



FRAUD IN CROSS-BORDER E-COMMERCE

Contents

| | |
|---|-----------|
| FOREWORD | 3 |
| SCOPE | 4 |
| INTRODUCTION | 5 |
| MOST COMMON FRAUDS | 6 |
| EMERGING ISSUES IN ONLINE FRAUD | 10 |
| TIPS & TRICKS TO AVOID BEING SCAMMED | 15 |
| GENERAL ONLINE SHOPPING CHECKLIST..... | 18 |
| RESPOND QUICKLY IF YOU ARE THE VICTIM OF FRAUD | 19 |
| LEGAL PROTECTION OF CONSUMERS | 19 |
| WHERE CAN CONSUMERS REPORT A SCAM? | 21 |
| THE EUROPEAN CYBERCRIME CENTRE (EC3)..... | 22 |
| CONCLUSIONS AND RECOMMENDATIONS | 23 |
| CONTACT DETAILS FOR ECCS | 25 |



FOREWORD

Fraud in cross-border e-commerce is a report prepared by the European Consumer Centres Network (ECC-Net) which looks at scams faced by consumers when shopping online. There are European Consumer Centres in 30 countries covering all of the Member States of the European Union, plus Iceland and Norway. European consumer centres are co-funded by the European Commission and national consumer authorities. The aim of the network is to increase consumer confidence in the European internal market by providing consumers with information on their rights under European consumer legislation, and by giving advice and assistance in the resolution of their individual cross-border complaints. ECC-Net cooperates in joint projects to investigate specific sectors where consumers experience particular difficulties.

Although EU legislation protects consumers when purchasing goods or services online, the number of consumers who experience online fraud is growing. What exactly is a fraud? Fraud is an intentional deception, done for personal gain or for the purposes of damaging another individual. Internet fraud refers to fraud that is committed with the help of the internet. This concerns fraud done via e-shopping but also through the use of internet services, such as chat-rooms, e-mails, message boards or even software to allegedly defraud victims or to otherwise take advantage of them. Fraud can be related to fake auctions, products that will intentionally not be delivered, credit and debit card fraud, check fraud, identity theft and phishing.

Many frauds that migrated to the Internet have existed in one form or another for years but are facilitated by the internet and can reach a huge number of consumers at the same time and across border. Technology also allows more and more advanced fraud techniques.

This report was led by ECC Lithuania, together with ECC Ireland, ECC Belgium and ECC Slovenia. These Centres have formed the working group for the project.

The views and interpretations reflected in this report are not those of the European Commission or the national funding bodies. They are solely those of the working group based on their conclusions and the data submitted to the working group by all project participants.

Miglė Akulevičienė, Jaunė Dalinkevičiūtė

ECC Lithuania

info@ecc.lt

Ann Neville, Caroline Curneen

ECC Ireland

Xavier Hopchet

ECC Belgium

Jana Huč Uršič

ECC Slovenia



SCOPE

The objective of this project is to highlight the problems and risks faced by consumers when shopping online and to provide them with tips and practical advice on how to avoid falling victim to scams. It is evident that the number of consumers making online purchases is growing steadily, with 45% of European consumers having bought over the Internet in the past year. According to industry estimates, Europe represents the largest B2C e-commerce market in the world, accounting for a 35.1% share of global B2C e-commerce.¹

E-commerce has many advantages: from which the most important are the global choice of goods and services, attractive prices that can be reached 24/7 even from your couch, with delivery at your door. It also has some disadvantages however; you cannot physically inspect the goods before buying them, you often do not know the websites and so do not know whether you can trust them, you usually have to pay before receiving the order and then wait for it to be delivered.

The project focuses on the issue of fraud in cross-border e-commerce. 12% of internet users across the EU have already experienced online fraud, and 8% have fallen victim to identity theft. The highest figures of internet users that say they have experienced online fraud are in Poland (18%), Hungary (17%), Malta (16%) and UK (16%), while respondents in Greece (3%), Slovenia (6%) and Spain (7%) are least likely to have experienced online fraud.² Therefore the main questions which are raised in the project are:

What is a scam?

How do scammers target consumers?

How to avoid fraud in cross-border e-commerce?

How to ensure the safety of e-purchases?

What are the most common frauds that consumers face?

How are consumers protected when engaging in e-commerce? Is this sufficient?

How could ECC-Net help improve consumer knowledge of scams?



¹ Source: The European B2C E-commerce report, Ecommerce Europe, May 2013, available at: http://www.retailexcellence.ie/images/uploads/downloads/members_resources/Europe_B2C_Ecommerce_Report_2013_-_August.pdf

² Source: Special Eurobarometer 390 on Cyber Security, July 2012, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

INTRODUCTION

Research shows that 70% of Europeans use the internet regularly.³ Almost half of EU consumers (45%) shop online, with 11% shopping from traders based in another European country.⁴ Consumers choose to shop online as it offers them greater choice and value for money, and such savings have been estimated to amount to €11.7 billion or 0.12% of EU GDP.⁵ The European Commission has set ambitious targets for the growth of e-commerce, with the Digital Agenda establishing targets of 50% of the population buying online and 20% buying online cross-border by 2015.

With increasing internet use and online shopping comes the risk of exposure to online fraud. As fraudulent practices are criminal activities, accurate figures about their incidence are difficult to access. But it is clear cheap methods of mass communication, such as email and the internet, can be used to perpetrate fraud and mass marketed consumer fraud is a feature of the globalised economy. The UK's National Fraud Authority publishes an *Annual Fraud Indicator* report which for 2013 estimates that cyber-fraud represented 41% of all crimes reported to the Action Fraud agency, with an average individual loss of £3 689.⁶ Europol suggests that victims lose around €290 billion each year worldwide as a result of cybercrime making it more profitable than the global trade in marijuana, cocaine and heroin combined.⁷

The perceived prevalence of internet fraud has affected consumer behaviour. For example, the sluggish uptake of cross-border e-commerce has been attributed, in two EU research reports, to fears of online fraud. In a consumer survey, 62% of consumers who had not made a cross-border distance purchase said that fears about fraud put them off⁸. In another survey, around a fifth of respondents expressed concerns that the payment card details may be stolen (21%) and that personal data may be misused (19%) when buying products online in another EU country. At the same time, each problem was actually experienced by less than 0.2% of online shoppers⁹. In general, over half of consumers (54%) say that they are most likely to come across misleading/deceptive or fraudulent advertisements or offers on the Internet — far more than those who mention phone (18%), post (15%), doorstep selling

³ *Digital Agenda for Europe: Internet use and skills*, available at <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DAE%20SCOREBOARD%202013%20-%203-INTERNET%20USE%20AND%20SKILLS.pdf>

⁴ *Consumer Conditions Scoreboard, Consumers at home in the single market*, Ninth Edition, July 2013 available at http://ec.europa.eu/consumers/consumer_research/editions/docs/9th_edition_scoreboard_en.pdf

⁵ *Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods*, Study on behalf of the European Commission, DG SANCO, 2011, available at http://ec.europa.eu/consumers/consumer_research/market_studies/docs/study_ecommerce_goods_en.pdf

⁶ National Fraud Authority, *Annual Fraud Indicator*, June 2013, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

⁷ <https://www.europol.europa.eu/ec/cybercrime-growing>

⁸ 62% of consumers who had not made a cross-border distance purchase said that fears about fraud put them off: 5th Consumer Scoreboard and Flash Eurobarometer 299. 'Consumer attitudes towards cross-border trade and consumer protection', March 2011, http://ec.europa.eu/consumers/consumer_research/editions/docs/consumer_eurobarometer_2011_en.pdf.

⁹ *Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods*, Study on behalf of the European Commission, DG SANCO, 2011.

