e-Crime

This volume contains the written evidence accepted by the Home Affairs Committee for the e-Crime inquiry.

<table>
<thead>
<tr>
<th>No.</th>
<th>Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Home Office</td>
<td>1</td>
</tr>
<tr>
<td>01</td>
<td>Serious Organised Crime Agency</td>
<td>16</td>
</tr>
<tr>
<td>01a</td>
<td>Supplementary</td>
<td>20</td>
</tr>
<tr>
<td>02</td>
<td>British Retail Consortium</td>
<td>22</td>
</tr>
<tr>
<td>03</td>
<td>NSPCC</td>
<td>26</td>
</tr>
<tr>
<td>04</td>
<td>Philip Virgo</td>
<td>31</td>
</tr>
<tr>
<td>05</td>
<td>Engineering the Future</td>
<td>34</td>
</tr>
<tr>
<td>06</td>
<td>Foundation for Information Policy Research</td>
<td>39</td>
</tr>
<tr>
<td>06a</td>
<td>Supplementary</td>
<td>42</td>
</tr>
<tr>
<td>07</td>
<td>City of London Police</td>
<td>46</td>
</tr>
<tr>
<td>08</td>
<td>EMC Corporation and RSA</td>
<td>56</td>
</tr>
<tr>
<td>09</td>
<td>Communications Crime Strategy Group</td>
<td>64</td>
</tr>
<tr>
<td>10</td>
<td>Get Safe Online</td>
<td>68</td>
</tr>
<tr>
<td>11</td>
<td>Symantec</td>
<td>69</td>
</tr>
<tr>
<td>12</td>
<td>National Trading Standards Board, the National Trading Standards eCrime Centre, the Association of Chief Trading Standards Officers, and the Trading Standards Institute</td>
<td>78</td>
</tr>
<tr>
<td>13</td>
<td>Paul Miloseski-Reid</td>
<td>83</td>
</tr>
<tr>
<td>14</td>
<td>Professor Peter Sommer</td>
<td>98</td>
</tr>
<tr>
<td>15</td>
<td>Financial Fraud Action UK</td>
<td>106</td>
</tr>
<tr>
<td>15a</td>
<td>Supplementary</td>
<td>108</td>
</tr>
<tr>
<td>16</td>
<td>Nominet</td>
<td>111</td>
</tr>
<tr>
<td>17</td>
<td>Google</td>
<td>118</td>
</tr>
<tr>
<td>17a</td>
<td>Supplementary</td>
<td>120</td>
</tr>
<tr>
<td>18</td>
<td>Alliance for Intellectual Property</td>
<td>122</td>
</tr>
<tr>
<td>19</td>
<td>Initiative for a Competitive Online Marketplace</td>
<td>124</td>
</tr>
<tr>
<td>20</td>
<td>British Bankers’ Association</td>
<td>126</td>
</tr>
<tr>
<td>21</td>
<td>Facebook</td>
<td>131</td>
</tr>
</tbody>
</table>

As at 23 April 2013
Written evidence submitted by the Home Office [EC 00]

Introduction

1. This paper sets out the Government evidence to the Home Affairs Committee inquiry into e-crime. This response refers to “e-crime” as “cyber crime” throughout in order to be consistent with the Government’s Cyber Security Strategy. It has been prepared in consultation with officials from other Government departments including Cabinet Office, Department for Education, Ministry of Justice, Department for Business, Innovation and Skills, Government Communications Headquarters and officers and staff from the Serious Organised Crime Agency (SOCA), the Police Central e-Crime Unit (PCeU), the Child Exploitation and Online Protection (CEOP) Centre and the National Fraud Authority.

2. The Science and Technology Committee previously examined the risks of both malware and cyber crime in the following reports: the third report of the 2010-12 Session entitled Scientific advice and evidence in emergencies and the twelfth report of that same session entitled Malware and Cyber Crime. The Government welcomed both reports as a valuable contribution to its work on cyber crime.

3. The internet has revolutionised our economy, our society and our personal lives. It enables innovative new businesses to start and grow. It allows existing businesses to lower their costs and increase efficiency, and it gives customers the opportunity to demand better, cheaper and more convenient services.

4. However with such benefits and opportunities come threats. The Government’s National Security Strategy, published in 2010, ranked UK cyber security, of which cyber crime is an element, as a tier 1 national security priority. The Government has committed £650m to the transformational National Cyber Security Programme (NCSP) to bolster its cyber defences. Last November, the Government published its Cyber Security Strategy which set out how the UK will support economic prosperity, protect national security and safeguard the public’s way of life by building a more trusted and resilient digital environment.

What is e-crime is understood to be and how does this affect crime recording?

Types of cyber crime
5. Cyber crime falls into a number of categories, within the general principle that what is illegal offline is illegal online. The first category encapsulates crimes that can only be committed by using computers and the internet, and that occur where a digital system is the target as well as the means of attack. This includes attacks on computer systems to cause disruption (for example Distributed Denial of Service (DDoS) attacks), and the stealing of data over a network often to enable further crime (for example through the spread of viruses and other malware, or computer and network intrusions (hacking).

6. The second category encapsulates “existing” or traditional crimes that have been transformed in scale or form by the use of the internet, such as fraud or the sharing of indecent images of children. Although these crimes have always existed, the growth of the internet has opened up a new (often global) market, which allows for a degree of anonymity, operation on an industrial scale, and has created new opportunities for organised criminal groups to finance their activities.

7. The final category comprises crimes that use the internet but that are not dependent on it. Here, networks are used for communication, organisation or to try to evade law enforcement. In the same way as the internet is indispensable to legitimate businesses, it can be used to organise more effectively a range of “traditional” crime types such as drug dealing, people smuggling and child exploitation and to conceal them more easily from law enforcement agencies.

8. This is a category of crime that is often neglected when discussing the scope of cyber crime. An increasing number of police investigations of crimes, both serious and volume, now have a cyber crime component, requiring the examination of computers, smartphones and digital CCTV evidence. These may not be recorded as cyber crime, but they do require the police to have access to both the skills and the technology to undertake this type of examination as a matter of routine.

9. The online environment provides opportunities for organised criminals to communicate anonymously, particularly through the use of Internet Relay Chat (IRC) and social media. The sole use of these communication services does not in itself constitute cyber crime, but is a clear example of how technology can assist criminals across a range of activities, including drugs, organised immigration crime and firearms.

10. Knowledge regarding the extent and nature of e-crimes is currently limited, but improving. We have more knowledge regarding some forms of e-crimes than others. It is not currently possible to provide an overall measure of the extent of e-crime. It is also not clear whether e-crimes are decreasing or increasing from the evidence currently available, and whether this varies
according to the type of e-crime. However work is underway to address these gaps and gather robust evidence in this area.

**Recording**

11. There is no such crime as an ‘e-crime’ formally defined in legislation. Police record offences\(^1\) categorised in traditional crime terms, and do not capture offences as a ‘cyber’ or ‘e-crime’. So, whilst a fraud, for example, might be facilitated by use of computers, it would be recorded as a fraud offence, or a denial of service with financial demands may well be recorded as extortion.

12. The computer or other technology used to commit crimes is the method (or modus operandi) by which a crime was committed. The details on methods are not collected centrally. In general, what is illegal offline is illegal online, and UK legislation on fraud or other forms of criminal behaviour applies to both. For example, on-line frauds such as lottery scams, dating scams, boiler room scams all constitute the offence of fraud by false representation, contrary to section 2 of the 2006 Fraud Act. Another example relates to online theft offences, which may be recorded under the Copyright, Designs and Patents Act (1988), Computer Misuse Act (1990) or the Communications Act (2003) depending on what is actually stolen.

13. The Home Office has introduced new crime recording classifications to enable law enforcement agencies to capture specific cyber crime offences as laid out in the Computer Misuse Act (1990), such as computer misuse crime, malware, DDoS attacks and hacking offences.

14. Cyber crime is also captured through victim surveys, such as the British Crime Survey (BCS). The Government is continuing to explore further opportunities to working with the police and other partners to improve the identification of cyber crimes within recorded crimes and crime and victim surveys.

*How we are improving reporting*  

15. The Cyber Security Strategy emphasises the importance of increasing the reporting of cyber crimes and there is significant activity under way to address this. The Government has taken steps to expand the role of Action Fraud, which is led by the National Fraud Authority, to become the single reporting point for financially motivated crime. Over the coming months Action Fraud, in partnership with the National Fraud Intelligence Bureau, will press ahead with the roll out of an improved reporting capability to all UK police forces. For the

---

\(^1\) Police recording of crimes is governed by the National Crime Recording Standard (NCRS) and the Home office Counting Rules (HOCR). These set out the principles under which reports received from victims are recorded. Police recorded crime statistics are based on a notifiable list of offences. The HOCR set out the broad classification groups into which those offences are managed for statistical purposes.
first time the police and the National Fraud Intelligence Bureau will have the capacity and capability to analyse all fraud and cyber crime data from one source. This will provide a much more coordinated and joined up approach to targeting those who attack our citizens and businesses.

What is the extent and the nature of the threats on which e-crime policy is based?

16. In October 2010, the National Security Strategy identified the cyber threat to the UK, which includes cyber crime, as a Tier One threat. £650 million of new funding was allocated to the National Cyber Security Programme (NCSP) which will bolster our cyber capabilities in order to help protect the UK’s national security, its citizens and our growing economy in cyber space. At least £63 million of this will go towards enabling the UK to transform our response to cyber crime, in addition to resources ordinarily allocated to law enforcement to tackle crime.

17. There has been some attempt to measure the cost of cyber crime, but it will not be possible to provide a robust estimate until data regarding prevalence and scale of cyber crime has been improved. One widely cited estimate from “The Cost of Cyber Crime” produced by Detica in February 2011, approximates the cost to the UK of cyber crime to be up to £27 billion per year, or around 2% of GDP. Whatever the cost, as businesses and Government move more of their operations online, the scope of potential targets will continue to grow.

18. GCHQ is the operational hub for cyber security in the UK and, through its information assurance and intelligence work is the best place in which to concentrate UK expertise in understanding threats and exploiting opportunities in cyber space. GCHQ also hosts the Cyber Security Operations Centre (CSOC), whose role is to provide greater awareness of threats and developments in cyberspace, and ensure that the UK can respond effectively in the event of a major cyber incident. Law enforcement agencies contribute learning from their activities to CSOC. Within the NCSP, a key element of CSOC’s role is to act as a central hub, to cultivate a greater holistic awareness of threats, vulnerabilities and developments in cyberspace and to communicate these to NCSP stakeholders and ultimately policy makers. CSOC have produced baseline assessments pertaining to various aspects of the cyber crime landscape and regularly produce topic reports, to which the PCeU, SOCA and GCHQ contribute. The most recent example of this involved contributing learning from their operations in relation to the “Hacktivist” threat.

