

Protecting Consumers from Cyberfraud

What are the most common types of cyberfraud?

How does fraud affect the digital marketplace?

What preventive measures are needed?

What role do enforcement and redress play?

What more needs to be done?

For further information

For further reading

Where to contact us?

Introduction

The Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping. Ever faster and more accessible connections available on a wider range of platforms, such as mobile phones or person to person portable devices, have spurred new e-commerce opportunities. Online shopping and banking are increasingly widespread and over the next 10 years, the Net is expected to become as common as gas or electricity. Google's "Internet Chief Evangelist" Vinton Cerf, has predicted that by 2016, *"everything from the family fridge to the office coffee pot ... heating, cooling, and security systems ... will be managed through the Internet; ... by then, the Internet will become so pervasive that connecting to it will no longer be a conscious act."*

Will this prediction come true? And will consumers take full advantage of it? OECD ministers discussing the fledgling phenomenon of e-commerce in 1998 saw the huge potential of the business-to-consumer online marketplace. But they also recognised the threat that fraud would undermine consumer confidence. The following year, the OECD adopted E-Commerce Guidelines to foster fair commercial practices on line. But as the online marketplace grew, so did awareness that crooks could use cyberspace to dodge the law by locating in one country and targeting consumers in another. To address this, in 2003 the OECD issued guidelines for international co-operation among consumer protection authorities.

Today, the Internet offers consumers worldwide more choice and easier ways to purchase goods and services, but the electronic marketplace has still not realised its full potential. One reason frequently given is consumer concern about fraud. This Policy Brief looks at the various forms of cyberfraud, assesses their impact on the digital economy and examines what governments can do now and in the future to address the problem. ■

What are the most common types of cyberfraud?

A wide variety of scams operate in the online environment, ranging from fraudulent lottery schemes, travel and credit-related ploys, modem and web page hijacking, and identity theft (ID theft) to name but a few. Many of these scams, such as pyramid selling, are simply online variants of fraudulent practices that have long existed offline. However, the Internet has given criminals access to a worldwide base of consumer targets as well as more opportunities to elude enforcement as they need not be in the same country, or even in the same hemisphere, as their victims.

The Internet allows fraudsters to masquerade as legitimate traders behind professional-looking websites or on virtual auction sites to advertise “free” or “bargain” prices, “miracle” products, and “exciting” investment and business opportunities. These deceptive and misleading offers trick unsuspecting consumers into buying goods and services on line which turn out to be far less than promised or even non-existent.

Many online scams originate in spam messages – usually through e-mail, but sometimes through text messages (SMS), voice messages delivered by Internet (Voice-over Internet Protocol or – VoIP) or other electronic channels. When the OECD set up a Task Force to deal with the scourge of spam in 2004, the problem was essentially one of unwanted and annoying advertising that blocked up e-mail inboxes. By the time the Task Force finished its work two years later, spam had evolved into a vehicle for the spread of fraud and other online abuses.

Many e-mail users will have received a message from a person claiming to be a government official or member of the royal family of a foreign country (usually in Africa), promising substantial sums of money in return for assistance in transferring money out of the country. Commonly known as the “Nigerian”, “West African” or “419” scam, once it has sucked in victims it convinces them to make small advance payments for various reasons, such as banking transaction fees. Needless to say, the victim never receives the promised substantial sums in return. Many pyramid and work-at-home schemes are also distributed through spam and follow the “advance fee fraud” format of requiring up-front payment or investment on the promise of high returns that are never forthcoming.

As consumers have become more skilled at detecting and avoiding scams, fraudsters have responded with more imaginative and worrying attacks relying on smart social engineering methods and sophisticated technology. Innovative attacks aim to steal an individual’s identity, (name, national identity numbers and other information such as credit card numbers) in order to commit fraud or other crimes. Again, spam is a key tool for the spread of ID theft, luring people into disclosing sensitive information such as credit card numbers or passwords. For example, *phishing* spams falsely claim to come from legitimate and well-known financial institutions or merchants. They ask recipients to click through on hyperlinks in order to verify or update their online accounts (see example below). These hyperlinks direct users to fake “look alike” websites where users are tricked into divulging personal information which can be used to access and illegally transfer money out of

the victim's bank account(s), open new bank or credit card accounts in the victim's name, make unlawful online purchases, etc.

These attacks are continually becoming more sophisticated. The past year has seen the growth of a new practice known as *spear-phishing* where accurate information about the recipient, such as the full name and home address, is included in the phishing e-mail making it even more convincing. Another new phenomenon known as *vishing* tricks people into making phone calls rather than clicking on links to websites. The number given is to a VoIP phone which records digits (such as account numbers) entered into the telephone, again enabling crooks to steal and use the information.