(14%) or shops (5%). People with home internet access are even more likely to regard the Internet as a primary source of this kind of advertising (61 % vs 24.6 %)¹⁰.

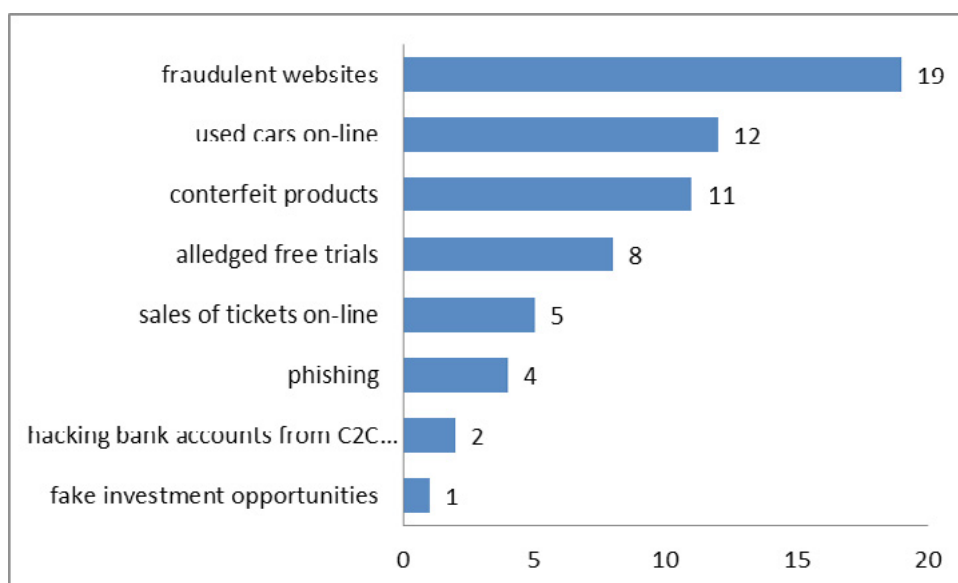
Fraud in general tends to be under-reported and online fraud even more so. For that reason the complaints handled by the European Consumer Centres Network (ECC-Net) offer a valuable source of data relating to the incidence of online fraud. The aim of ECC-Net is to provide consumers with a wide range of services, from providing information on their rights when shopping across borders to giving advice and assistance with their complaints and the resolution of disputes.¹¹ The complaints handled by ECC-Net provide a snapshot of the difficulties which consumers encounter when they shop online.

This report analyses the complaints reported by consumers to ECC-Net during 2012 and provides an analysis of the main areas where consumers reported detriment due to clearly fraudulent practices during the year.

MOST COMMON FRAUDS

The working group circulated a questionnaire to all ECC-Net centres to gather information on the most common scams reported by consumers and seek details of any emerging scams. A total of 27 ECCs responded to the questionnaire. The column bar below shows the number of ECCs that reported fraud in specific areas.

Number of ECCs reporting that the following type of fraud is frequent (among the 27 ECCs which participated to the project)



¹⁰ Flash Eurobarometer 358 'Consumer attitudes towards cross-border trade and consumer protection', June 2013, http://ec.europa.eu/public_opinion/flash/fl_358_en.pdf

¹¹ *Help and advice on your purchases abroad, the European Consumer Centres Network 2012 Annual report*, available at http://ec.europa.eu/consumers/ecc/docs/report_ecc-net_2012_en.pdf

Some types of scams are widespread and were reported by nearly all ECCs participating to the project. 70% of them mentioned **fraudulent websites** selling implausibly cheap electronic products that in fact are never delivered. Consumers are attracted by the low prices on some websites that may offer a significant discount on popular electronic products such as smartphones or cameras. Usually there is no option to pay by credit card, or there is a prohibitively expensive charge to do so and a bank transfer is generally required. These shops appear online; gather as many advance payments as possible, only to disappear from the web, leaving their customers without money nor the product. The trader generally requests payment via a money wiring company which leaves the consumer with no recourse when the item fails to arrive.

Case study

A Bulgarian consumer was contacted by a British seller on Skype. The consumer ordered three mobile phones for the total price of 600 USD which was paid via a money transfer service. The consumer had suspicions about the trader's credibility, but as the price was so low he wanted to buy anyway. The trader reassured him that he had a legitimate business in the United Kingdom and he could easily be pursued in case of non-compliance. After a few days the trader requested the consumer to pay an additional 750 USD for tax and custom fees. The consumer paid this money as well but received nothing. Then he was asked to pay 1000 USD more. The consumer did not agree and asked for his money back. The trader refused and the consumer filed a complaint to the ECC in Bulgaria. The case proved to be a fraud and was closed without a solution because it is impossible to reach amicable solutions with fraudulent cases.

Another common scam involves the sale of **used cars online**. 45% of participating centres responded that this was one of the most common scams reported to them. Consumer finds a very attractive offer on the internet. Websites publish adverts offering incredible discounts or very low prices. The seller often says they are moving abroad or needs the money urgently because of financial problems due to the crisis. After choosing a car in an online advertisement portal, the consumer gets in touch with the seller who provides the consumer with full information on the car. The seller often insists on the use of a shipping company as an escrow service to ensure 'payment security'. Before transportation the consumer is required to pay a deposit and the balance has to be paid after the car receipt. After the payment is done (generally requested by the scammer to be made by bank transfer or money wiring service), the consumer receives information on what date and time the car will be delivered. As no car is delivered, consumer contacts the trader regarding this. The seller informs him that the car has been blocked on the customs and that a duty is needed to release it. The trader asks to make additional payment to the seller or the courier. Regardless of consumer's actions (payment made or not), the seller and the currier disappear without having delivered the good. A variation of this scam may see used cars offered for sale on fake websites. The consumer is often asked to make the prepayment via money transfer. After the money is received, usually the website is deactivated and the "trader" does not respond to any emails and the given tracking number of the order is false. The seller just disappears.

Scams involving the sale of counterfeit products are also frequent and these were highlighted by 41% of ECC offices participating. A consumer finds a very good offer for a low price in the internet (generally for designer or popular branded products) on a website, purporting to be based in the EU. Some fraudulent websites take great steps to look like the official distributor of the brand and often the website address looks quite genuine. The products are stated to be less expensive because the website claims to be an 'outlet'. The consumer orders an item and payment is often requested by money transfer. These companies are usually located outside Europe. When the products arrive in the EU, they can be intercepted by customs and destroyed. Consumers may lose their money and often receive a warning from a trademark office asking them to pay compensation. When the consumer tries to contact the trader, he finds out that the contact details of the company are also fake. Consumers should remember that in some member states buying counterfeit products is considered a criminal offence. Some counterfeit products such as medicines or car components are simply life-threatening.

30% of ECC offices reported receiving a large number of complaints regarding **free-trial scams** and this is known to be a common problem across ECC-Net. In adverts on social network sites and other websites, there are often offers to sample miracle products free of charge, different test packages of health-related and other products, different services (for example downloads of free applications, like Adobe Reader, Open Office, Skype; song lyrics; tattoos; poems; cooking recipes; dating services; the possibility to use the trader's website), which hide important information about costs and the duration of a contract in the terms and conditions. In order to avail of the offer, consumers provide their credit card details to cover the delivery costs. Often the consumer must pay only for shipping. However, if the product is not returned within the requested time, the consumer is tied to a subscription period at a significant cost for new shipments. The products are charged on the consumer's credit card or in other cases with invoices, reminders and even letters from debt collectors and solicitors. Consumers should carefully read all the information about the prices and conditions of membership before signing up for free trials online. This can be found in the general terms and conditions of sale, but all too often in the 'small print'.