19. The Government is also supporting law enforcement agencies in their work to improve the timely exchange of intelligence with a broad range of industry,

2 http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime
academia and other agencies both in the UK and abroad. This intelligence contributes to law enforcement operations and informs threat assessments and subsequent programmes of activity. Intelligence may take various forms, including brigaded victim reports and the latest network vulnerabilities or methodology. For example, the PCeU routinely shares intelligence concerning threats with industry, academic and law enforcement partners, in addition to tactical and strategic learning from their operational and prisoner debriefing activity. The benefits to this approach mean that law enforcement can respond with one timely investigation, rather than dealing with numerous isolated, reports from individual members of the public. Furthermore, once a trusted space within industry is established and a common vulnerability or attack is experienced, then businesses are more likely to report the issue.

20. The cyber crime Threat Reduction Board, established under the Government’s organised crime strategy “Local to Global” provides an operational context in which law enforcement and intelligence agencies can assess operational and intelligence activity against the Stem, Strengthen and Safeguard themes of the organised crime strategy and provide assurance to Ministers that the cyber crime threat is being effectively tackled. A Cyber Crime Board, chaired by the Parliamentary Under-Secretary for Crime and Security (James Brokenshire MP), has been established to deliver appropriate Ministerial oversight and ensure that policy development is fully informed by the best possible understanding of the threats.

21. What is the effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and what are the potential impacts of proposed organisational change? Are there any gaps in the response to e-crime and, if so, how should they should be addressed?

The current law enforcement landscape

22. Co-ordination of law enforcement efforts is key to providing a joined up, end-to-end response to cyber crime. Our agencies and law enforcement partners work closely together to make this happen, including the UK Intelligence Agencies, Ministry of Defence (MOD), Centre for the Protection of National Infrastructure (CPNI), Police Central e-Crime Unit (PCeU), Serious Organised Crime Agency (SOCA), HM Revenue & Customs (HMRC), UK Department for Business, Innovation and Skills (BIS), the National Fraud Authority and City of London Police among others.

23. The Government has committed £63 million specifically to tackle cyber crime, which has significantly strengthened the capacity and capability of the PCeU and SOCA. In the first 6 months of the programme, PCeU operational intervention has resulted in a reduction of impact on the UK independently
assessed as £140 million. Last financial year (2011/12) there were 45 arrests for cyber crime with 100% victim satisfaction. Over 21,377 web sites have been taken down from April 2011 to April 2012, resulting from evidence gathered by the PCeU Internet Governance Team.

24. There has been significant progress internationally, specifically cooperation to progress cyber investigations with Ukraine and China, and a cyber Joint Investigation Team (JIT) with Estonia which has been authorised and funded by Europol, and which resulted in substantial prison sentences for an Eastern European organised crime network working in the UK. SOCA has carried out a number of investigations (further details at paragraph 44), and further examples can be found in SOCA’s separate submission which sets out its recent successes against cyber crime.

Legislative Capability

25. What is a crime offline is a crime online, and whilst some cyber crime offences such as hacking, phishing, malware or virus attacks are set out in the Computer Misuse Act (1990), many crimes committed online are prosecuted under existing legislation such as the Fraud Act (2006) or the Communications Act (2003).

26. The Government has committed to reviewing the existing legislation relating to cyber crime, to ensure that it is fit for purpose, and remains relevant and effective.

27. In particular, the Government wants the Police and the Courts to have the most effective powers to disrupt, prevent and prosecute those responsible for these crimes. We are therefore reviewing our powers to support law enforcement, including on areas such as gathering and preserving data for use as evidence and information-sharing between sectors and internationally. We have also committed, as part of the Cyber Security Strategy, to encourage Courts in the UK to use existing powers to impose appropriate online sanctions for online offences.

Proposed organisational change

28. Subject to the will of Parliament, the National Crime Agency (NCA) will be established by the end of 2013, at the centre of the reformed law enforcement landscape.

29. The National Cyber Crime Unit (NCCU), which will be part of the National Crime Agency, will focus on tackling the first two types of cyber crime, as set out in paragraphs 5 and 6 above. This will allow the NCCU, to focus its resources and skills on the most sophisticated areas of cyber crime, whilst supporting the NCA and wider law enforcement to take responsibility for tackling cyber-enabled crime. This principle of supporting law enforcement to take responsibility for tackling cyber enabled crime, rather than looking to a
specialist cyber unit to lead, will underpin the work of the NCCU. The third
definition of cyber crime, that of crimes that are facilitated by the internet, is
being tackled through the police who are mainstreaming cyber awareness,
capacity and capabilities throughout their service.

30. The creation of the National Cyber Crime Unit (NCCU) is a critical part of the
Government’s wider National Cyber Security Programme (NCSP). It will bring
together the national law enforcement response to cyber crime under one
roof. This single capability will work closely with other partners, such as
GCHQ, to strengthen the UK’s overall resilience and incident response to
cyber threats and to ensure individuals and industry can take full advantage of
the many opportunities presented by the internet.

31. The National Cyber Crime Unit will deliver a range of benefits to the current
law enforcement response to cyber-enabled crime. By bringing together the
PCEu and SOCA Cyber, the NCCU will eliminate remit overlaps, delivering
efficiencies and spare capacity that can be utilised to bear down harder on
organised cyber criminals. Building on the successes of SOCA Cyber and the
PCEu, the NCCU will deliver:

- A single, high-profile law enforcement lead dedicated to combating
  organised cyber criminals;
- A more targeted focus on the most serious incidents of cyber crime,
  removing the criminals who facilitate cyber-enabled crime further
downstream;
- A stronger, more cohesive response to the most serious cyber-enabled
  crime;
- Dedicated resources to drive a step-change in cyber capabilities across
  law enforcement, police service and wider partners;
- Stronger partnerships at all levels, including delivery of a single point of
  contact for rapid response to dynamic threats and closer engagement
  with industry and academia;
- Closer joint working with the Security and Intelligence Agencies
  through improved ICT connectivity and intelligence sharing.

32. Police and Crime Commissioners will be a powerful local representative, able
to set the priorities for the police force within their force area, respond to the
needs and demands of their communities more effectively, ensure that local
and national priorities are suitably funded by setting a budget and the local
precept, and hold to account the local Chief Constable for the delivery and
performance of the force.

Local Capability

33. In 2008 the National e-Crime Programme conducted a national survey of
police capability on cyber. A new project is being developed by PCEu to
update this research including staffing numbers, training, equipment and best
practice. This will further inform in relation to capability and provide updated information in relation to national response.

34. The publication of the Strategic Policing Requirement will support national co-ordination and collaboration between police forces to respond to serious and cross-border criminality. In order to ensure that local police forces can still access specialist services, the Strategic Policing Requirement seeks to ensure that local policing plans account for cyber capability as well as the contributions that local agencies will provide to the national response.

35. On a national scale, the police response has had limited resources and infrastructure to respond to, exploit, and harness the benefits of the digital environment owing to a fragmented approach to policing cyber crime. The National e-Crime Programme delivered three PCeU hubs to address this situation. The Hubs enhance existing PCeU national operational capability to respond and investigate cyber crime. The regional hubs are based in the North West, East Midlands and Yorkshire & the Humber. The ‘hubs’ were launched in February 2012 and despite their infancy and early stages of development are already contributing to PCeU operations contributing to a fast and dynamic response outside London.

Bringing together law enforcement capabilities

36. Building on the successes of both SOCA Cyber and the PCeU, the establishment of the NCCU will further strengthen the law enforcement response to the most serious cyber crime by addressing a number of gaps that we know exist in law enforcement’s response to cyber crime.

37. First and foremost the NCCU will deliver a single, high-profile law enforcement lead dedicated to combating organised cyber criminals. This will provide increased clarity and coherence in the law enforcement response and a more targeted focus on the most serious incidents of cyber crime where the NCCU can add most value.

38. This ambition fits with the overall goal of the NCA to address the sometimes fragmented law enforcement response to serious and organised crime by creating a new Agency with the mandate to task and co-ordinate the UK law enforcement response. The NCCU will form a vital part of the NCA, able to undertake tasking and coordination across the whole of operational law enforcement, ensuring that appropriate action is taken against criminals at the right level, led by the right agency. The NCCU will also benefit from the NCA’s single national intelligence picture of serious and organised crime to inform its operational activity.

39. As part of this, a key principle of the NCCU is to support law enforcement partners to take the lead in tackling cyber and cyber-enabled crime, rather
than looking to a specialist cyber unit. We know that mainstream cyber capability across law enforcement needs to be enhanced, and so the NCCU will house dedicated resources to drive a step-change across law enforcement, the police service and wider partners. This will build on the existing work of the PCeU in the National e-Crime Programme, including roll-out of the digital forensic triage tools, supporting the Police Professional Body on developing cyber training, providing a single national centre of expertise to provide guidance to wider law enforcement, as well as ensuring that cyber capability is mainstreamed throughout the NCA itself as a role model for wider law enforcement.

40. The expertise and information needed to combat cyber crime sits largely outside law enforcement including in the Security and Intelligence Agencies (SIAs), industry, international partners and others. The NCCU will draw upon the range of experience and expertise from these partners in order to stay effective against cyber criminals. This will involve closer joint working facilitated by enhanced ICT connectivity and intelligence sharing and maintaining a diverse workforce with experience from a range of sectors. The NCCU will look to utilise NCA Special Constables to bring in the relevant expertise, as well as seconding staff out to industry to strengthen relationships and gain experience. The NCCU will also work with operational partners to ensure that there are clear lines of responsibility when responding to the range of cyber threats, from terrorist cyber attacks to cyber attacks on critical national infrastructure.

41. Given the rapid increase in both the volume of digital data generated by individuals and the range of devices and locations on which it can be found (computers, smartphones, CCTV systems, games consoles, in-vehicle GPS systems, remote (cloud) storage etc.), there is a corresponding increase in the number and type of traditional crimes that now have at least some e-crime component to them. These are generally crimes that would be investigated at a local force level rather than by specialist cyber crime units such as PCeU. One of the key emerging gaps is therefore in the provision at a local level of suitable tools, techniques, skills and common processes to enable the police to routinely investigate these crimes effectively.

Addressing gaps in the response

42. In order to improve our local policing response and appropriately direct police resources, law enforcement agencies and the Home Office are working to improve our knowledge around the prevalence and nature of cyber crime, particularly where they relate to volume crimes. This will allow us to effectively train and equip local police officers to tackle these crimes on a day-to-day basis. In this regard, the Home Office Centre for Applied Science and Technology (CAST) is working with policing to evaluate and develop specialist
tools and techniques for use both in serious and volume crime investigations, particularly to assist with rapid and automated examination of large volumes of data.

43. Other activities are being considered to improve knowledge on prevalence and nature of cyber crime in relation to volume crime, for example, ensuring appropriate data capture mechanisms are in place and that we are addressing under-awareness and under-reporting of cyber crimes amongst businesses and the general public. More widely, there is consideration around how we address gaps in knowledge regarding ‘what works’ in terms of preventing cyber crime by encouraging the public and businesses to better protect themselves online.

44. There is evidence of a number of successful SOCA, PeCU, CEOP and NFIB disruptive operations in tackling cyber related activities and reporting to agencies such as Action Fraud, NFIB and CEOP has increased. However, wider evaluations of cyber policing structures, initiatives and performance are currently lacking:

- The PCeU have taken forward work to mainstream cyber awareness, capacity and capability throughout their service. The regional hubs of PCeU launched in February 2012 increase operational capacity and capability and awareness of cyber within the regions. Work is ongoing with Skills For Justice to produce a competency framework for PCeU enforcement and intelligence officers. This framework will be available nationally.