Other variants of fraud rely on the use of identity stolen through technological methods. For example, *pharming* interferes with the domain name system (DNS) look up process and redirects users attempting to reach a particular website to a "spoofed" one where they divulge personal information to the crooks. *Malware* (or malicious software), can be downloaded unwittingly by consumers from spam attachments or as they surf on line. Such malicious code, which increasingly targets mobile phones and other portable devices in addition to computers, can install "key stroke" loggers and other programs to steal information stored on, entered into, or received by these devices. The information collected through these kinds of technological attacks, such as passwords and other sensitive data, can then be used to perpetrate fraud.

A common misperception is that only naïve consumers fall victim to cyberfraud. However the growing sophistication of online crooks means that even the most Net-savvy can be caught out. As a 2005 OECD report concluded "being fooled by a scam is not a reflection of the education, age, or background of a victim". ■

Figure 1.
HYPOTHETICAL EXAMPLE
OF PHISHING E-MAIL
TARGETING CUSTOMERS
OF A FICTIONAL BANK
(Designed by OECD)

From: YourBank's Security Department <security@yourbank.com>
Sent: 19 September, 2006 5:13 PM
To: Recipient
Subject: Verify your account information

YourBank

Dear customer,

As part of our routine security monitoring, we noticed multiple suspicious attempts to log into your account. As a preventative measure, we have temporarily suspended access to your online banking services. In order to regain access to these services, please click the link below and complete all steps to verify your account information.

[Your account information](#)

Protecting the security of your account is YourBank's primary concern. Thank you for your prompt attention to this matter.

Please do not respond to this message. Mail sent to this account cannot be answered. For assistance, please log into your account and chose the "Help" link in the header of any page.

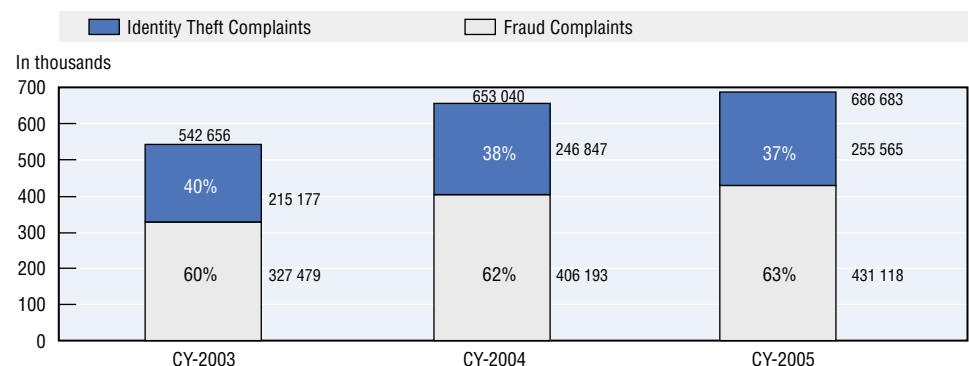
How does fraud affect the digital marketplace?

Judging by the continuing increase in consumer complaints, cross-border fraud would certainly appear to be on the rise. A report by the European Consumer Centre Network in 2006 shows that E-Commerce complaints, including fraud, more than doubled between 2004 and 2005. Similarly, a 2006 report from the US Federal Trade Commission (FTC) shows that cross-border fraud complaints jumped from 16% of all complaints in 2004 to 20% of all complaints in 2005. Among the 685 000 complaints received in 2005, 63% represented fraud and 37% were ID theft complaints.

This explosion of consumer fraud could help explain why business-to-consumer online transactions continue to lag so far behind business-to-business ones. The European Information Technology Observatory reported in 2004 that practically 90% of the e-commerce market consisted of business-to-business transactions, and little has changed since then.

Recent estimates show that phishing and other Internet fraud costs US consumers USD1.2 billion annually, while in Germany, official figures show consumer losses of more than EUR4.5 million – and that figure only covers cases reported to and investigated by the police. Moreover, a 2006 survey published by the US Better Business Bureau points out that the amount of time victims of ID fraud have to spend resolving their cases increased from 33 hours in 2003 to 40 hours in 2006. The resulting risk is that consumers may start spending less on online purchases to avoid not only the financial cost of cyberfraud but also the time lost in putting things right. Business also suffers considerable loss from fraud, including lost productivity and direct costs of setting up of technical support and software solutions to counter it (e.g. through filters). Payment card companies have policies in place (either voluntarily or by regulation) to limit consumer liability and cover most of their losses from unauthorised withdrawals. In the United Kingdom, the Association for Payment Clearing Services reported that banks' losses from Internet banking fraud more than trebled to GBP14.5 million for the six months to June 2005. According to the Annual Fraud Report from CyberSource, a worldwide provider of secure electronic payment, credit card fraud management, and verification software, e-commerce merchants were expected to lose as much as USD2.8 billion to payment fraud in 2005, representing an 8% increase over the year before. ■

Figure 2. ID THEFT AND FRAUD COMPLAINTS BY CALENDAR YEAR



Source: US FTC, 2006 Report on ID Theft and Fraud Complaints Data.

