous authentication events
● Payment systems facilities - debit/credit/cheque/charge cards, virtual wallets etc.

Thus, in order to obtain a new passport, for example, an individual would typically have to produce a selection of two or more of the above documents or sources of identity. It is also apparent that the older a person is, the more evidence there is to establish his or her identity. If this list were used to develop a national database that contained all or most of these sources of identity verification, this would be an extremely powerful database. Another possibility would be to construct a single database by linking the many existing databases together and developing a search engine that would pull out from each database the required information. Many of the search engines used on the Internet do something similar to this. There are services on the Internet that promise, with varying degrees of success, to do just that. And these are not government web sites, but private, or interest group web sites.

Large databases are not needed in order to process smart cards. This is because a large amount of individual information can be stored, certainly all the information listed above, and then some. It can also be categorized into different levels of security right there on the card, so that depending on the level of verification needed in a particular transaction, the appropriate level of identity authentication could be retrieved. There are already smart cards that have this capacity. Their great virtue is that they do not require a central database, or any database at all for their authentication, once the original authentication data have been entered. There is no need for the agent, say an immigration official checking a passport, to check with a database of passports. The information is right there on the card itself. And if the card also contains biological data that link the life event contents of the card to the cardholder, then there is a very good chance that this person is who he says he is. Of course, if there were a list of outlawed persons, the agent would have to consult it. But this would be a highly specialized list of suspects, not a broad list of the kind that the opponents of national ID cards envisage. The wide application of such super smart identification cards is probably a long way off. But if technology continues to force change at the rate it did during the 20th century, we may expect that it will come about. The fact that American Express has recently introduced its Private Payments system, which creates a one-time credit card number for every transaction, while keeping the customer’s account number private looks like a small step in this direction. *193

In any event, it can be seen that the issue of privacy in the 21st century becomes one of defence against intrusions not by governments, but by private enterprise. On the one hand, consumers, especially those plugged in to the information society, must give up their private and personal details to merchants and other credit assessing organizations in order to establish a valid commercial identity. Without this, they cannot exploit all the benefits that the online world has to offer. And one of those major benefits, if not the major benefit, is to be able to move freely about the open society - the real society and the virtual one. But against this giving up of personal identity, is the philosophical and historical notion of western thought, (probably deriving from the enlightenment thinkers of the 17th and 18th centuries of Europe and England) the idea of remaining free from external constraints of any kind, of being able to form and protect one’s own personal identity, especially to be able to keep it apart, unsullied by the demands of others, whether they be governments or private organizations.

In sum, what may be happening is that the vague and idealistic idea of personal or individual identity as propagated in western thought is being replaced by a new idea, that of one’s commercial identity. And this identity will be forged, not out of dealings with government as was the great concern of the 18th century enlightenment thinkers such as Rousseau and Montesquieu, but out of dealings with open markets, an idea almost realized by Adam Smith in the 17th century. This is clearly a highly sensitive point, one thatetailers have quickly recognized. Thus on all web sites of major tailers, there is a privacy statement, and many also guarantee additional options to preserve privacy, such as electing not to have one’s personal details shared with other merchants. It is not clear whether etailers have taken these protective steps in response to what they see as economic or business concerns, or whether in response to the pressure brought upon them by governments, especially those international organizations that have been quite forward in delivering directives.

*183 Rusch, Jonathan. The department of justice’s role in identity theft enforcement and prevention. Department of Justice.
*185 Privacy Rights Clearinghouse, http://privacyrights.org. This organization publishes many fact sheets on privacy rights and identity theft on the web. See also the Federal Trade Commission (FTC) Identity theft hotline and data clearinghouse. In the U.K. extensive advice to consumers concerning purchasing online and privacy rights is provided by the Office of Fair Trading at http://www.of.t.gov.uk.
*187 Ibid.
Legislation and regulation

The role for national governments in the information society is certainly complex. For example U.S. law does not view the right to privacy as a human right. Rather, it is treated as a property right. The U.S. Constitution is largely silent on the privacy issue, although the Supreme Court has managed to come up with some claims to the right to privacy in the fields of search and seizure and abortion.*194 The United States does not have one single piece of legislation that deals with the privacy online issue. Rather there are several different acts that concern different aspects of protection such as protection of financial data (Gramm-Leach-Bliley Act), health information (Health information portability and accountability act) and children’s information (Children’s online privacy protection act.). However, in the information society that embraces the world in its scope, national governments have difficulty in ignoring the directives and pressure issued not only by other governments, but also by international organizations of various kinds. For example, the European approach has been broader than the U.S. It restricts export of information about EU citizens to other countries that do not have the same standards of protection (such as the U.S.A.). In the European Safe Harbour Data-sharing agreement (November 1, 2001), the U.S. department of commerce agreed to the EU’s more stringent privacy requirements. This meant, among other things, that U.S. Internet companies could risk losing access to European clients if they broke the agreement.