- Over the coming year, funding from the National e-Crime Programme is supporting an interim National Hash Set database, which will amalgamate law enforcement databases and apply consistency to grading and processing indecent images of children.

- Virgin Media worked with SOCA to warn customers on its network that they might have been infected with the dangerous SpyEye Trojan variant. This collects personal and banking information and poses a high level threat to infected users. It is comparable in severity to the ‘Zeus’ Trojan which reportedly siphoned over half a million pounds from UK consumers’ bank accounts last year. SOCA detected around 1,500 Virgin Media customers’ Internet Service Providers (ISPs) infected with the SpyEye Trojan and at risk of identity theft or fraud. Virgin Media wrote to these customers to get help if they were unable to manage the disinfection process themselves.
• SOCA identified and, through its Alerts system, reported several hundred cases of domain name abuse directly to ICANN\(^3\), highlighting continuous failures in the customer validation of domain name registrations by the specific ‘registrars’ directly responsible for the sale of domain names to users. Targeted SOCA Alerts highlighted areas of abuse and registrar practice that disrupted a major online malware distribution group by preventing it from registering and using malicious domain names over a long term period. Collaboration with ICANN to amend the Registrar’s Accreditation Agreement (RAA) has assisted law enforcement efforts in crime prevention and detection, and direct reporting to ICANN, highlighting specific criminal use of domain names and methodology, has encouraged due diligence measures to prevent abuse.

• Following a referral from the Internet Watch Foundation, CEOP identified a website that was hosted in Germany, which contained a large number of child abuse material and a section for people to buy and sell children from sexual exploitation. CEOP worked to identify a suspect who was thought to have produced the website and assisted Kent Police in setting up an undercover operation to gather further evidence against the suspect. This was successful and the suspect, Darren Leggett, was arrested. Leggett was found to have committed a number of sexual offences against young children, and was given an indeterminate sentence on the 21st June this year, with a minimum term of 7 years.

• Action Fraud has reported over 33,000 instances of cyber-enabled fraud or internet crime-related issues, of which 2017 were crimes under the Computer Misuse Act (1990). In addition 19,000 instances of attempted online scams have been reported to the service along with 1,200 reports of virus attacks.

**Working with stakeholders**

45. The Government recognises that in tackling cyber crime there is a key opportunity for industry, Government agencies and law enforcement to come together to provide a joint threat picture, to gather intelligence and to provide a joint response.

Building trust and confidence between the private sector and law enforcement authorities is vital to address any gaps in the response the threat of cyber crime. Industry has a vital role to play and also needs to invest in effective information security in order to reduce the threat from cyber crime. We cannot

---

\(^3\) Internet Corporation for Assigned Names and Numbers, the body responsible for the administration and allocation of domain names.
achieve our goals in isolation. The prosperity of the UK, creating a secure UK business environment, a secure UK (critical) national infrastructure is just as important as bringing criminals to justice. The Cyber Security Strategy creates a framework for an alliance that is greater than its constituent parts. An excellent example of this cross-sector working is the UK Council for Child Internet Safety (UKCCIS) which brings together government, industry, law enforcement, academia and charities to work in partnership to help keep children and young people safe online.

46. We are now considering how best to build on this successful formula to address the interests of industry and Government in dealing with cyber crime. We are also looking at international partnership models for operational information-sharing, such as the National Cyber-Forensics Training Alliance (NCFTA), based in Pittsburgh, USA. The NCFTA brings together private industry and law enforcement in a neutral, trusted environment to identify, mitigate and prevent cyber crime through joint working and data exchange. We will be looking at this, and other such structures, to inform our work to enhance operational-level partnerships between Government and the private sector on cyber crime.

47. At a tactical level, the PCeU continues to build upon the good work with the existing Virtual Task Force (VTF). The VTF was established in July 2009, incorporates staff from the Police Central e-Crime Unit and has achieved considerable success which has resulted in international recognition of the benefits of this model of public/private sector operational delivery. Member organisations have committed a strategic lead member and tactical representatives.

International work

48. Cyber crime is an international crime, and the Government has been clear that a major part of our response is to work internationally at Government and at law enforcement levels.

49. The Government has ratified the Budapest Convention on Cybercrime, as the main international agreement in this area, and has taken an active approach to encouraging countries to sign and ratify it. The Government believes that all countries should put in place the appropriate legislation and law enforcement capability to tackle cyber crime, and the ability to support international partners. The Government believes that the Convention offers the only current and comprehensive framework for this.

50. The Government has opted in to the EU Directive on attacks on information systems to ensure that there is common agreement across EU Member States on offences and sentences to allow our law enforcement agencies to together to identify suspects, gather evidence and bring criminals to justice.
51. The Government supports the creation of the EU Cybercrime Centre, and in particular the decision to locate it in Europol, which will build on its existing high-tech crimes capability. The Government expects the Centre to support Member States in working together to tackle cyber crime, and to develop effective best practice in areas such as cross-border cooperation and information sharing.

52. The Government strongly supports the EU Council Conclusions on the creation of a Global Alliance against Child Sexual Abuse, put forward by the Presidency and the Commission. The Government recognises the need for Member States, third countries, international law enforcement and industry to continue to work together to prevent the spread of child pornography. The Alliance will build on the existing work in this area.

53. The Government strongly supports the work of the Hungarian Government in organising the Budapest Conference on cyber issues that will be held in October. This is a follow up to the London Conference on Cyberspace that was hosted by the Foreign Secretary in November 2011.

What are the options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use?

54. All processing of personal data in the UK, online and offline, must comply with the Data Protection Act 1998 (DPA) and its data protection principles. Importantly, the seventh principle requires that “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

55. The expansion of the Internet and the emergence of social media networks has recently led the European Commission to publish proposals for updated data protection legislation. These proposals were published on 25 January 2012 and contain a Regulation (setting out a general EU framework for data protection) and a Directive (covering authorities dealing with criminal offences and penalties). Amongst other things, the proposals seek to provide individuals with strengthened rights to delete their personal data (including a so-called ‘right to be forgotten’), which could affect the way in which people’s information is held by online services, such as social networks.

56. Given the practicalities, costs and potential for confusion of a full-scale ‘right to be forgotten’, the UK Government will push in negotiations for an overhaul of the provisions as drafted. However, the Government is committed to giving individuals the right to delete their personal data, where this is appropriate. The principles of ‘data minimisation’ and ‘privacy by design’, if adopted by organisations in their systems, should help to ensure that people’s personal
data does not proliferate online and is held securely, minimising the opportunities for those who would seek to use it for criminal purposes.

57. The Information Commissioner, the UK’s independent data protection supervisory authority, enforces the DPA’s requirements and promotes good practice. As part of the latter role, the Information Commissioner’s Office (ICO) has produced guidance for individuals and young people on keeping their personal data safe online, including specific advice on using social networks.

58. There is work under way across Government and industry to improve data protection for customers. BIS and the Home Office are working in partnership with the six major Internet Service Providers (ISPs) in the UK: BT, TalkTalk, Sky, Everything Everywhere, Vodafone, and VirginMedia, to explore what more could be done or done differently to better protect businesses and consumers from online threats such as malware and botnets. This covers the basic security packages that ISPs are offering to their customers, as well as raising awareness amongst customers about the importance of behaving securely online.

59. Further work is under way with Government, industry and law enforcement through the Forum for Innovation in Crime Prevention. This is a strategic expert advisory group drawn from science, business and industry, law enforcement agencies and Government that identifies major opportunities for preventing and disrupting crime through innovative design, technology and behavioural change and proposes solutions that incentivise business engagement.

60. Our law enforcement agencies work with their counterparts overseas to carry out work such as restricting criminal access to the Internet. This is achieved through work with organisations such as the Internet Corporation for Assigned Names and Numbers.

**How effective are current initiatives to promote awareness of using the internet safely and what are the implications of peoples’ online behaviours for related public policy?**

61. Prevention is key, and we are working to raise awareness and to educate and empower people and firms to protect themselves online. GCHQ estimates that 80% or more of currently successful attacks could be defeated by simple best practice, such as updating anti-virus software regularly. The Government works in close partnership with industry on cyber security, recognising that this is crucial to protecting individuals and their data.

62. Organisations can be attractive targets for cyber criminals, who may seek to exploit security vulnerabilities in order to access intellectual property or other commercially sensitive information. In the Cyber Security Strategy, the
Government committed to improving both the information sharing and risk management between businesses, law enforcement and business service providers.

63. The Government supports Get Safe Online, which is a joint public and private sector campaign which provides up to date, accurate and authoritative advice to online consumers on how to protect themselves, their families and their businesses online. We have increased funding for Get Safe Online to £395,000 this year to improve the website and enable it to reach out to more people across the UK. The campaign is working in partnership with various police forces, as well as their private sector partners to provide advice on cyber security that is accessible to everyone.

64. Action Fraud has a key role to play in terms of encouraging and enabling behaviour change in relation to preventing citizens and businesses from becoming victims of crime in this area. An excellent start has been made in this arena with the successful delivery of the “Devil’s in Your Detail” campaign which was a joint initiative between the NFA and private sector organisations from the banking and telecoms industries. This campaign was video-driven and aimed to encourage people to treat their personal information as a valuable commodity. The campaign reached over 4 million people. Subsequent analysis of 4,000 people who watched the videos resulted in over 60% stating that they would take more steps to protect themselves from fraud.

Home Office
August 2012
Written evidence submitted by the Serious Organised Crime Agency [EC 01]

Introduction:

1. This submission sets out the Serious Organised Crime Agency’s (SOCA) written evidence to the Home Affairs Select Committee’s inquiry into e-crime. In the terms of this response we will refer to e-crime as cyber crime throughout the submission.

2. The submission outlines the current level of knowledge within the organisation on cyber crime. This submission has been written in coordination with the Home Office, and should be considered supplementary to its submission.

What e-crime is understood to be and how this affects crime recording

3. SOCA works with its partners, under the Home Office’s Organised Crime Strategy (“Local to Global”), to address the threat of organised cyber crime. Under the Strategy, the multi-agency Cyber Threat Reduction Board\(^1\) (TRB), chaired by SOCA, adopted the following definition of cyber crime in November 2011:

   - ‘pure’ online crimes, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to enable further crime);

   - ‘existing’ crimes that have been transformed in scale or form by their use of the internet. The growth of the internet has allowed these crimes to be carried out on an industrial scale; and

   - use of the internet to facilitate drug dealing, people smuggling and many other ‘traditional’ types of crime.

The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers

4. Organised crime is increasingly globalised and IT-enabled, a trend inevitably accelerating with society’s dependence on the internet. Organised criminals operate their own self-regulated market for cyber crime goods and services, including stolen data, malicious software, technical infrastructure and money laundering: and they operate on an industrial scale. As more data is acquired, stored and shared and ever increasing use is made of mobile devices, so the risk increases. SOCA contributed to the development of the Government’s Cyber Security Strategy which was published in November 2011. The Strategy references research suggesting that the costs to the UK of cyber crime could be in the order of £27 billion per year\(^2\).