What preventive measures are needed?

The first line of defence to prevent online consumers from becoming online victims is good education. Tips on the major forms of Internet fraud and how to combat them have been developed by public authorities, enforcement agencies, and the private sector on various platforms such as government websites, brochures, posters, videos, reports, etc. The International Consumer Protection and Enforcement Network (ICPEN), an informal network of enforcement authorities from OECD and other countries, has launched *Fraud Prevention Month*, an awareness campaign taking place on a designated month every year. As part of the campaign members organise activities to educate consumers on how to recognise, report and stop fraud. In 2006, 25 ICPEN members participated in the event. Similarly, through the London Action Plan, 34 agencies and 24 private sector representatives from over 24 countries explore education strategies to combat spam.

The private sector also offers a number of technical tools to provide consumers with real-time protection against cyberfraud. For example, business has developed means to counter spam messages, which are a significant source of fraud, through authentication, filters, and listings. Likewise, anti-phishing systems have been put in place allowing Internet users to report phishing sites and block them.

However, little has been done so far to measure the impact of these initiatives on consumer behaviour in the e-market. Only a few studies have identified the extent to which consumers actually process the information and make use of the tools provided to them to avoid online fraud. And the results can be surprising. A 2005 survey conducted by the Momentum Research Group in the United States, France, the United Kingdom, and Germany, for example, found that European consumers were less aware of ID theft than those in the United States. The survey notes that while nine out of ten US consumers are conscious of the danger of ID theft, one in three consumers are still unfamiliar with the concept in France and Germany. Although this estimate helps identify the scale of the problem, more data should be collected to understand why such a discrepancy occurs and how to solve it. ■

What role do enforcement and redress play?

While prevention is crucial, strengthened international co-operation is also vital to detect and stop fraudulent activities on line. Since cyberspace does not respect national borders, law enforcement authorities need to work together to catch crooks on line. Following the recommendations in the 1999 E-Commerce Guidelines and the 2003 Cross-border Fraud Guidelines, OECD member countries have put in place more appropriate and adapted law enforcement frameworks both at domestic and international levels. A recent OECD report on the implementation of the 2003 Guidelines concludes that, to date, member countries have devoted considerable efforts to modernise their laws and enforcement co-operation schemes (see box below).

But if consumers are to gain confidence in the online marketplace, they also need to be able to obtain compensation from wrongdoers for the losses they have incurred. Depriving the wrongdoers of their ill-gotten gains in order to compensate their victims may also serve as a deterrent to future would-be fraudsters.

It is very difficult, however, for consumers to take private legal action to obtain redress in cases of cyberfraud. Firstly, consumers do not have the investigative and enforcement powers to identify the perpetrator and establish sufficient proof of wrongdoing. Secondly, the practical burden and financial costs of going to court often outweigh the loss that consumers have incurred. This is particularly true in cases of fraud originating in another country.

Consumer protection authorities, on the other hand, relying on their enforcement powers and international co-operation networks, are well placed to obtain compensation for consumers in fraud cases. At present there is still a sharp contrast between the abilities and experiences of consumer protection authorities in OECD countries in this respect. In some countries authorities have no powers at all to recover losses for consumers, whereas in other countries authorities may recover on behalf of both foreign and domestic consumers. Developing common policy principles in this area is a clear priority for future OECD action. ■

What more needs to be done?

Undoubtedly, significant progress has been achieved in building an effective strategy against cyberfraud – educational campaigns, technical prevention measures, and law enforcement capabilities and co-operation have all advanced. Nonetheless, key elements of this strategy need further development in order to stem the tide of ever-increasing incidences and costs of cyberfraud.

A simple first step would be to develop internationally comparable statistics on the volume of consumer complaints and monetary injuries from fraud. This would help measure the scale of current obstacles to the development of the business-to-consumer digital market and to establish priorities for enforcement. Currently, statistics-gathering and analysis vary greatly from country to country.