In some ECC-Net countries **phishing scams** are also frequent. ECC offices in France, Belgium, Germany, and Spain highlighted this activity. Consumers receive fraudulent emails pretending to come from government bodies or financial institutions which claim that consumer's data is not valid and asks that this be corrected. Consumers may also receive an e-mail from lottery companies informing them that they have won a large amount of money even though the consumer never participated in the lottery. Consumers are usually asked to send sensitive information such as their name, residential address, etc. The scammer then notifies the victim that releasing the funds requires some fees (insurance, registration, or shipping). Once the victim sends the fee, the scammer invents another one. Successive amounts are required to cover costs of different "formalities". Another common approach is that you get informed about a large heritage that you can benefit from, only after paying fees to cover the formalities.

The fraudulent sale of tickets online is another problem cited by 5 participating ECC centres. It can often be incredibly difficult to get hold of tickets for popular concerts or sporting competitions. Fans sometimes pay unrealistically high amounts for tickets that offer no guarantees. They don't know which seats you will be getting, or even if they will receive the ticket. Consumers should only purchase from the official sales channels. This could be done by clicking on the organiser's website to see which sites are authorised to sell tickets and avoid all other ticket sites.

Case study

A Maltese consumer ordered tickets from an online trader for a football match for the price of €827.50. Subsequently the trader informed the consumer that the tickets are not available and that a refund will be given to the consumer, but this was never received.

A Hungarian consumer ordered tickets for Opera Tosca (Scala-Milano) and paid €479 EUR via bank transfer. The website of the Dutch trader offered delivery within 6 to 24 hours, but - in spite of the promises of the trader – the consumer did not receive the tickets at all and the website became unavailable.

A Belgian participant in the Olympic Games in London bought tickets for his family and most loyal supporters from a Norwegian company, for an amount of almost € 3000. The tickets were never delivered. Afterwards, it seemed the company sold 15-20 000 unauthorized tickets to the 2012 Olympics, to over 7000 consumers and for a total value of about € 5 million. Most consumers never received the tickets; nor did they obtain a refund by the company which is now bankrupt. Many consumers received a chargeback from their credit card providers.

The majority of scams reported in this area relate to the sale of tickets for concerts and sporting events but can also extend to transport tickets.

Case study

A Polish consumer bought flight tickets for his family from Poznan to Copenhagen. The day before departure he was unable to check in online, therefore he called the air carrier and they informed him that the reason was simple – he was not on the passenger's list. The consumer tried to contact the agent who sold the tickets but he was unavailable and their website had disappeared. A few months later, ECC Poland received a letter from the local police headquarters asking to explain situation, answer some questions and send it together with relevant documentation.

ECC-Net also receives information about less frequently occurring scams which although rare, are useful to be aware of.

Consumers might become involved in a scam if their **computer or personal information is unprotected**. This type of scam was reported by ECC Belgium and ECC Czech Republic. This scam is typically involved, when the consumer, while acting as a trader places an order to sell something online. An hacker buys it with a hacked account (for example hacked money transfer account). The consumer sends the item and receives money. However, later on, the money transfer company takes back the money once the real account-holder realises that his account has been hacked and abused. The consumer is left behind without item or money.

Investment scams target consumers who want to invest some money on the Forex market or in binary options. Full and adequate information must be given to consumers in such markets because

of the high risk involved. In this type of scheme, as reported by ECC France, traders are registered somewhere outside the EU or do not have the authorisation to sell their products to consumers on the EU territory. For example, the consumer tries to invest small amount of money and wins a small amount of money because it is the objective of the trader to become trustworthy for the consumer. Then the consumer invests bigger amounts of money. However, afterwards he/she loses everything. In other cases the consumer wins money but it is impossible to get the transfer to his account and the trader stops communicating with him.

Consumers should also avoid **purchases concluded outside the auction platform**. This scam is typical when consumer bids on a good in the auction but does not win it. After some time, consumer receives a message from the trader, that the winner of the auction refused to buy the good, and therefore the trader agrees to sell it to the consumer. Any further contact is maintained outside the auction platform. When the consumer pays for the good, the trader does not send the good claiming that the payment is not received or stops communicating.

EMERGING ISSUES IN ONLINE FRAUD



With scammers becoming ever-more inventive and their approaches more sophisticated, it is important that consumers are vigilant and are aware of the latest threats. While new variations of scams emerge daily, often there are common threads which make fraudulent approaches easier to identify. The following fraud have been described by the participating ECCs:

Mobile Fraud

Mobile phones have developed rapidly over the last few years and now offer a huge range of functions. Consumers have grown increasingly comfortable using their phones to transfer money, purchase goods, and engage in other types of financial transactions.¹² However, as mobile phones have evolved into mini-computers with increasingly advanced capability, scammers have evolved with them and users face new threats.

The ECC-Net eCommerce Report 2012¹³ noted. *“The need for mobility and the rapid proliferation of smart-phones and other mobile devices have contributed to an increasing number of users engaging in m-commerce.”* Indeed a recent study has forecast that mobile commerce will represent 6.8% of all online sales across Europe by 2017, reaching €19.25 billion¹⁴

¹² The Future of Money in a Mobile Age <http://pewinternet.org/Reports/2012/Future-of-Money/Overview.aspx>

¹³ The European Online Marketplace: Consumer complaints 2010-2011, September 2012, page 42 http://www.eccireland.ie/downloads/E-commerce_Report_2012.pdf

¹⁴ Forester, EU Mobile Commerce Forecast, 2012 To 2017 http://blogs.forrester.com/michael_ogrady/12-07-19-mobile

The high level of convenience offered by smartphones and other mobile devices is accompanied by higher levels of risk. Europol noted;

*The “always on” culture fostered by mobile devices ensures that potential victims are online, and their data exposed, for a longer amount of time, while the mass distribution of corporate smartphones and the increasingly porous boundary between individuals’ professional and private lives has resulted in cybercriminal exploits against iPhones and Blackberries in an attempt to access data which mirrors information on corporate servers. Handheld devices are arguably also less physically secure than notebooks and desktop computers, in as much as they are more likely to be subject to loss or theft, and less likely to be encrypted (many organisations disable encryption in order to preserve battery life and optimise performance).*¹⁵

A report by Javelin Security and Research found that 7% of smartphone owners were victims of identity fraud, an incidence rate 33% higher compared to the general public. The report suggested that this may be due to certain unsafe customer behavior. For example consumers may not always update to the newest operating system, do not use a password on their home screen, or may store login information on their device.¹⁶ Because smartphones and tablets are so small and portable, they are easier to lose or steal, leading to potential breaches of personal and financial security.

Smartphone users should also be aware of the increasing prevalence of malicious software, or malware, on their devices. Visiting unsafe links from a mobile device is one of the most common ways people encounter such mobile threats. According to security firm Symantec, 31% of mobile users have received a text message from someone they didn’t know asking them to click on a suspect link or dial an unknown premium number.¹⁷ Consumers should be careful what sites they visit on their phone and only download Apps from authorised stores or they may risk a substantial loss of sensitive personal data.



Gaming Fraud

Online gaming is a huge industry and one which is rapidly growing in popularity with reports suggesting that Massive Multiplayer Online Role Playing Games (MMORPGs) will generate 14 billion dollars in revenue by 2014¹⁸

[commerce_will_be_worth_19_billion_euros_within_the_eu_7_by_2017](#)

¹⁵ Europol: Threat Assessment, Internet Facilitated Organised Crime <https://www.europol.europa.eu/content/publication/iocta-threat-assessment-internet-facilitated-organised-crime-1455>

¹⁶ Javelin Security and Research 2012 Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier

¹⁷ 2012 Norton Cybercrime Report http://nowstatic.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

¹⁸ Greengard, (2011). ‘Social games, virtual goods.’ <http://www.iei.liu.se/facksprak/engelska/civilingenjorsutbildning/them18/>

Increasingly, online games involve spending real money to purchase in-game property and so there are significant opportunities for scammers to take advantage of unsuspecting users. Phishing scams and other cyber threats are prevalent, facilitated by the interaction amongst gamers from all over the world.