---

\(^1\) Threat Reduction Boards were established under the Government’s Organised Crime Strategy to provide focus for law enforcement partners including HMRC, SOCA and UKBA. Each board is chaired by a senior operational partner, responsible for assessing operational and intelligence activity against the three themes set out in the Organised Crime Strategy (stem, strengthen, safeguard). The activities of the boards are subject to scrutiny by the senior officials group and Ministerial structure.

\(^2\) “The Cost of Cyber Crime”, Detica - 14 February 2011
5. SOCA, along with other departments and agencies, has also played a part in contributing to activity led by the Department of Business, Innovation and Skills (BIS), helping to raise awareness at a senior level within private sector organisations of the threat posed by on-line crime to business performance, shareholder value, reputation, intellectual property and the security of information systems.

The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

6. Key activity aligned to the Organised Crime Strategy in respect of cyber crime includes:

   • improving the understanding of, and intelligence about, cyber crime in order to identify changes to drive the response;

   • ensuring that the operational response to cyber crime is being coordinated effectively and is reducing the risk to the UK of cyber crime; and

   • providing assurance that identified organised crime groups are subject to an appropriate level of operational response and that the maximum impact against the threat area is being achieved, improving our understanding of the threat that impacts on the UK.

7. SOCA responded to the Government’s National Cyber Security Programme by expanding its current cyber capability, including the posting of dedicated Cyber Liaison Officers in key locations overseas.

8. Recent successes achieved against cyber crime include:

   • a SOCA led global day of action took place on the 25 April 2012 to tackle Automated Vending Cart (AVC) websites selling compromised financial data. Two UK arrests were made and SOCA intelligence assisted the US in seizing data for 26 AVCs and 36 domains. In addition, as a direct result of eight alerts issued, a further 44 AVCs have been taken down – resulting in significant disruption.

   • in 2011/2012 SOCA and its partners seized over 1,200,000 items of compromised card data from cybercriminals and passed these details to industry via the Alerts system.

   • as a result of SOCA operational activity two men who provided a range of services to credit card fraudsters were sentenced to almost five years imprisonment after facilitating fraud valued at more than £26m. Both pleaded guilty to a range of fraud, money laundering and computer misuse offences, and were sentenced at Bristol Crown Court to three years and 21 months respectively. Forensic analysis revealed payment

---

3 Automated Vending Cart (AVC) is a term coined by SOCA (and now adopted internationally) to describe click and buy e-commerce websites that automate the sale of compromised personal financial data.
card details of more than 340,000 individuals. The estimated losses are a conservative figure and the actual loss is likely to be considerably more. In addition, the information brokered would also have been sufficient to enable fake bank accounts to be set up, which could be used to commit further fraud, such as cheque or identity fraud.

9. SOCA has been involved in dealing with cyber crime on an international level as well. Cyber crime investigations almost inevitably have an international element, with criminals, data and infrastructure typically based across multiple jurisdictions. SOCA has therefore developed close working relationships with many foreign partners, which enables intelligence sharing, evidence gathering - support with the preservation of data in particular - and operational engagement. Recent examples include joint working on the selling of compromised financial data online. A coalition of overseas partners worked together to make arrests and take down websites, multiplying the effectiveness of UK law enforcement activity. Tackling cyber crime internationally will also require new ways of working. The UK is working closely with Interpol, Europol and United States partners to establish more innovative approaches to tackling cyber crime.

10. Mainstreaming of cyber capabilities is underway within SOCA, and will harness the potential of every investigator to use cyber crime tools, not solely those from dedicated cyber units. All officers will receive training on cyber crime, internet security, open source capabilities and online investigation techniques, following the completion of a comprehensive training needs analysis. SOCA operational teams have embedded officers specialising in digital forensics and open source research, making these techniques more readily available at every stage of an investigation. In addition, officers with a dedicated cyber remit have also been placed within other key business areas enabling cyber mainstreaming to grow from within departments.

11. Going forward, the National Crime Agency (NCA) presents the UK with the opportunity to improve its national law enforcement response to crime perpetrated in cyber space or enabled by the internet, through the establishment of a National Cyber Crime Unit (NCCU). The NCCU will act as a centre of expertise for tackling cyber crime. The NCA will have the specialist operational capabilities and the latest technology to ensure that its intelligence gathering and analytical capabilities match the threat posed by cyber criminals. It will bring together the digital investigation capabilities of SOCA and the MPS Police Central e-crime Unit (PCeU) to provide an enhanced response to the cyber crime threat.

Whether there are any gaps in the response to e-crime and, if so how they should be addressed

12. There are a number of factors that can hinder law enforcement in the response to cyber crime. For example, the majority of cyber criminals are not within UK jurisdiction, and international barriers inhibit their identification and prosecution. Differing domestic legislation is also an issue, for example in some countries cyber crime is not recognised in domestic legislation.

13. In response SOCA has worked closely with the Foreign and Commonwealth Office and other government departments to encourage the implementation of
legislation and recognition of cyber crime in key countries. For example the Commonwealth Initiative has agreed to target priority countries for assistance. SOCA Cyber Liaison Officers overseas will work to ensure that cyber crime is also identified as a priority and enhance overall international relations.

14. The UK is also working with global partners to encourage wider adoption of the Budapest Convention on cyber crime, putting in place compatible frameworks of law that enable effective cross-border law enforcement and deny safe havens to cyber criminals.

15. Beyond those law enforcement agencies with a specialist role there is also a general lack of awareness of cyber crime, which hinders the ability to investigate and target both ‘pure’ cyber crime and ‘digitally enabled crime’. It is essential that the message is conveyed across the whole law enforcement community that cyber crime is a priority. The establishment of the NCCU in the NCA, bringing together SOCA and other cyber law enforcement units, will help to further improve the UK’s response.

Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use. The effectiveness of current initiatives to promote awareness of using the internet safety and the implications of peoples’ online behaviours for related public policy.

16. The Government’s Organised Crime Strategy identified ‘Safeguarding’ as one of the key themes for tackling organised crime by reducing the vulnerability of communities, business and the state to become victims of crime. In line with this theme SOCA supports raising awareness of cyber crime to prevent consumers becoming victim to cyber criminals. For example, Get Safe Online (GSOL) is one a number of initiatives between the Government, SOCA, and the private sector. This highlighted the increased use of smart phone malware during ‘Get Safe Online Week’ in November 2011. Criminals use online application stores to entice smart phone users to download rogue applications. The malware is often disguised as ‘free levels’ to popular and legitimate games, or even as security tools. Users are often unaware that fraudsters have control of their phone (and access to personal and payment data) until they receive their monthly bills or otherwise find themselves victims of identity crime. GSOL has produced a free download, The Rough Guide to Online Safety, in order to reduce the threat.

Serious Organised Crime Agency
11 July 2012

---

4 The Commonwealth Initiative is a new multi-stakeholder approach to developing a safe cyberspace internationally, drawing together the combined mandates of existing organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the United Nations Office on Drugs and Crime (UNODC), Council of Europe, International Telecommunications Union (ITU) and Commonwealth Secretariat to develop and implement coherent, holistic cyber capacity building programmes for developing Commonwealth states. It is co-funded by the UK Government (Department of Culture Media and Sport). SOCA chairs the Executive Board.

5 The Budapest Convention on Cyber Crime is the first international treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.
During my appearance before the Committee on the 11 December 2012 to give evidence to the e-Crime inquiry, I promised to write listing the EU Justice and Home Affairs (JHA) measures that SOCA utilises in regards to cyber crime investigations.

There is extensive law enforcement collaboration at an operational level between SOCA and partners across Europe, which supports and informs EU policy. This joint activity takes place through a number of JHA measures. I set out details of these, with a particular emphasis on cyber crime below.

- With the support of other UK law enforcement agencies, SOCA has established a multi-agency UK Liaison Bureau at Europol which, via a network of other national liaison bureaux and contact points, coordinates international operational engagement with other Member States and third countries/organisations which have cooperation agreements with Europol. The UK (SOCA) participates in Europol’s Focal Points Cyborg, Twins and Terminal, working with other partners to address the threat of cyber crime through operational cooperation and sharing intelligence, utilising Europol’s expert analytical capability as the EU’s information hub to identify opportunities for further cooperation.

- On 11 January 2013 the EU Cyber Crime Centre based within Europol opened. This centre will support Member States and EU institutions in coordinating operations and investigations with international partners in line with Europol’s wider mandate; and, will provide an expert analytical capability to partners. The Centre will improve evaluation and monitoring of existing preventive and investigative measures, support the development of training and awareness-raising for law enforcement and judiciary, establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs).

- SOCA also participates in a European Multidisciplinary Platform against Criminal Threats (EMPACT) project on cybercrime, which is led by Romania. This is one of eight EMPACT projects overseen by the EU Standing Committee on Operational Cooperation on Internal Security (COSI) set up to streamline and help coordinate operational cooperation on priority threats to the EU, as part of the EU Policy Cycle on serious and organised international crime. Europol plays a supportive role to this work, through its Focal Points, hosting project meetings and assisting in coordinating operational activity associated with the project.

- SOCA also partakes in the use of Joint Investigation Teams (JITs) to support international operational engagement. The use of JITs provides a mechanism for Member States to cooperate operationally, establishing a clear agreement between participating countries setting out terms of engagement for cooperation and information sharing in accordance with Member States’ national legislation. Both Europol and Eurojust provide support to JITs; Europol in providing analytical support and Eurojust in providing judicial expertise, legal assistance and funding.
In addition to the above measures SOCA also regularly utilises the following JHA measures:

- European Arrest Warrant
- Schengen Article 40
- Financial Intelligence Unit (FIU) Cooperation
- Asset Recovery Offices (ARO)

Yours sincerely,

Andy Archibald
Deputy Director
Serious Organised Crime Agency
1. Introduction

1.1. The British Retail Consortium (BRC) is the lead trade association for the retail sector representing the whole range of retailers, from small independent stores through to the large multiples and department stores, selling a wide selection of products through centre of town, out of town, rural and online stores.

2. Summary

2.1. Retail is at the heart of local communities, employing close to three million people across the country and providing important local goods and services to consumers. The sector is an essential contributor to economic growth and to the regeneration of areas affected by crime and disorder.

2.2. Online retailing is a significant element of the future strategy for many businesses and increasingly important to the economy. The value of UK internet retailing in 2011 was £25 billion (up from £21 billion in 2010). Internet sales growth averaged 15 per cent in 2011 and the sector represented 10 per cent of total retail spending over the 2010-2011 period. The growth of e-commerce and corresponding opportunities for increasing fraudulent behaviour should not be underestimated. Retailers need to be sure that as they seek to expand their businesses via e-commerce the customers they attract will be well protected. Retailers invest significant resources in protecting their customers. But, too often, the current law enforcement response to e-crime and fraud is inadequate. The BRC is calling for a dedicated national unit tasked to investigate and respond to the increasing levels of e-crime.

2.3. Engagement between the private sector and law enforcement agencies should be focused on finding the most effective way to achieve a better response to e-crime and fraud. The focus must be on finding ways in which the public and private sectors can work more effectively together to reduce the level of offending and to raise consumer confidence.