**Box.
MAIN IMPLEMENTATION
ACTIONS OF THE 2003
GUIDELINES ON
CROSS-BORDER FRAUD**

<p>Domestic modernisation</p>	<ul style="list-style-type: none"> • New enforcement authorities have been created. • Existing ones have been empowered with more authority to dissuade rogue traders from committing repeated wrongs. • Penalties against fraudsters have been significantly raised. • Public-private partnerships have helped catch infringers around the world.
<p>Enhanced international consumer protection enforcement co-operation</p>	<ul style="list-style-type: none"> • Notifications of illegal activities ongoing in one country. • Increased sharing of information on ongoing wrongs and fraudsters. • Assistance with investigations. • Landmark cross-border fraud cases.

Source: OECD.

Measuring the impact of consumer education would help improve methodologies for designing and running further campaigns. An analysis of the different kinds of initiatives conducted in member countries and their impact on consumer understanding and behaviour could provide a useful basis from which to derive best practices.

In some countries, legislative changes are still needed to enable authorities to successfully investigate and take enforcement action against fraud, particularly in the cross-border context. More generally, more resources and training should be allocated to alleviate some of the practical problems that authorities face in co-operative actions.

OECD member countries are committed to achieving further significant progress against cyberfraud to ensure that the risks lurking on the Internet do not outweigh its benefits for consumers, as well as for economic and social development as a whole. Plans are underway for a ministerial meeting on Internet-policy issues in 2008, 10 years after the OECD's last high-level meeting on this subject. The period leading up to the next ministerial provides the ideal opportunity to address outstanding gaps in the fight against fraud. ■

For further information

For more information on OECD's work on consumer fraud, please contact Brigitte Acoca, brigitte.acoca@oecd.org, Tel: +33 1 45 24 93 65 or Sarah Andrews, sarah.andrews@oecd.org, Tel: +33 1 45 24 90 05, or visit www.oecd.org/sti/consumer-policy.



For further reading

- OECD (2006), **Report on the Implementation of the 2003 Guidelines on Cross-border Fraud**, available at www.oecd.org/dataoecd/45/53/37125909.pdf.
- OECD (2006), **Anti-Spam Toolkit of Recommended Policies and Measures**, available at www.oecd.org/dataoecd/63/28/36494147.pdf.
- OECD (2005), **Report on Consumer Information Campaigns Concerning Scams**, available at [www.ois.oecd.org/olis/2005doc.nsf/linkto/dsti-cp\(2005\)12-final](http://www.ois.oecd.org/olis/2005doc.nsf/linkto/dsti-cp(2005)12-final).
- OECD (2005), **Report on Consumer Dispute Resolution and Redress in the Global Marketplace**, available at www.oecd.org/dataoecd/26/61/36456184.pdf.
- OECD (2003), **Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practice across Borders**, available at www.oecd.org/sti/crossborderfraud.
- OECD (1999), **Guidelines for Consumer Protection in the Context of Electronic Commerce**, available at www.oecd.org/sti/consumer-policy.

OECD publications can be purchased from our online bookshop:

www.oecd.org/bookshop

OECD publications and statistical databases are also available via our online library:

www.SourceOECD.org

Where to contact us?

OECD HEADQUARTERS

2, rue André-Pascal
75775 PARIS Cedex 16
Tel.: (33) 01 45 24 81 67
Fax: (33) 01 45 24 19 50
E-mail: sales@oecd.org
Internet: www.oecd.org

GERMANY

OECD Berlin Centre
Schumannstrasse 10
D-10117 BERLIN
Tel.: (49-30) 288 8353
Fax: (49-30) 288 83545
E-mail:
berlin.contact@oecd.org
Internet:
www.oecd.org/deutschland

JAPAN

OECD Tokyo Centre
Nippon Press Center Bldg
2-2-1 Uchisaiwaicho,
Chiyoda-ku
TOKYO 100-0011
Tel.: (81-3) 5532 0021
Fax: (81-3) 5532 0035
E-mail: center@oecdtokyo.org
Internet: www.oecdtokyo.org

MEXICO

OECD Mexico Centre
Av. Presidente Mazaryk 526
Colonia: Polanco
C.P. 11560 MEXICO, D.F.
Tel.: (00.52.55) 9138 6233
Fax: (00.52.55) 5280 0480
E-mail:
mexico.contact@oecd.org
Internet:
www.oecd.org/centrodemexico

UNITED STATES

OECD Washington Center
2001 L Street N.W., Suite 650
WASHINGTON DC. 20036-4922
Tel.: (1-202) 785 6323
Fax: (1-202) 785 0350
E-mail:
washington.contact@oecd.org
Internet: www.oecdwash.org
Toll free: (1-800) 456 6323

The OECD Policy Briefs are prepared by the Public Affairs Division, Public Affairs and Communications Directorate. They are published under the responsibility of the Secretary-General.