Risks include inadvertently or recklessly giving away personal or sensitive information, or downloading 'cheats' which claim to help you but which, in fact, may contain viruses/spyware.

Gamers may receive fake emails or be approached by other gamers within the game, and encouraged to reveal personal information which can be used to harvest money and information from online gaming accounts or enticed to visit bogus web sites or open email attachments containing malicious software.

Gamers should be very cautious if requested to reveal personal information or credentials to their accounts.

Case study

A French consumer was a regular player of an online game. While playing, another gamer approached him and advised him to purchase items on a specified website. This looked exactly like the traders official website and the consumer inserted all of his personal details. The consumer's account was hijacked and he lost all his items in his payer account worth approximately €350. The trader also suspended his account for breach of its terms and conditions.

Online Dating Fraud

Online dating has exploded in popularity over the past 10 years, with studies indicating that Europeans spent approximately €811 million on online dating in 2011.¹⁹

However, online dating and social networking has opened up a new avenue for fraudsters who pose as potential romantic partners online. This is a form of advanced fee fraud. Scammers create false profiles on online dating websites, usually accompanied by notably attractive photos, and develop a close online intimacy with a victim, who is then asked for cash to help their new partner out of a crisis of some sort. The perpetrators spend long periods of time developing a close relationship with their victims and give convincing reasons why they cannot meet. Victims often feel they have developed a close relationship with the fraudster and may be unable to accept that the relationship was a scam.

Last year a study²⁰ by the universities of Leicester and Westminster, working with the UK Serious Organised Crime Agency, estimated that 200,000 people had been victims of online dating fraud. However the report noted that this is a significantly under-reported scam.

kursmaterialarkiv/lesson-thirteen/1.333662/social_games_virtual_goods.pdf

¹⁹ Metaflake The Online Dating Market in Europe 2012 <http://www.datingsitesreviewed.com/press/online-dating-market-europe-2012-us.pdf>

²⁰ Whitty and Buchanan 'An examination of the online romance scam' <http://www.esrc.ac.uk/my-esrc/grants/RES-000-22-4022/read>

Animal Rescue

An emerging fraud noted by the ECC-Net eCommerce Report and reported by 3 ECCs in the questionnaire involves the purchase of pets online. The fraudsters post advertisements online for unwanted pets which are available for free. However, consumers are then requested to pay for auxiliary services such as airport storage charges and transport fees in order to receive the pet and are informed that until payment is received the pet is waiting in the airport without any food or care. Alternatively, the consumer is told that the pet has had an accident and requires additional expensive medical care.²¹

Case study

An Austrian consumer found an offer for a kitten from the UK online trader. As requested by the trader he paid € 98 to an animal transport agency in Cameroon. A few days later the consumer was contacted that a problem occurred at the airport and he would need to pay another € 320 as a deposit. The consumer became suspicious but the trader threatened to sue him unless he paid. Intimidated, the consumer paid the money plus an additional sum for cat food. Soon afterwards neither the agency nor the seller could be contacted and no kitten was delivered.

Penny Auctions

'Penny auctions' (or bidding fee auctions) are a relatively recent trend in e-commerce. Essentially they are an online shopping method where users purchase bids in order to participate in the auctioning of an item. The bids are non-refundable so they are unlike traditional auctions where nothing is paid unless your bid is successful. Penny auctions are very popular but consumers should exercise caution as it is possible to spend a lot of money and still lose an auction, or ultimately spend more than the retail value of the item they end up winning.

In the United States the Better Business Bureau, listed penny auctions in their top ten scams of 2011 and warned consumers that, "although not all penny auction sites are scams, some are being investigated as online gambling. BBB recommends you... know exactly how the bidding works, set a limit for yourself, and be prepared to walk away before you go over that limit".²²

Potential fraudulent practices which can disadvantage buyers include shill bidding, where artificial bids are placed automatically by the site operator and hidden membership fees. Shill bidding enables the penny auction operator to unfairly inflate the price of the item, extends the auction time and increases the number of bids required to win.

In late 2010 the UK's Office of Fair Trading took action against the use of auto-bid functions by companies that were using software programs to place artificial bids against consumers²³. The OFT

²¹ The European Online Marketplace: Consumer complaints 2010-2011, September 2012, page 51 http://www.eccireland.ie/downloads/E-commerce_Report_2012.pdf

²² BBB names top ten scams of 2011 <http://www.bbb.org/us/article/bbb-names-top-ten-scams-of-2011-31711>

²³ <http://www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-completed/penny-auctions-battybid/#named5>

found that artificial bids are unlawful as they can mislead consumers into bidding against fictitious 'players' and incur additional costs.

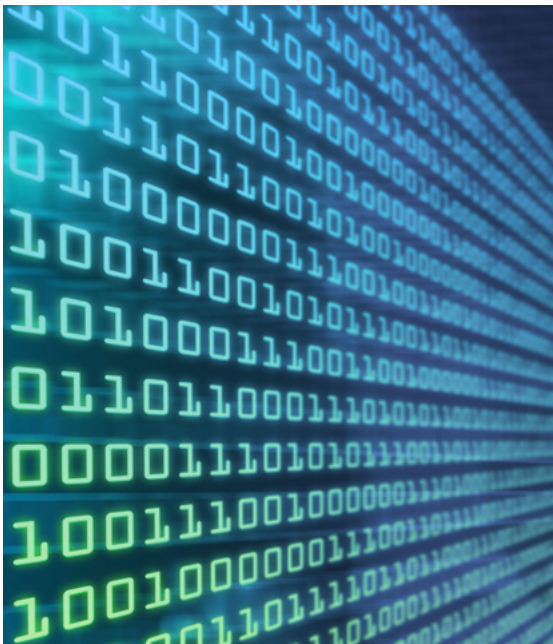
The Belgian Gaming commission considers this kind of auctions as a game of chance. To offer games of chance in Belgium, a license is needed. If a company does not have this license and a website uses this practice and directs itself to the Belgian territory or market, it will be blocked, independently of where the site or company is registered.²⁴

Some penny auction sites deduct on going subscription or membership fees once a free offer is availed of so it is important that consumers take the time to read the relevant terms and conditions before providing credit card details.

Consumers should research the auction sites very carefully before purchasing bids and make sure to understand what's involved before agreeing to any terms and conditions.

Case study

An Irish consumer completed a survey online and received 7 free bids for 7 days for a Maltese based auction company as a reward. He won an iPhone and had to pay €7 delivery charge but the phone was never delivered. He then discovered that this credit card had been debited €200 in addition to the €7. The company claimed that this was a membership fee which he had agreed to in the terms and conditions.



Blocked Computer

An emerging scam, in which consumers get a malware (eg. a virus or Trojan horse) on their computer and it blocks the computer. On the screen consumer then sees the message that falsely claims that, due to copyright infringements, police and authorities have blocked the computer and the only way to unlock it, is to pay money on a banking account. This type of malware is also known as 'ransomware'. The message received usually displays elements that make it look as coming from a legitimate law enforcement agency, in order to scare the victims. It normally gets unlocked once the ransom has been paid, but consumers are giving money to deceivers/organized crime.