3. What e-crime is understood to be

3.1. The BRC uses the following ACPO definition of e-crime:

3.2. The use of networked computers or internet technology to commit or facilitate the commission of crime.

4. The effectiveness of current law enforcement and the potential impacts of proposed organisational change

4.1. Retailers are concerned that the law enforcement community has failed to keep pace with the rapidly expanding threat of e-crime. This situation may be exacerbated in the future by diminishing police resources and the introduction of locally elected police commissioners who may, in some cases consider business crime a low priority.
4.2. A number of BRC members have reported dissatisfaction with the level and quality of communications they receive from the police regarding e-crime. Retailers want far more clarity about what they can expect in terms of support and engagement throughout the process of prevention, detection and punishment of e-crime and fraud.

4.3. Retailers are generally dissatisfied with current police responses to e-crime and often do not report incidents. The reason for this is that e-crime is not considered to be a priority for many police forces. There are also concerns that national units such as the National Fraud Intelligence Bureau of Police Central e-Crime Unit (PCeU) do not have the resources or capacity to carry out further investigations.

4.4. Currently, there is no mechanism for retailers to report offences directly to Government/the law enforcement community via a centralised model for reporting. BRC members believe that this would be a valuable innovation which would permit more effective analysis of combined data from all sectors. It would also ensure greater awareness of the threat of e-crime to the UK and better inform the public, private and SME sector about potential threats to their businesses.

5. Gaps in the response to e-crime and how they should be addressed

5.1. The central concern of BRC members relates to the case acceptance criteria for each of the national agencies who deal with e-crime and fraud. Too often, retailers find themselves preparing detailed reports with the expectation that the relevant agency will accept the case. However, because of the opaque and diverse range of case acceptance criteria, retailers frequently find their case falls just short of the requirements for acceptance. When offences do not reach the acceptance criteria they need to be reported locally. Retailers therefore need clarity around where, in the first instance, offences should be reported and, if they must be reported locally, then it is vital that local operational capacity is available to progress an investigation adequately.

6. Options for addressing key emerging issues

6.1. The BRC has identified two distinct areas where challenges are likely to arise in the future. These are the increase in the use of mobile technology and the introduction of locally elected Police and Crime Commissioners.

6.2. The shift towards m-commerce will undoubtedly bring a number of challenges for the retail sector. The balance between providing flexibility for consumers versus protecting consumers and brands will become increasingly complex.

6.3. Some industry observers predict that mobile payments are likely to be an important trend for the future and fraudsters will certainly be looking to exploit this new channel. However, until adoption increases it is too early to tell exactly where the risk lies for merchants. What is clear, however, is that retailers will have to become increasingly aware of the end-to-end process involved in m-commerce and understand exactly where the risks and liability lie for any fraud that is carried out.

6.4. However, developments in electronic crime are fast paced and highly unpredictable. BRC members would like to see the Government and law enforcement community
issuing alerts on key and emerging threats to UK retail businesses and working with these businesses to ensure that the threats against them are clearly understood.

6.5. The British Retail Consortium is supportive of the introduction of elected PCCs. Retailers across the UK are keen to work with the police to build and support safer communities. We believe it is important that newly elected PCCs are supported in reconciling demands from the community and the needs of business when setting local policing priorities. It is also vitally important that candidates have opportunities to engage with a wide range of stakeholders before the elections and that, if necessary, Government should facilitate this.

6.6. It is also vital that new PCCs are encouraged to share best practice to ensure that crime is tackled consistently across England and Wales. This is especially true for retailers who operate national businesses and expect a standard response from the authorities no matter where a crime takes place. A consistent approach is vital when tackling e-crime and fraud.

7. The effectiveness of current initiatives to promote awareness of using the internet safely

7.1. Retailers invest heavily in anti-fraud systems and are continually seeking ways to safeguard themselves and their customers. However, more needs to be done to encourage consumers to keep their details safe. As e-commerce grows, the burden of educating customers must be spread further than the retail sector. There is a real role for the Government and the third sector to provide such support. BRC members would welcome a Government campaign aimed at helping consumers stay safe online.

7.2. Emphasis also needs to be placed on the public keeping their details safe offline as well – information collected in the real world is often used as the basis upon which virtual crimes are perpetrated. Though these precautions alone will not eliminate e-crime and fraud, they are part of a package of steps that can be taken to reduce the risk of crime.

8. BRC recommendations

8.1. In our 2011 report *The Futures of E-crime*, the BRC made six key recommendations around how to make the future of online sales more secure:

8.1.1. Improve law enforcement communication

8.1.1.1. Communication between law enforcement agencies and retailers should be improved so that each is clear about the evidence that is needed to support a successful investigation. Frequently law enforcement agencies waste time and resources by unnecessarily conducting investigative work which has already been undertaken by the retailer.

8.1.2. Clearly define law enforcement responsibilities

8.1.2.1. There needs to be more comprehensive information about which law enforcement agencies have responsibility for e-crime and online fraud, and the extent of those responsibilities. Such information should identify overlaps and intelligence gaps. There should also be greater transparency about the case acceptance criteria for each of these agencies.

8.1.3. Make effective use of intelligence
8.1.3.1. The National Fraud Intelligence Bureau should work with third party screening companies to enable more effective use of intelligence. There is a wealth of intelligence held by third party screening companies which could prevent offences occurring by enabling action before an offence is committed. This would reduce the number of victims and help provide reassurance to the public that they are being fully protected.

8.1.4. **Undertake a National Threat Assessment**

8.1.4.1. There should be a National Threat Assessment on Online Shopping. This will help to identify the extent of the need for an economic crime capability as part of the new National Crime Agency.

8.1.5. **Communicate with banks/card issuers**

8.1.5.1. There needs to be better communication and information exchanged between the bank and card issuers, and retailers to facilitate greater detection and prevention of e-crime and fraud.

8.1.6. **Identify effective practice**

8.1.6.1. Good practice guidance should be developed to enable retailers to reduce incidents of internal fraud and to increase the understanding of how to best protect consumers. Police forces should be encouraged to share best practice on how to engage with retailers and each other on detection and prevention of e-crime and fraud.

British Retail Consortium
August 2012
Written evidence submitted by the NSPCC [EC 03]

The internet has brought considerable benefits to children as well as society in general. Children use the internet as a source of information, learning, advice, and as a safe place to provide support to and communicate with each other. However, the internet and new technologies can also expose children and young people to harm, for example by exposing them to age-inappropriate material or illegal content, or to sexual predators or bullies.

There should be a continued focus to make the internet a safe environment for children to use for entertainment, socialising and learning. The NSPCC wants to see children able to use the online world to thrive and develop, and have the support, guidance and resilience to cope with the risks and dangers it can present.

1. The NSPCC welcomes the opportunity to provide written evidence to the Home Affairs Committee on the topic of e-Crime. E-crime affects people of all ages but children are particularly vulnerable to abuse and being exposed to inappropriate or illegal content. We know that children have access to and use the internet regularly. According to Ofcom 91% of 5-15 year olds have internet access at home and this age group spends an average on 90 minutes per day online. Our evidence will focus on the impact that the internet has on children and how children can be better protected from some of the risks and dangers that the internet poses to children.

2. What children and young people have told us about their views on using the internet safely through ChildLine

2.1 The NSPCC runs ChildLine, the UK’s free, 24-hour confidential helpline for children and young people. Trained counsellors provide comfort, support and advice about any problem to children over the phone or online. Last year, children called the ChildLine phone line 1.3 million times. In 2011/2012 the ChildLine website was visited by 1.9 million children and young people looking for help, information and advice. ChildLine’s website also provides children with a safe forum for peer-to-peer support on its message boards.

2.2 These contacts with children and young people provide a unique way for us to understand what issues they are concerned about. The NSPCC recently conducted an online survey of 851 children and young people aged 5-18 years on their use of the internet. The information we gathered in the survey gives us an up-to-date insight into the views of young people about the online world and internet safety.

---

1 Ofcom (2011) ‘Children and parents: media use and attitudes report’
2.3 In the survey children told us that:

- The best things about the internet are games and fun sites, the availability and variety of information and social networking sites.
- Over the last year children said they have started using the internet more safely, more for social networking and more for education.
- 69% of children said they access the internet via their mobile phone.
- 95% of children said they know how to protect themselves online (69% answered ‘Yes’, 26% answered ‘most of the time’).

2.4 However, the internet and new technologies can also expose children and young people to harm, for example by exposing them to age-inappropriate material or illegal content, or to sexual predators or bullies.

- Children told us that the worst things about the internet include bullying, access to inappropriate material and being contacted strangers.
- 41% of children said they have seen or read something that upset them online.

2.5 We also asked children their views on who should be responsible for online safety and how this can be best achieved:

- 63% thought that primary responsibility for ensuring online safety rested with themselves, followed by parents/carers, internet companies and teachers.
- 43% felt that parents / carers should choose what you can access depending on age.
- 56% thought that all illegal or inappropriate things should be blocked automatically.
- 42% said that they would be safer if parents or guardians blocked inappropriate content.

2.6 As part of the survey, children and young people gave qualitative information about their experiences online and some of their concerns. Comments from young people included:

“**You can literally access anything and sometimes you end up coming across things by mistake and once you get on them/see them they can become addictive even though you never intended to go on**”

“**It is way too easy nowadays for a child under 18 to click 'Yes I'm over 18' and view something they shouldn't.”**

2.7 Young people were pessimistic about whether anything could be done to prevent children accessing inappropriate materials online. However, the options that they considered that might be effective included better education about internet safety and blocking inappropriate material.

3. **NSPCC Sexting research**
3.1 Mobile technologies have created new issues for young people. One of these is sexting, which involves the exchange of sexual messages or images between peers. We recently commissioned an in-depth piece of research into sexting and the use of mobile technology by young people. This was a qualitative study in two London secondary schools which has greatly enhanced our understanding of this new issue. The research found that:

- The threat to young people comes mostly from peers, rather than strangers.
- Sexting is often coercive, linked to harassment, bullying and even violence.
- Girls are the most adversely affected by sexting.
- Technology amplifies the problem by allowing the creation, exchange, collection, ranking and display of images.
- Ever younger children are affected by sexting – year 8 (aged 12/13 years) children were worried, confused and in some cases upset by the sexual and sexting pressures they face.

3.2 The full report on sexting can be accessed here: http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting-research-report_wdf89269.pdf. The issue of self-generated images should be explored further if we are to want to address this issue effectively. It would be beneficial to understand the norms or pressures that influence young people to produce and share these images. It is also important to understand why young people are motivated to do this, and whether they knowingly engage in risk-taking behaviour, or engage in this behaviour without knowing about the potential long-term consequences. Young people should not be criminalised for sexting and we agree with the Association of Chief Police Officers (ACPO) that children and young people should not be prosecuted for sending sexually explicit pictures of themselves by text or email, colloquially known as ‘sexting’.

4. Key NSPCC policy calls to tackle e-crime

4.1 We believe that there are a number of ways to help protect children from being abused or bullied online and to protect them from accessing inappropriate, illegal or harmful material online. It is important that children know how to use the internet safely and that parents understand the risks that the internet can pose so that they are better able to support their children.