This EU directive has been highly controversial, and its effect yet to be seen. Two thirds of the EU’s countries have enshrined its principles into their own law. *195 The principles of the EU directive are:

- **Notice**: Individuals must be told what the information collected from them is to be used for.
- **Choice**: Individuals must be given a clear choice of not allowing their personal information to be used by third parties.
- **Security**: Organizations must make every effort to safeguard the data.
- **Access**: Individuals must be able to access their own information and amend it as needed.

The OECD has also been very active in developing guidelines for consumer protection *196 and has campaigned to implement them in member countries. Table 7 lists a selection of the most active international organizations dealing with online etailing issues.

In general, the ITU and UNCITRAL *197 have concerned themselves with adapting existing policies to the online world. OECD, UNCTAD and the EU have concerned themselves with ecommerce issues, especially privacy and security. New groups such as ICANN and W3C are partnerships among government, companies and non-profit organisations. While many guidelines, rules, regulations, directions and reports have been produced by these organisations, it remains to be seen what actual effect these will have, and the question of enforcing these many rules remains. In general, it may also be said that the US in contrast with European countries adopts a market-oriented approach to regulation and control of privacy and identity issues, whereas European countries depend more heavily on government intervention or influence. *198 Table 7 suggests that education of the public is a major concern of most organizations, and this is an issue that is also in the forefront of all major etailing web sites. The question therefore is whether or to what extent governments should take on responsibility for educating consumers concerning the many issues raised in this paper, or allow market forces - consumer demands, the processes of civil and criminal law, the innovations in technology and information systems - to find the right balance between protection of individual rights and the satisfaction of individual wants.


Table 7: International organizations addressing etailing issues

<table>
<thead>
<tr>
<th>Digital signatures</th>
<th>Standards</th>
<th>Security</th>
<th>Privacy</th>
<th>Consumer protection</th>
<th>Education</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>International Telecommunications Union (ITU)</td>
<td>a</td>
</tr>
<tr>
<td>UN Commission on International Trade and Law (UNCITRAL)</td>
<td>a</td>
</tr>
<tr>
<td>UN Conference on Trade &amp; Development (UNCTAD)</td>
<td>a</td>
</tr>
<tr>
<td>UN Educational, Scientific and Cultural organization (UNESCO)</td>
<td>a</td>
</tr>
<tr>
<td>World Bank</td>
<td>a</td>
</tr>
<tr>
<td>Organisation for Economic Cooperation and Development (OECD)</td>
<td>a</td>
</tr>
<tr>
<td>Free Trade Area of the Americas (FTAA)</td>
<td>a</td>
</tr>
<tr>
<td>European Union (EU)</td>
<td>a</td>
</tr>
<tr>
<td>Internet Corporation for Assigned Names and Numbers (ICANN)</td>
<td>a</td>
</tr>
<tr>
<td>World Wide Web Consortium (W3C)</td>
<td>a</td>
</tr>
<tr>
<td>Internet Engineering Task Force (IETF)</td>
<td>a</td>
</tr>
</tbody>
</table>
Yet new, marked, or consecutively numbered bank notes reduce the opportunity for theft. The VIVA model stated earlier offers a starting point for evaluating which things make better crime targets. For example, videocassette players have made good targets because they are high in value and low in inertia, that is, they have high. In addition, businesses would be encouraged to make detailed studies of their losses so as to focus improved security on high risk items rather than to disperse it across all product lines without much benefit. Research on hot products will also assist police efforts to undermine fencing operations. Opportunities, precipitators, and criminal decisions: A reply to Wortley’s critique of situational crime prevention. In M. J. Smith & D. B. Cornish (Guest Eds.), Theory for practice in situational crime. Transforming piecemeal social engineering into a grand crime prevention policy: Toward a new criminology of social control. Journal of Criminal Law and Criminology, 105(1), 209–238.