²⁴ List of blocked sites: http://www.gamingcommission.be/opencms/opencms/jhksweb_nl/gamingcommission/news/news_0001.html

TIPS & TRICKS TO AVOID BEING SCAMMED

Online shopping can be very worthwhile in terms of the choice and value offered, but it is important to take some precautions to make sure difficulties are not encountered. When shopping online, the product or service is usually paid for before it is delivered. The consumer places faith in the seller that the product will be dispatched as soon as he received payment.

Sometimes, however, the consumer may pay for a product that will never be delivered and he/she will no longer be able to contact the seller. By taking a sensible and critical look at the website, consumers can avoid such difficulties, even if some fraudulent offers are very professionally presented and not easy to detect.. Potential scammers will try to catch consumers unaware. This increases their chance of being able to convince consumers to part with their money or personal information. Consumers must be attentive to certain signals indicating a potential fraud: our tips and advice can equip them with tools to recognise and avoid online fraud.

1. The first and foremost rule is: **if an offer seems too good to be true, it most probably is!**

A simple internet search should reveal any negative feedback about the trader left by other consumers, but be aware that some unscrupulous traders may also leave false positive feedback about themselves.

2. It is important to **verify where the website is located.**

The domain-extension²⁵ does not mean that the shop is actually located in the corresponding country, for example .co.uk does not necessarily mean that the website is based in the United Kingdom. Websites operating in the EU must display a physical address and contact information. Public company registers can help you find if the company is really registered in that country. You can search for any domain and IP website in publicly available databases which checks the registrant's data, like who.is or similar.

Is the website located in Europe? Anyone buying on a website registered in the European Economic Area (or EEA), to which all European member states, Norway, Iceland and Liechtenstein belong, is protected by European law. Under EU legislation consumers have many rights and basic consumer protection is guaranteed throughout the EEA. If you buy outside the EEA, then you may not benefit from this protection and you may have to abide by the legislation of the country where the website is based.

Is the website located outside Europe? If you buy goods outside the EU, you have to pay the VAT-rate of your country in addition to customs duty in most cases. These costs depend on the price and the type of product you have bought. The transport firm also often charges an administrative fee. A price that initially looks low can turn out to be much higher than expected if you purchase outside the EU, so

²⁵ http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

check the level of duties you will have to pay. You may also not be able to rely on European consumer protection legislation if something is going wrong.

In April of 2001, responding to the challenges of multinational Internet fraud, and working to enhance consumer protection and consumer confidence in e-commerce, 13 countries unveiled econsumer.gov, a joint effort to gather and share cross-border e-commerce complaints. Today, consumer protection agencies in 28 countries participate in this initiative where consumers can submit their complaints online. Consumers International (CI) - the world federation of consumer groups that, working together with its members, serves as the only independent and authoritative global voice for consumers: <http://www.consumersinternational.org/>. Consumers can find contact details of all consumer organisations in the world.

3. Some websites are affiliated to a **trustmark scheme**. As such, they must respect the conditions of the scheme set out in a code of conduct that affiliated websites must follow. Watch out for fake trustmarks or websites that fraudulently post a trustmark logo. Check on the website of the trustmark to see if that website is indeed a member²⁶.

4. **Pay with a safe payment method.** The most secure payment method is to pay after the receipt of your package. However, most sellers require you to pay for the product or service before delivery. Check whether the website offers a secure method of payment. You can see this from a little key or lock that appears at the bottom of your screen, or if the internet address begins with <https://> instead of the usual <http://>.

The most common method of payment is by **credit card**. This is also the safest payment method, because you can dispute the payment with the credit card company if the purchased item or service is not delivered.

Never pay for purchases online using a money-wiring service because you will have no recourse if something goes wrong. Many fraudsters encourage this method of payment for this very reason. Money wiring services should only be used to send money to people you know and trust and is not suitable for ecommerce transactions.

5. **Verify the information** provided by the webtrader. European legislation obliges online traders to put certain information on their website, such as (but not limited to):
 - identity, geographical address (not a PO box number), e-mail address, ;
 - the method of payment and delivery;
 - the minimum duration of the agreement for a subscription to a magazine, for example;
 - Cooling off period to change your mind;
 - Delivery and return conditions;
 - The main characteristics of the product or services that you will purchase.

²⁶ ECC-Net report: Can I trust the trust mark? <http://www.eccbelgie.be/ecc-net-report-can-i-trust-the-trust-mark-s76441.htm>

Check if the website mentions this minimum information. If the information is not clear or incomplete, you should seek clarity by asking the seller questions. Do not make a purchase if you have any major questions or concerns.

Find the company's headquarters on the internet and verify that it matches that displayed in ads and on company's web site. If the supplier claims to be a multinational company, but the given address is located in the middle of a residential area in the suburbs, usually there is something wrong.

6. Think about the way the traders present themselves.

Is the layout of the web site professional? E-mail addresses on free or anonymous servers are generally best avoided as they are not a good indicator of professionalism. Also if a website is placed on a free hosting server²⁷, this may not be a good indicator of professionalism. Things to watch out for include: website which has only recently registered, incorrect language style, requests for payment in advance by bank transfer or money wiring service, additional requests for further payments under a false pretence (customs, insurance, more packed products than ordered).

7. Be careful with your personal data. It is very valuable so be careful not to provide unfamiliar websites with more information than is necessary.

Always update to the newest operating system, use a password on your home screen, do not store login information on your device. Be careful what sites you visit on your mobile phone and only download Apps from authorised stores otherwise you may risk a substantial loss of sensitive personal data.



Ignore spam. Never provide any personal or financial information if requested by email and never click on suspicious links or open unknown attachments. Legitimate companies will never seek sensitive information from you in this way.

You may wish to share your experiences with friends and family or leave feedback online to warn other consumers about suspect traders.

²⁷ A free web hosting service is a web hosting service that is free, usually advertisement-supported. Free web hosts will usually provide a subdomain (yoursite.example.com) or a directory (www.example.com/~yourname).

GENERAL ONLINE SHOPPING CHECKLIST

Try to shop on a familiar or recommended sites and carefully research unfamiliar traders by following this check-list:

- Is there a **geographical address**? Never rely solely on an email address or a post office box number as these are difficult to trace.
- Is there a **landline number**? Call the number to check if it is working and correct.
- Is the business **registered**? Look up the VAT number and check that the number is valid on the European Commission VIES website (VAT Information Exchange System²⁸).
- When was the **website registered**? Beware of sites that have only recently been set up as fraudulent sites come and go very quickly. You can find this information on domain lookup websites²⁹.
- Research the **background** of unfamiliar websites by carrying out a simple internet search to see if the website is mentioned on forums and has a good or bad reputation.
- Be extra careful with commercial offers that **'pop-up'** or otherwise appear unrequested on your screen.
- Don't blindly trust **trustmark** logo, check the trustmark's website to verify that seller is really affiliated.
- Ask **questions** about the product and assess how serious the answers provided are.
- Does the **price** you have to pay correspond to the price indicated on the website? Does the price include everything, even administrative and delivery costs?
- What **guarantee** is offered on the products?
- Does the site mention the **right of withdrawal**? Is it indicated correctly?
- Does the website offer a **secure payment** system (https or padlock)? Never pay for a purchase with money wiring service or any other unsecure payment method.
- Can you find the **general terms and conditions** and are they clear?
- **Keep** the order details, print or save a copy where necessary (print screen).
- If you have any **doubts**, ask your local European Consumer Centre or another reliable source for information.
- Remember, if it sounds too good to be true, then it probably is.