5. Raising awareness

---

2 Sexting has been defined as the “creating, sharing and forwarding sexually suggestive nude or nearly nude images” through mobile phones and the Internet.” see Lenhart, A. (2009) ‘Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging’. Pew Research Centre Report. http://pewresearch.org/assets/pdf/teens-and-sexting.pdf

5.1 There is a pressing need for more education and awareness raising of online risks for young people, with industry bearing a particular responsibility for funding and running such campaigns. In particular:

- Children and young people should learn about online safety and sex education as part of the school curriculum.
- Parents and teachers need support through more easily available online resources.
- All professionals working with children need support and training to help keep children safe online.
- Teenagers’ awareness of practices to reduce online risk from strangers indicates the success of e-safety campaigns. The focus of these campaigns now needs to shift towards reducing the risk from their peers.
- Results and good practice from awareness raising campaigns should be shared to ensure we learn from successful approaches.

6. Opt-in content filtering systems

6.1 The NSPCC supports the introduction of an opt-in content filtering system for all internet accounts in the UK, if necessary supported by Government regulation. This is where internet service providers (ISPs) should provide broadband connections into homes with filters already in place as the default setting to block access to adult content. Adults who wanted these filters removed from their service would have to inform ISP they wished to ‘opt in’ to these sites.

6.2 We consider that such a measure would help support parents to protect their children online, we recognise and emphasise that technical tools have to form part of a broader package of measures to address online safety issues. It is noticeable that in the Childline survey that we highlighted earlier in the evidence that 56% of young people thought that illegal or inappropriate material should be blocked automatically which indicates that young people are in favour of an opt in content filtering system. We supported the work and findings of the inquiry into Online Child Protection led by Claire Perry MP and welcome the Government consultation on this issue. We think that involving parents in the consultation process was welcome and we look forward to the response to this consultation from the Government.

7. Age verification

7.1 Providers of age sensitive services and products such as social networking sites should utilise robust age verification systems to protect children and young people from illegal activity.

7.2 Ultimately, what is needed is a framework for classifying content as adult or universal, and a widely used method of age verification so that users can prove they are old enough to access adult content. The mobile phone companies have already developed such a framework, as well as an age verification process, and so we know that this is achievable. Age verification systems are also already used by the online gambling industry. We accept that verifying the age of children under the age of 18 is more
difficult, but this should not be used as a reason to delay the widespread roll out of age verification for content which is clearly aimed at adults.

7.3 Independent reviews commissioned by both the current and previous governments both favoured the use of age verification processes (Letting Children be Children: the report of an independent review of the Commercialisation and Sexualisation of Childhood (2011); Safer Children in a Digital World, the Byron Review (2008)

8. Future research

8.1 We need to know more about the long-term consequences for children of online abuse. In order to understand what their needs are and how to provide the best treatment and support. In recognition of this, the NSPCC will be conducting research on the impact of online abuse on victims over 18 months, starting in October this year.

9. In conclusion

9.1 The internet brings huge benefits to children and society. However, this in turn also presents new risks and dangers to young people and work needs to continue to make the internet as safe as possible for children to use.

9.2 Young people’s views should also be taken into account as policy makers consider how to make the internet safer. Our contact with young people through ChildLine shows that the concerns that young people have about the internet and e-crime include issues like bullying and accessing inappropriate material which may be different to the concerns that adults have. We would welcome the opportunity for young people who have contacted us through our services and through ChildLine to give evidence to the Home Affairs Select Committee about their concerns and experiences in relation to e-crime.

About the NSPCC

The National Society for the Prevention of Cruelty to Children (NSPCC) aims to end cruelty to children in the UK by fighting for their rights, listening to them, helping them and making them safe.

We share our experience with governments and organisations working with children so together we improve the protection of children and we challenge those who will not learn and change. We campaign for better laws and we educate and inform the public to improve understanding about child abuse.

Our services include the NSPCC Helpline, for adults worried about a child, and ChildLine, the UK’s free, confidential helpline for children and young people.

NSPCC
August 2012
1) Introduction

The Home Affairs Select Committee announced the inquiry into e-Crime a week before the Information Society Alliance (EURIM) changed its name to the Digital Policy Alliance and appointed new Parliamentary and Industry Chairmen for its work stream on e-Crime and Cyber Security. The new group was not therefore in a position to assemble and agree a formal response. I retired as Secretary General of EURIM is September 2011 but remain a consultant and have assembled the submission below based on the published work of the studies which I organised over the period 2002 – 2011, plus two industry round tables earlier this year to plan the programme which is now being carried forward.


The six main papers http://www.eurim.org.uk/activities/e-crime/partpolicing.php covered:

- Separating Myth from Reality and Snake-Oil from Practicality (with an appendix on the scale and nature of computer assisted crime)
- Protecting the Vulnerable: (addressing the needs of small firms plus associated crime prevention material)
- Supplying the Skills for Justice: (addressing the needs of law enforcement and industry for investigatory and enforcement skills)
- Reducing Opportunities for e-Crime: (making it harder for criminals to identify and attack or impersonate Internet users and their systems)
- The Reporting of Cybercrime: (who should report what to whom? How should they do so? What should happen next?)
- Building Cybercommunities: Beating Cybercrime: The organisation of Internet policing

An update, “Tackling Crime and achieving confidence in the on-line world”, with “technical appendices”, covering specific areas http://www.eurim.org.uk/activities/ecrime/PIC07_AdvanceNote.pdf was produced for the 2007 Parliament and the Internet Conference. The Alliance subsequently assisted a further mapping exercise conducted by Professor Michael Levi, the results of which are due to be presented on 10th September 2012. The industry members of the Group have also organised a number of meetings this year to review progress in specific areas.

2) What e-crime is understood to be and how this affects crime recording

Little has changed since the first report from the EURIM – ippr study http://www.eurim.org.uk/activities/ecrime/partnerpolicing.pdf found three broad categories of activity being addressed under the umbrella of e-crime:

“Crimes made more efficient by using computers and the Internet to gain access to larger numbers of potential victims at lower cost/risk to the perpetrator. Examples include auction fraud, identity cloning, mis-selling and paedophilia.

Conventional criminal activities managed through use of electronic services. Examples include the use of email, mobiles, search engines, funds transfer et al in support of blackmail, fraud, extortion, drug or people trafficking.

Attacks on computer systems themselves. Examples include viruses and denial of service. Many of these look to victims like familiar crimes such as vandalism (e.g. defacing web sites) or criminal damage (e.g. causing a computer to crash).”
The fifth report from that study http://www.eurim.org.uk/activities/ecrime/reporting.pdf looked at the issues of reporting. Its recommendations finally bore fruit earlier this year when an on-line “one stop shop” website for reporting of possible e-crimes finally went live under the aegis of Action Fraud http://www.actionfraud.police.uk/report_fraud. No analyses have yet been published. Meanwhile victims still have no incentive to report unless they think action will be taken as a result. A consequence is that we have no reliable data on the scale and nature of e-crime: only extrapolations from anecdotal data in support of special pleading.

3) The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers

A consequence of the assumptions made when extrapolating from that which reported is that we have wildly differing claims as to what is “really” happening. Thus £27 billion in a report for Cabinet Office www.baesystems.com/cs/groups/public/documents/document/mdaw/mdm5/~edisp/baes_020885.pdf Is countered by a paper http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf which contracts criminal earnings in the $millions with security spend in the $billions.

Much, perhaps most, fraud is now linked to on-line activities, including to establish fictional identities or to obtain credentials (e.g. credit card details, account numbers and passwords) in the name of the victims. Even bigger figures are given for the cost of Fraud http://www.bbc.co.uk/news/uk-17548260. But much of this is again extrapolations, with estimates of the cost to HMRC and DWP (for example) going up or down in support of bids for powers and resources to address tax or benefit fraud.

Given the consequent conflict regarding the scale and nature of the threats, let alone whether proposals (e.g. on electronic identities or on data breach notification) help address them, it is not surprising that policy makers are confused.

4) The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

In its submission to the 2004 Home Office consultation paper on the Police Reform White Paper http://www.eurim.org.uk/activities/ecrime/policereform.pdf EURIM noted that “The total funding available to the NHTCU (including for supporting Computer Crime Units) is less than the individual electronic security and investigation budgets of most major High Street banks or of the main network or outsource suppliers.” The current budgets for the equivalent activities today of the Police Central e-Crime Unit, the Serious and Organised Crime Unit and the Economic Crime team of the City Police are many times those of the NHTCU. But the disparities remain. One bank alone is said to spend over £600 million a year securing its systems and taking action against those attempting to attack or defraud it and its customers. That may be exceptional but budgets of over £100 million are not unusual. More-over investigations under civil and contract law are said to earn UK-based private sector investigation operations (e.g. Computer Forensics, Transaction Tracing etc.) several £billion a year.

5) Whether there are any gaps in the response to e-crime and, if so, how they should be addressed

Since the demise of the Internet Crime Forum there has been no mechanism for bringing together the internet industries, law enforcement and relevant government departments to review what is happening, including progress with regard to the initiatives being planned or under way. The industry members of the Digital Policy Alliance are planning a quarterly review mechanism covering those initiatives with which they are already involved or which are seeking their support.

6) Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use

EURIM members supported the House of Lords enquiry into Personal Internet Safety and agreed with its findings http://www.publications.parliament.uk/pa/ld200607/ldselect/lddsctech/165/165i.pdf. A well received EURIM paper on Security by Design http://www.eurim.org.uk/activities/lg/1010-SbD_Full.pdf subsequently identified that a core point of leverage was to ensure that privacy and security are built into online systems at the design stage. The study team suggested that the Government’s main contribution should be as a more intelligent customer working with the relevant trade associations and professional and academic bodies. Among its other recommendations were that:
• Government should support the provision of shared audit services and databases of assessed products and services and help enable these services to be widely used at affordable cost: perhaps building on the work of The National Technical Authority for Information Assurance (CESG) and Centre for the Protection of National Infrastructure (CPNI).

• Professional bodies, such as The British Computer Society (BCS) and the Institution of Engineering and Technology (IET) and the UK chapters of the international associations, should review the standards of competence and integrity they expect of their members and co-operate to improve the quality of registers of current practitioners and reduce duplication of effort and cost.

• Trade associations should facilitate co-operation in the validation, cross-licensing and use of relevant audit tools and techniques so that these can be routinely used, including by small innovative firms, while fairly rewarding those who develop and maintain them.

• Accounting, actuarial and legal professional bodies should work with those for information and security and technology systems to produce shared practice notes and guidelines on assessing the value and security of systems to support better informed decisions on investment, insurance, responsibility and liability.

• Government, Industry, professional bodies and education and training providers (including those responsible for electronic warfare, law enforcement and service delivery) should co-operate in bringing the current confusion of standards, accreditations, qualifications and courses into line and fit for purpose.

• The Law Society should be asked to convene a cross-professional group to look at whether mass market systems without embedded SbyD are "fit for purpose" and to draft guidance for members who may be consulted on the consequences that might arise from legal action in this area.

7) The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples’ online behaviours for related public policy.