²⁸ http://ec.europa.eu/taxation_customs/vies/

²⁹ For example: <http://www.eurodns.com>

RESPOND QUICKLY IF YOU ARE THE VICTIM OF FRAUD

- If you have paid with a credit card, ask the credit card provider **to reverse the payment**. If an investigation shows that you have been the victim of fraud, you will be reimbursed.
- **Consult** ECC-Net or another consumer service that can advise and assist you.
- If you have been the victim of online fraud, you can **report it to the police**. Save all evidence – mails, web addresses, phone numbers, account numbers, make print screens. You can find the contact details of police offices on **page 21**.

LEGAL PROTECTION OF CONSUMERS

Before mentioning consumer legislation, it should be explained that **on-line fraud is, first of all, covered by the criminal laws of the Member States**, under the powers of the competent police bodies (and that there are international police agreements which aim at ensuring cooperation between police forces in cross-border cases).

In addition to (and outside) the remedies available in the Member States to counter cases of outright fraud (see table below on responsible national police bodies), there is EU legislation which protects the economic interests of consumers when shopping on line from real traders.

Below is an non-exhaustive overview of the main pieces of EU consumer protection legislation.

- **Directive 97/7/EC on the protection of consumers in respect of distance contracts** (Distance Selling Directive) applies to both goods and services, where the contract is made between a supplier (a seller acting in the course of a business) and a consumer and there is no face-to-face contact between them.
- As of 13 June 2014 the Distance Selling Directive will be replaced by **Directive 2011/83/EU on consumer rights**. The new Directive strengthens consumer protection in particular when buying on the Internet. Consumers will have to be provided with essential information before they order goods or services on-line, including about the functionality and interoperability of digital content. The new Directive furthermore bans pre-ticked boxes when offering additional services, internet cost traps and charges of which the consumer was not informed in advance.
- **Directive 2005/29/EC on Unfair Commercial Practices** lays down harmonised rules to protect consumers against unfair commercial practices. It ensures that consumers are not misled or exposed to aggressive marketing and that any claim made by traders in the EU is clear, accurate and substantiated, enabling consumers to make informed and meaningful choices. Although this legislation protects consumers when shopping online, scammers do not follow legislation.

- **Directive 93/13/EEC on unfair terms in consumer contracts** ensures that standard terms that cause a significant imbalance in terms of rights and obligations to the detriment of the consumer, are not binding on the latter.

Despite the popularity of online payments, the available options for payment service users to increase their protection are not well known. A **chargeback** is the practice of forcefully recovering funds from the recipient by a payment service provider. A chargeback can be initiated on the basis of law or contractual obligations. The Payment services directive³⁰ deals with two specific chargeback situations; a) transactions made without authorization and b) transactions made without the user knowing the amount of the transaction.

The payment services directive does not deal with intent when it comes to erroneous or fraudulent transactions, it only looks at whether or not the transaction is authorized or if the consumer was aware of the exact sum.

Chargebacks based on contractual obligations are often used for the non-delivery situations consumers face. These obligations stem from the contract the consumer has with the payment service provider(s); this can be a bank, an intermediary (VISA, MasterCard, Eurocard, Diners, American Express etc.) or another payment facilitator. The payment instrument most likely to include protection against non-delivery is the credit card, but it is also present to some extent for other payment methods.

The payment services directive gives the payment service user a time limit of thirteen months to notify the payment service provider of the error. For chargebacks based on contractual obligations the time limit is often much shorter.

A number of ECCs have reported that consumers have difficulties obtaining a refund from the credit card company, unless they can clearly prove that fraud was involved. Regardless of whether the chargeback option is provided by the contract with the credit card issuer or by national law, consumers always have to turn to their credit card provider first in order to receive a refund. In the event that the credit card provider refuses to refund the consumer, the question of how the chargeback option is regulated becomes relevant. If the chargeback option is provided under the contract with the credit card provider, the consumer may only file a claim individually at an ADR body or court. If the chargeback option is provided under national law, the consumer may either file a lawsuit individually or can turn to a national enforcement body.³¹

Consumers should remember:

- Scammers do not respect legislation.
- Criminal spectrum is involved here. Police authorities around the EU are committed to identifying and arresting those involved in criminal activities online, in particular when it comes to large-scale scams. However, it can prove challenging for enforcement authorities to track down the perpetrators due to specific characteristics of the internet, such as its cross-border nature and the anonymity it offers.
- The best protection against scams is knowledge!

³⁰ The Payment services directive 2007/64/EC

³¹ The European Online Marketplace: Consumer complaints 2010-2011, September 2012, http://www.eccireland.ie/downloads/E-commerce_Report_2012.pdf

WHERE CAN CONSUMERS REPORT A SCAM?

| Country | Institution | Contact |
|----------------|---|---|
| Austria | Police – Cyber crime department | against-cybercrime@bmi.gv.at www.bmi.gv.at/cms/BK/meldestellen/internetkrimina/start.aspx |
| Belgium | Police together with the Ministry of Economy | www.ecops.be |
| Bulgaria | Police, Cybercrime Police | Local police office |
| Cyprus | - | - |
| Czech Republic | Police | - |
| Denmark | - | - |
| Estonia | Police | - |
| Finland | Police | - |
| France | Police | - |
| Greece | Police – Cyber Crime Unit | ccu@cybercrimeunit.gov.gr , Tel. No. for local calls: 11012. For international calls: +30 210-6476464 & +30 210-6476000 |
| Germany | Competent public prosecutor | - |
| Hungary | Police | - |
| Iceland | Police | - |
| Ireland | The Garda Bureau of Fraud Investigation | www.garda.ie |
| Italy | Police, Postal Police | - |
| Latvia | Economic Crime department of Police | - |
| Lithuania | Police | Local police office |
| | Lithuanian Cybercrime Investigation Board of Criminal Police bureau | http://www.cyberpolice.lt/ ³² |
| Luxembourg | - | - |
| Malta | Cyber Crimes Bureau in Police | - |
| Netherlands | The Dutch Fraud helpdesk | www.fraudehelpdesk.nl |
| Norway | Police | - |
| Poland | Police | - |
| Portugal | Police | - |
| Romania | The General Inspectorate of the Romanian Police | Tel.: 021.310.17.57, E-mail: crimaorg@politiaromana.ro . All complaints must be submitted in Romanian. |
| Slovakia | - | - |
| Slovenia | Police, SI-CERT | - |
| Spain | Dirección General de la Policía Nacional | www.policia.es |
| | Unidad de Investigación de la Delincuencia en Tecnologías de la Información | Email: delitos.tecnologicos@policia.es Tel: 91 582 27 51 / 91 582 23 07 |
| | Brigada de investigación tecnológica | http://www.policia.es/org_central/judicial/udef/bit_alertas.html |
| | Dirección General de la Guardia Civil | www.gdt.guardiacivil.es |
| | Grupo de Delitos Informáticos | https://www.gdt.guardiacivil.es Email: delitostelematicos@guardiacivil.org Tel: 91 514 64 00 |

³² Crimes committed in cyberspace whose value according to the Criminal Code of Republic of Lithuania does not exceed the amount of 250 minimum standard of living (MSLs, currently 250 MSLs equals to: 32500 LTL or 9412 EUR), which does not cause high societal impact or which are not technically complicated are investigated by the territorial police units

| Country | Institution | Contact |
|----------------|--|---|
| Sweden | International Public Prosecution Office (National Intellectual Property Crime Unit) Patent and Trademark Office (Design and Trademark Department) Swedish Police Swedish Companies Registration Office Swedish Customs (Law enforcement) and Medical Products Agency | - |
| United Kingdom | The Serious Organised Crime Agency in the UK Actionfraud | http://www.actionfraud.police.uk/ |



THE EUROPEAN CYBERCRIME CENTRE (EC3)

The European Cybercrime Centre (EC3) was set up within Europol, the European law enforcement agency in The Hague, The Netherlands. The EC3 officially commenced its activities on 1 January 2013.

The EC3's aim is to provide EU police with a central platform to coordinate investigations and collect information on cybercrime activities. It should boost the EU's capacity to identify and dismantle perpetrators of criminal activities carried out on the internet.

In line with Europol's mandate, EC3 is here to increase cooperation in law enforcement operations but is not empowered to receive direct reports from victims nor launch investigations on their basis.

EC3 a mandate to tackle the following areas of cybercrime:

- That committed by organised groups to generate large criminal profits such as online fraud;
- That which causes serious harm to the victim such as online child sexual exploitation;
- That which affects critical infrastructure and information systems in the European Union.

CONCLUSIONS AND RECOMMENDATIONS

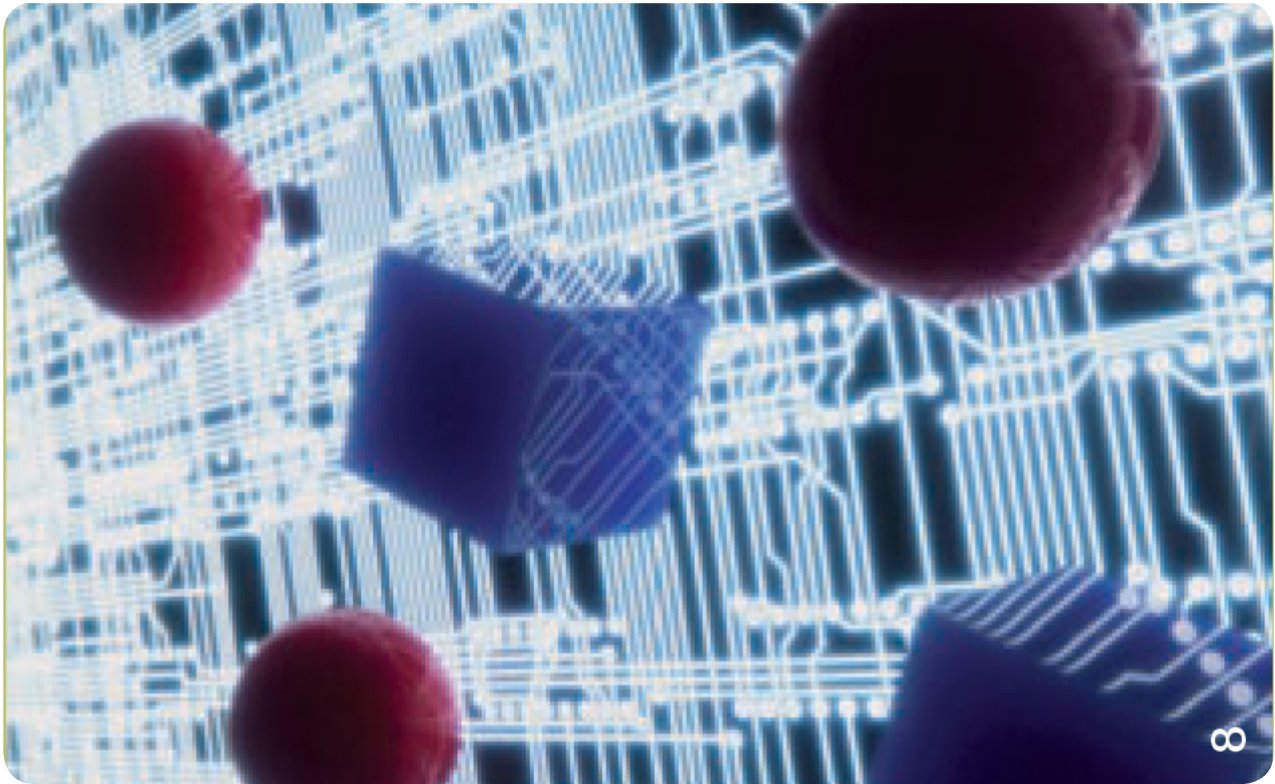
The Working Group described the most commonly reported fraud cases in cross-border e-commerce that were encountered by ECCs and came to the following conclusions:

- According to the ECCs experience, fake offers, second hand cars and counterfeit products were the most commonly types of fraud, with free trial and phishing scams, being less frequent but still significant.
- The ECC-Net competence in the event of a fraud is limited as their role is mainly to advise on consumer rights and assist in solving trade disputes with honest traders. In fraud cases, originating from dishonest traders, usually difficult to locate, consumers are always advised to turn to the police or criminal enforcement authorities (see table on page 21) At EU level, the European Cybercrime Centre (EC3) provides a platform for the coordination of national police investigations on cybercrime activities. It also collects information on cybercrime from a wide array of public, private and open sources in order to enrich available police data, provides forensic support as well as other services which in the end aims to protect EU citizens from online fraud. It is therefore important that consumers report the fraud for which they were a victim to their competent national authorities.
- The ECC-Net is preparing a report on "chargeback", i.e. the possibility for consumers to obtain a refund from the credit card company in case the product ordered is not delivered. Regardless of whether the chargeback option is provided by the contract with the credit card issuer or by national law, consumers always have to turn to their credit card provider first in order to receive a refund.
- Many frauds that migrate to the Internet have existed in one form or another for many years, but have evolved with technology. Consumers must be cautious and understand that frauds will continue to evolve into new forms and new platforms. As almost half of EU consumers shop online, with 11% shopping from traders based in another European country, it is inevitable that online shoppers may encounter e-commerce fraud at some stage. The goal of this report, as well as other information efforts done by public authorities is to minimize the risk to consumers by increasing their awareness and their knowledge on how to shop safely online.



In this respect, it is important to stress that although the ECC-Net has a limited role in securing redress for consumers in the event that they fall victim to a scam, the network is very proactive in promoting

scam awareness. The websites of most ECC-Net members contain a wealth of information for consumers on scams and how to avoid them in their national language. They regularly highlight scam issues in their local media.



What more can the ECC-Net do?

- Encourage consumers to spread the word and share their new scam knowledge with family and friends.
- Target younger consumers via interactive presentation in schools, colleges and universities, as well as use modern technologies that help explaining scams and risks that they can pose.
- Inform consumers about new types of scam as soon as the ECC office finds out about it
- Inform the competent authorities of the new scams.

CONTACT DETAILS FOR ECCS

AN UPDATED LIST OF THE EUROPEAN CONSUMER CENTRES CONTACT DETAILS IS ALSO AVAILABLE AT:
<http://ec.europa.eu/ecc-net>

AUSTRIA
 EUROPEAN CONSUMER CENTRE AUSTRIA
 MARIAHILFER STRASSE 81
 1060 WIEN
 TEL: +43 1 588 77 0
 EMAIL: info@europakonsument.at
 WEB: www.europakonsument.at

BELGIUM
 EUROPEAN CONSUMER CENTRE BELGIUM
 RUE DE HOLLANDE/HOLLANDSTRAAT 13
 1060 BRUXELLES/BRUSSELS
 TEL: +32 2 542 33 46 (NL)
 TEL: +32 2 542 33 89 (FR)
 EMAIL: info@eccbelgium.be
 WEB: www.eccbelgium.be

BULGARIA
 EUROPEAN CONSUMER CENTRE BULGARIA
 BACHO KIRO STREET 14
 1000 SOFIA
 TEL: +359 2 986 76 72
 EMAIL: info@ecc.bg
 WEB: www.ecc.bg

CYPRUS
 EUROPEAN CONSUMER CENTRE CYPRUS
 ANDREAS ARAOUZOS 6
 1421 NICOSIA
 TEL: +357 228 67 177
 EMAIL: ecccyprus@mcit.gov.cy
 WEB: www.ecccyprus.org