The National Audit Office report on “Staying Safe On-line” said that “Get Safe On-line” http://www.getsafeonline.org/ and “ThinkUKKnow” http://www.thinkuknow.co.uk/ “have achieved good value for their limited resources, using cost effective means to disseminate advice”. It also described the failure of Government departments to link to the sites and the risk of duplicated effort. Earlier this year a EURIM round table found that industry was confused by calls from government departments and agencies to support apparently duplicated efforts. They felt it important for Government to build on what was already understood and supported - such as Get Safe On-line and ThinkUKKnow.

It was also important to cross-fertilise initiatives, for example using the research commissioned by the National Fraud Authority into types of fraud http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/our-work/fraud-typologies?view=Binary and the experiences and needs of victims http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/our-work/better-deal-for-fraud-victims?view=Binary to help plan and inform on-line safety and awareness programmes, including those the staff of government departments and agencies. On September 13th The National Archive is hosting an all-day knowledge transfer workshop to that end, using those already large scale behaviour change (i.e. not just awareness) programmes in the private sector.

8) Conclusion

I would be pleased to provide follow up evidence on any of the above topics, either written or oral but might also wish to ask some of those working on the new Digital Policy Alliance programme in this area to help me update some of the answers.

Philip Virgo, Former Secretary General of EURIM, the Information Society Alliance
August 2012
1. What e-crime is understood to be and how this affects crime recording.

"E-crime" (and its near-synonym “cyber-crime”) is an ambiguous term that is used to mean, variously, crimes whose nature intrinsically requires the involvement of one or more computers. These offences fall within the remit of The Computer Misuse Act or what might be termed “traditional” crimes, such as fraud or extortion, where the use of a computer is a subsidiary element. Crimes such as “phishing”, where an email is used to obtain private information for fraudulent purposes, possibly in concert with a fraudulent website, are recent variants on a technique known in the security community as “social engineering” and among journalists as “blagging”.

For this reason, any reported statistics that purport to state the extent of, growth in, or damage caused by cyber crime or e-crime, should be regarded with considerable caution unless they are accompanied by full definitions of these terms, a breakdown of the incidents that fall into each sub-category and full details of how any losses have been calculated. It would be absurd, for example, to count every illegally downloaded music track as a lost sale at the retail price, just as it would be absurd to assume that everyone who buys a fake Rolex watch at a car boot sale was, in fact, intending to buy the real thing.

It is noticeable that the highest estimates of the prevalence of cyber crime or cyber attacks come from organisations whose business depends on the sales of technical countermeasures or whose budgets could be seen to depend on the degree of alarm about cyber security within government. So far as we are aware, there are no independently verified statistics about the extent of any individual categories of cyber crime.

It is likely that a great deal of e-crime goes unreported and unrecorded. Most internet users will receive several phishing emails, malicious attachments or attempted money-laundering or advance-fee-fraud approaches each week. In practice, most of these will be deleted. While there is a facility for recipients to forward such email to phishing@cityoflondon.police.uk with all the headers intact, it is unclear whether they are recorded or are followed up.
While the police are the natural first line responders for any crime, few of the UK’s 52 geographical police forces have the expertise and the resources to deal with large scale e-crime, especially on a national or international scale. While there are specialist units, the UK does not have a single authority for the reporting and investigation of e-crime. The present system appears to lack the coordination and process to reassure the citizen and deal with an industrial scale threat. Victims and suspected victims of e-crime would benefit from a greater awareness, more transparency and a single point of contact when seeking advice and incident reporting.

2. **The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers.**

The Cabinet Office has stated that government and the citizen are affected by rising levels of e-crime, at an estimated cost of £2.2bn and £3.1bn respectively. However it acknowledges that business bears the lion’s share of the cost of e-crime, at a total estimated cost of £21bn. These figures should be treated with caution for the reasons given earlier. It is clear, however that e-crime is a significant threat to UK citizens and businesses.

The rapid growth of eCommerce increases our dependency on the availability and integrity of the internet and our computer and communications infrastructure. While the extent of that dependency is easy to understand in terms of the potential impact of the denial or corruption of those services, it is more difficult to comprehend the true extent and nature of the threat. The source of the threat is extensive, ranging from the substantial resources of a nation state to the ingenuity of an inspired individual or the copycat behaviour of “script kiddies” (see glossary of terms, page 6). The nature of the threat is variable depending on the business and technology employed. However, in the modern industrial-size processing environments on which our economy depends, the integrity and availability of information will remain our principal vulnerability and the focus of any attack, while the vulnerabilities in systems controlling industrial plant and national infrastructure should not be overlooked.

Some threats have been researched, clearly defined and are understood by policy makers: such as online child exploitation covered by Child Exploitation and Online Protection Centre (CEOP) and understanding of online phishing, identity theft and crimes involving financial fraud by the Serious Organised Crime Agency (SOCA). However other areas like bullying online, defamation, invasion of privacy, particularly where social media are employed, are not so well defined or understood by policymakers.

The UK is experiencing a period of rapid social, economic, technical and political change which has engendered a more challenging and permissive environment. New technology enables a raft of traditional non-violent crimes to be committed in new ways, across borders and at scale previously unimagined. Policy makers must remain vigilant and maintain a far greater awareness of the potential and the vulnerability of our information society to malicious attack.

3. **The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change.**

Law enforcement in the UK struggles to address the magnitude of the task of combating e-crime. While there are some notable successes in combating serious online crime, anti-terrorism and espionage, the vast bulk of e-crime inevitably goes undetected or unreported and therefore unresolved. Policing is nearly non-existent at the more mundane levels that

---

most citizens experience e-crimes. This is very serious since it creates an impression that the police do not care about e-crime as it affects the ordinary citizen, particularly where the local response is close to non-existent or patchy at best. E-crime is now much more frequent than physical crime but is largely unrecorded and unresolved.

There is growing action to increase the percentage of police officers who have been trained to handle the burgeoning amount of digital evidence that is relevant to solving and successfully prosecuting all kinds of crime and this will increase the potential resources that could be used to address the more serious forms of e-crime. Resources will always be limited and the potential task faced by the police is huge. A single seizure following a referral by CEOP may contain hundreds of hard disks containing hundreds or thousands of gigabytes of data, dozens of mobile phones and other digital devices. These will need to be properly recorded, managed and controlled to preserve the evidence chain, and forensically examined as a matter of urgency as a child’s life may be at risk. Yet each phone examined and each email chain may lead to one or more addresses across the country that must be searched and where similar scale seizures may be required. Resources are soon stretched beyond breaking point.

Recent legislation has promised much but delivered little to aid the combating of e-crime. The Digital Economy Act 2012 has been widely perceived as supporting intellectual property interests and placing the onus of policing on the ISP, while potentially stifling creativity and offering little in the way of protection to the citizen with few barriers to those who wish to avoid the additional restrictions. In effect, the planned legislation has been designed to address the perceived terrorist and organised conventional crime threat, rather than addressing the wider e-crime threat which in an international context may not be within its powers. The election of Police and Crime Commissioners may affect the priority that local Chief Constables give to e-crime but will not increase the available resources. The Strategic Policing power that the Director General of the new National Crime Agency (NCA) will have is a further factor that will influence prioritisation by Chief Constables. The cyber resources of the NCA will be limited and will probably be directed against the highest priority targets.

While the devolved administrations of Scotland and Wales have introduced schemes to better coordinate the fight against e-crime little progress has been made on a UK scale. Proposed organisational change appears to offer little in the short term to combat the rapid growth in e-crime and provide greater clarity and reassurance to the citizen.

4. **Whether there are any gaps in the response to e-crime and, if so, how they should be addressed.**

The UK response to e-crime presently lacks the clarity and co-ordination seen elsewhere in the world. There needs to be greater clarity about the types of e-crime, with a clear definition and understanding of what is criminal, what is civil and where responsibility lies between business and law enforcement. There needs to be a simple well-coordinated process for reporting e-crime with clear lines of responsibility for recording, investigating and where necessary apprehending and prosecuting offenders. We need to move away from any presumption that the banks’ technology is secure and that customers who report fraudulent activity on their accounts are at fault or lying – there have been too many examples of weaknesses in banks’ security for it to be reasonable for the burden of proof to lie with the customer.

There are major problems in investigating crimes and pursuing criminals where the offence originates overseas. The UK does not have the same power to require foreign

---

2 [www.ecrimescotland.org.uk](http://www.ecrimescotland.org.uk)
3 [www.ecrimewales.com](http://www.ecrimewales.com)
4 [www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/default_en.asp](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/default_en.asp)
telecommunication service providers to provide communications and user data that can be required from UK-based companies. Attempts to negotiate bilateral agreements could easily founder because of understandable reluctance to open UK companies’ and citizens’ private data to scrutiny by agencies in countries that may have national interests that are not wholly aligned with the UK’s. Our growing dependency on technology and the magnitude of the threat demands a balance of legislative framework and administrative structures that protect the citizen while supporting e-business and innovation; promoting the UK as a safe well regulated environment in which business can thrive. To achieve this will require a more collaborative approach between the public and private sector in addressing the threat and the acquisition and development of new capabilities and skills by our regulators and law enforcement professionals.

5. **Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use.**

The massive and growing volumes of personal data held by social networking sites already expose individual users to significant risk. This data can be employed for a wide range of criminal purposes including identity theft, extortion, stalking, and defamation. Our society has embraced a more open and transparent attitude to free expression and personal information. While embracing this culture, individuals need to be aware of the risks they expose themselves to and the level of personal accountability and liability they must accept. They also need to understand the precautions they need to take to minimise their personal exposure to malicious attack. At the same time, all large databases of personal information need to be designed and managed in a way appropriate to the risk to citizens if the data is misused. In general, this should mean that such databases conform to GCHQ guidance for databases handling secret data and, where they do not, the data controller should carry liability for any misuse of the data.

In attempting to address this issue any legislative framework must be perceived as fair, setting the right balance between protecting an individual’s right to privacy and protecting society from irresponsible behaviour. The frequently employed analogy is that of the Highway Code, where a set of laws and best practices have been applied for the common good to protect the users of our roads and the individual must operate within those rules or face legal or commercial penalties. Perhaps we need to capitalise on aspects of this analogy in mounting a national education campaign to improve awareness of our vulnerability to e-crime and correctly assign accountability for protecting our personal data.

Nevertheless, it is essential to recognise the software vulnerabilities that expose computer users to risk, through the propagation of viruses and worms. The capability of seemingly benign attachments, such as pdf files or jpeg pictures to execute malicious code or website attacks such as SQL injection, all result from wholly avoidable mistakes by the developers of the faulty software. It is misguided and ineffective to try to change the natural way in which millions of computer users use their computers without creating sufficient incentive for software manufacturers to create products that do not expose their customers to such serious risks. We would like to see a timetable announced for introducing a Europe-wide measure of liability on manufacturers and importers of faulty software for the damage that these avoidable defects cause. This would build on the precedent set by the Consumer Protection Directive and similar UK legislation and should similarly allow a state-of-the-art defence.

6. **The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples’ online behaviours for related public policy.**
Current national initiatives appear to have been largely ineffective. The ‘Get safe online’ joint initiative between the government, law enforcement and leading businesses provides free, independent, user-friendly advice to users that allows them to use the internet confidently, safely and securely. While an excellent concept which was well implemented, it has not been widely promoted and there is little evidence that it has achieved significant engagement with the citizen or commerce. In any case, the guidance cannot address the real sources of vulnerability, as explained above.