CROATIA
 EUROPEAN CONSUMER CENTRE CROATIA
 ULICA GRADA VUKOVARA 78, ZAGREB
 TEL: +385 1 6106936
 FAX: +385 1 6109150
 EMAIL: anijela.markovickrstic@mingo.hr

CZECH REPUBLIC
 EUROPEAN CONSUMER CENTRE CZECH REPUBLIC
 ŠŤĚPÁNSKÁ 15
 12000 PRAGUE 2
 TEL: +420 296 366 155
 EMAIL: esc@coi.cz
 WEB: www.evropskyspotrebitel.cz

DENMARK
 EUROPEAN CONSUMER CENTRE DENMARK
 CARL JACOBSENS VEJ 35
 2500 VALBY
 TEL: +45 4171 5000
 EMAIL: info@forbrugereuropa.dk
 WEB: www.forbrugereuropa.dk

ESTONIA
 EUROPEAN CONSUMER CENTRE ESTONIA
 RAHUKOHTU 2
 10130 TALLINN
 TEL: +372 6201 708
 EMAIL: consumer@consumer.ee
 WEB: www.consumer.ee / www.ecc.ee

FINLAND
 EUROPEAN CONSUMER CENTRE FINLAND
 HAAPANIEMENKATU 4A, 7TH FLOOR
 P.O. BOX 5
 00531 HELSINKI
 TEL: +358 1 194 676
 EMAIL: ekk@kkv.fi
 WEB: www.ecc.fi

FRANCE
 EUROPEAN CONSUMER CENTRE FRANCE
 BAHNHOFSPLATZ 3
 77694 KEHL
 TEL: +49 7851 991 48 0
 EMAIL: info@cec-zev.eu
 WEB: www.europe-consommateurs.eu

GERMANY
 EUROPEAN CONSUMER CENTRE GERMANY
 BAHNHOFSPLATZ 3 77694 KEHL
 TEL: +49 7851 991 48 0 EMAIL: info@cec-zev.eu
 WEB: www.eu-verbraucher.de
 ECC KIEL OFFICE
 ANDREAS-GAYK-STR. 15
 24103 KIEL
 TEL: +49 7851 991 48 0
 EMAIL: info@cec-zev.eu
 WEB: www.eu-verbraucher.de

GREECE
 EUROPEAN CONSUMER CENTRE GREECE
 ALEXANDRAS AV. 144
 114 71 ATHENS
 TEL: +30 21064 608 62
 EMAIL: ecc-greece@synigoroskatanaloti.gr
 WEB: http://www.synigoroskatanaloti.gr/index_ecc_en.html

HUNGARY
EUROPEAN CONSUMER CENTRE HUNGARY
JÓZSEF KÖRÚT 6
1088 BUDAPEST
TEL: +36 1 459 48 32
EMAIL: info@magyarefk.hu
WEB: www.magyarefk.hu

ICELAND
EUROPEAN CONSUMER CENTRE ICELAND
HVERFISGÖTU 105
101 REYKJAVIK
TEL: +354 545 1200
EMAIL: ena@ena.is
WEB: www.ena.is

IRELAND
EUROPEAN CONSUMER CENTRE IRELAND
MACRO CENTRE, 1 GREEN STREET
7 DUBLIN
TEL: +353 1 8797 620
EMAIL: info@eccireland.ie
WEB: www.eccireland.ie

ITALY
EUROPEAN CONSUMER CENTRE ITALY
VIALE DEGLI AMMIRAGLI 91
00136 ROMA
TEL: +39 06 442 38 090
EMAIL: info@ecc-netitalia.it WEB: www.ecc-netitalia.it
ECC BOLZANO OFFICE
VIA BRENNERO 3
39100 BOLZANO
TEL: +39 0471 98 09 39
EMAIL: info@euroconsumatori.org
WEB: www.euroconsumatori.org

LATVIA
EUROPEAN CONSUMER CENTRE LATVIA
Brīvības street 55
LV- 1010
TEL: +371 67388625
info@ecclatvia.lv
WEB: www.ecclatvia.lv

LITHUANIA
EUROPEAN CONSUMER CENTRE LITHUANIA
ODMINIŲ G. 12
01122 VILNIUS
TEL: +370 5 265 03 68
EMAIL: info@ecc.lt
WEB: www.ecc.lt

LUXEMBOURG
EUROPEAN CONSUMER CENTRE LUXEMBOURG
2A, RUE KALCHESBRÜCK
L-1852 LUXEMBOURG
TEL: +352 26 84 64 1
EMAIL: info@cecluxembourg.lu
WEB: www.cecluxembourg.lu

MALTA
EUROPEAN CONSUMER CENTRE MALTA
SOUTH STREET 47A
VLT 1101 VALLETTA
TEL: +356 21 22 19 01
EMAIL: ecc.malta@gov.mt
WEB: www.eccnetmalta.gov.mt

THE NETHERLANDS
EUROPEAN CONSUMER CENTRE NETHERLANDS
CATHARIJNESINGEL 55E
3511 GD UTRECHT
TEL: +31 30 232 64 40
EMAIL: info@eccnl.eu
WEB: www.eccnl.eu

NORWAY
EUROPEAN CONSUMER CENTRE NORWAY
ROLF WICKSTRØMS VEI 15
0404 OSLO
TEL: +47 23 400 500
EMAIL: post@forbrukereuropa.no
WEB: www.forbrukereuropa.no

POLAND
EUROPEAN CONSUMER CENTRE POLAND
PLAC POWSTAŃCÓW WARSZAWY 1
00 950 WARSAW
TEL: +48 22 55 60 118
EMAIL: info@konsument.gov.pl
WEB: www.konsument.gov.pl

PORTUGAL
EUROPEAN CONSUMER CENTRE PORTUGAL
PRAÇA DUQUE DE SALDANHA 31-1
1069-013 LISBOA
TEL: +351 21 356 4750
EMAIL: euroconsumo@dg.consumidor.pt
WEB: <http://cec.consumidor.pt>

ROMANIA
EUROPEAN CONSUMER CENTRE ROMANIA
MAIOR AVIATOR STEFAN SANATESCU STR. 44, FLOOR
1, AP. 2, SECTOR 1
011478 BUCHAREST
TEL: +40 21 315 71 49
EMAIL: office@eccromania.ro
WEB: www.eccromania.ro

SLOVAKIA
EUROPEAN CONSUMER CENTRE SLOVAKIA
MIEROVÁ 19
827 15 BRATISLAVA 212
TEL: +421 2 4854 2019
EMAIL: info@esc-sr.sk
WEB: www.esc-sr.sk

SLOVENIA
EUROPEAN CONSUMER CENTRE SLOVENIA
FRANKOPANSKA 5
1000 LJUBLJANA
TEL: +386 1 432 30 35
EMAIL: epc@epc.si
WEB: www.epc.si

SPAIN
EUROPEAN CONSUMER CENTRE SPAIN
PRINCIPE DE VERGARA 54
28006 MADRID
TEL: +34 91 822 45 55
EMAIL: cec@consumo-inc.es
WEB: <http://cec.consumo-inc.es>

SWEDEN
EUROPEAN CONSUMER CENTRE SWEDEN
TAGE ERLANDERGATAN 8A BOX 48
65102 KARLSTAD
TEL: +46 54 19 41 50
EMAIL: info@konsumenteuropa.se
WEB: www.konsumenteuropa.se

UNITED KINGDOM
EUROPEAN CONSUMER CENTRE UK
1 SYLVAN COURT, SYLVAN WAY, SOUTHFIELDS
BUSINESS PARK
SS15 6TH BASILDON ESSEX UK
TEL: +44 8456 04 05 03
EMAIL: ecc@tsi.org.uk
WEB: www.ukecc.net