BCS has produced the ‘Personal Data Guardianship Code’ and ‘Top Tips for Security’ to better protect personal data and improve computer and internet security. Whilst these have been deployed by a growing number of public and private sector organisations, the impact on the bulk of online users has been minimal.

To enable any new initiatives to succeed requires a co-ordinated, comprehensive, continuing education and change programme aimed at changing peoples’ online behaviours by increasing awareness and creating a safety conscious online society although, as we said earlier, the main source of risk is not, as widely claimed, unsafe behaviour by computer users but, rather, the design flaws and programming errors that make normal, reasonable behaviour unsafe.

Glossary of Terms and Acronyms

pdf – Portable Document Format – A standard for storing documents electronically in a form that is readable on most computer platforms using freely available reader software. File names often end with a ‘pdf’ file extension

jpeg – Joint Photographic Expert Group – A file format commonly used to electronically store graphical / photographic images. File names often end with a ‘jpg’ file extension

SQL injection – Structured Query Language. A common database language used to extract or display information held within a database. The injection element refers to a process whereby SQL commands can be inserted within user input strings, such as usernames, addresses or passwords, to exploit system weaknesses that in turn may allow access to the database or operating system in a way that effectively bypasses system security checks and safeguards.

Script kiddies - Usually fall into the category of younger or immature users who unfortunately can often be dangerous exploiters of security vulnerabilities in communications systems such as the Internet or the attached computer based systems. A typical script kiddy uses existing and frequently well known, easy-to-find techniques and programs or scripts to search for and exploit these vulnerabilities. These are often carried out randomly with little regard or perhaps even understanding of the potentially harmful consequences of such actions.

Engineering the Future
August 2012
Written evidence submitted by the
Foundation for Information Policy Research [EC 06]

The Foundation for Information Policy Research (FIPR) is an independent body that
studies the interaction between information technology and society. Its goal is to identify
technical developments with significant social impact, commission and undertake
research into public policy alternatives, and promote public understanding and dialogue
between technologists and policy-makers in the UK and Europe.

Last year, the Cabinet Office put its imprimatur on a marketing brochure from Detica
claiming that the UK was losing £27bn a year to cyber-crime. This was greeted with
widespread ridicule, whereupon Sir Mark Welland, then Chief Scientific Advisor at the
Ministry of Defence, asked us whether we could come up with more defensible numbers.
The result was “Measuring the Cost of Cybercrime”, a major study of what’s known and
what’s not known about cyber-crime, in the UK and internationally. This was published
in June at the Workshop on the Economics of Information Security, the leading peer-
reviewed academic conference in the field. The authors included two members of FIPR’s
advisory council (Ross Anderson and Richard Clayton) plus industry experts and
academics from the UK, the USA, Germany and the Netherlands.

We urge the Committee to read our report, which we include here by reference. Its main
points are summarised below.

1. The Committee first wants to know “what e-crime is understood to be and how
this affects crime recording”. The EU issued a Communication in 2007 where the
definition extended from traditional forms of crime such as fraud and forgery
committed over electronic networks, to crimes unique to electronic networks such
as service denial attacks. Our report teased this out into three categories. The first,
the traditional frauds now conducted electronically, includes tax fraud and welfare
fraud as its biggest components by value. The actual crimes here are mostly
unchanged from a generation ago, having to do with misrepresentation of
circumstances rather than any technical wizardry. The second, which we called
‘transitional cybercrime’, consists of crimes such as card fraud which existed
already but where the modus operandi has changed almost completely. The third,
the ‘pure’ cyber-crimes which did not exist before the Internet, range from
stranded-traveller and fake escrow scams to extortion via fake antivirus software.

2. The UK government takes a different view. VAT fraud is not seen as cyber-crime
despite the fact that all VAT returns are now filed electronically. Most seriously,
it has been policy since 2005 to tell fraud victims to report the fraud to their banks
first. This had the advantage, from the viewpoint of the Home Office, of making
fraud almost disappear as a recorded offence. Yet according to the British Crime
Survey UK households are more than twice as likely to be victims of fraud as of
‘traditional’ acquisitive crimes such as burglary and car theft; and according to

Eurostat’s 2010 survey, the UK ranks second behind Latvia for fraudulent payment card use and for losses caused by phishing/pharming.

3. The Committee’s second question is “the extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers”. In our experience, policymakers have a very poor understanding of cyber-crime; it is truly disturbing that the Cabinet Office was willing to co-brand the Detica brochure. Policy appears to be driven by scaremongering from GCHQ and the major suppliers who want the Government to spend ever more money on cyber-war preparations and on surveillance. As for the reality of the threats, we refer the Committee once more to our report.

4. The Committee’s third topic is “the effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change”. As our report makes clear, most of the global law-enforcement response to cybercrime is in the USA, and the rest of the world tends to free ride. The reasons are easy enough to understand and follow directly from cyber-crime’s global nature. Suppose a bad man in St Petersburg sends out a million phishing emails; as London is 1% of the Internet, the Commissioner of the Met will see 10,000 of them in his manor. He will be tempted to say “The FBI will have seen 200,000 of these; let them deal with it.” This classic public goods problem has made it very difficult to sustain cybercrime enforcement activities in the UK (and in most other countries). Things are made more complex in Britain by the capture of some crime-fighting resources by particular interests; for example, the banks pay most of the budget of the Dedicated Plastic Card and Cheque Unit, which is unsurprisingly perceived to be reluctant to investigate insider frauds seriously.

5. The Committee then asks “whether there are any gaps in the response to e-crime and, if so, how they should be addressed”. The top priority should be arresting cyber-criminals and putting them in jail. A lot of economic damage is done by a small number of gangs, yet many police forces throw up their hands and assume it’s all too difficult. Government has from time to time advocated that users take more care, or that people buy more anti-virus software. Yet these measures are ineffective, inefficient or both (see 7 below). A small additional effort in enforcement could yield much bigger returns. The Government should have given more of the cyber-security budget to the police, and less to GCHQ.

6. The Committee wants “options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use”. When bad things happen to citizens online, the material harm that results usually amounts to disputed transactions on the citizen’s bank or credit-card account. The biggest failing in the UK, of those which could be tackled by legislative means, is in bank regulation: specifically poor consumer protection, the incompetence and indifference of the FSA, and the fact the Financial Ombudsman Service is not up to dealing with the consequences of online and electronic fraud. The problem is not, as is sometimes said, a matter of the burden of proof. British banks found that they could get away with dumping much of the liability for fraud on the customer, by asserting in disputes that their system provided evidence that carried the day
on the balance of probabilities. That assertion is routinely accepted by the Ombudsman, and cannot easily be challenged by the customer for want of access to the banks’ systems for expert examination. The few customers with the stomach and resources to make a fight of it in the courts have often found that the bank fold, in order to avoid a precedent, but this has not helped the others. The banks’ greed was exacerbated by ministers’ decision to have people report fraud to the banks rather than the police, in order to minimise the fraud statistics. What Parliament might usefully do here is to hold hearings into the failures of the FSA and the Ombudsman. This could document the problems: citizens have suffered, and the UK has failed to meet its international obligations, in that the Payment Services Directive has not been adequately implemented.

7. The Committee finally asks about “the effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples’ online behaviours for related public policy”. A number of ministers have in the past claimed that Internet security could be promoted by raising public awareness. This view is also echoed by banks and software vendors – anyone who seeks to externalise liability for poorly designed systems. However the experience of system engineers is that poor design cannot be fixed by “blame and train” as the strategy is known. This strategy does not even work in environments such as aviation, where the users (pilots) are subject to mandatory and regular retraining and recertification; it is accepted that when safety hazards arise from poor cockpit design, the vendors must change the design rather than blaming pilots for the resulting accidents. It is even less likely to work in the world of consumer electronics and online services, where vendors no longer ship manuals with their products; users are expected to learn to use them through exploration. And while knowledgeable users might mitigate risks, vendors and system operators usually push the wrong way. For example, a good rule for naïve Internet users would be “if you get to a website by clicking on a link, don’t even think of entering a bank password there. If you want to do bank transactions, always go to your bank using a browser bookmark or by typing in the URL directly.” Yet bank marketing departments deluge customers with marketing emails which entreat them to click on links. Against this marketing barrage, government PR can achieve nothing. Legislators should merely ensure that if banks’ poorly-designed systems and risk-encouraging marketing programmes lead to customers losing money to phishing attacks, then the customers must be made good.

Ross Anderson FRS FREng
Professor of Security Engineering, Cambridge University
Chair, Foundation for Information Policy Research
Supplementary written evidence submitted by the
Foundation for Information Policy Research [EC 06a]

The Foundation for Information Policy Research (FIPR) is an independent body that
studies the interaction between information technology and society. Its goal is to identify
technical developments with significant social impact, commission and undertake
research into public policy alternatives, and promote public understanding and dialogue
between technologists and policy-makers in the UK and Europe.

We refer to the evidence I gave to your inquiry on December 20th and the subsequent
letter from the banks’ trade association Financial Fraud Action (FFA) to the Chairman,
the Right Honourable Keith Vaz MP, of January 29th this year. We would like to offer
the following observations and suggest a few questions for the FFA witness.

1. The FFA’s Ms Worobec objects to my remark to you that banks find it easy to
   blame customers for fraud, and often blame people as a routine matter, even when
   there is no evidence of negligence at all.
2. Ms Worobec claims that “the innocent victims of fraud can expect to receive full
   protection against any losses … it is only in circumstances where customers have
   been grossly negligent in protecting their PIN and card that they sustain any loss –
   which is a high threshold to overcome”.
3. This has been the line taken by the banking industry since at least 1994 but it is at
   variance with both the statistical evidence and the facts of many cases.
4. I was recently the expert witness for the defence of Mr W, a national of Sri Lanka
   who has been granted asylum in the UK. He disputed 38 transactions totalling
   £7861.85 on his account at the Nationwide. The Nationwide claimed that
   according to their records his card and PIN had been used so he must have been
   negligent or complicit. When he complained, he was arrested for fraud by false
   representation; the police believed the bank’s claim that fraud was not possible. I
   submitted an expert witness report showing how fraud was indeed possible and
   the case collapsed. My report described how the bank’s fraud analyst, on whom
   the police relied, had made more than one untrue statement. However Mr W has
   not been reimbursed; and he also lost his job as a consequence of being arrested.
   Honourable members might ask Mr Worobec whether she will get the Nationwide
   to refund and compensate Mr W. (I have his permission to send you the papers so
   long as his name is not published.)
5. My colleagues and I at Cambridge University Computer Lab have published most
   of the academic research on payment fraud over the last 20 years, so victims often
   find us when they search online and come to us with their stories. It is thankfully
   rare for a complaining cardholder to be actually prosecuted (Mr W is only the
   third we’ve come across in 18 years, and all three were acquitted). But it is
   extremely common for cardholders to be told “Our records show that your card
   and PIN were used, so you must have been negligent or complicit”.
6. The steady stream of victims is scientifically useful as it enables us to see how
   fraud tools and methods are developing. In the last five years we have seen and
documented a number of clever technical frauds that enable card data to be
captured from tampered terminals, and which even enable stolen cards to be used without knowledge of the PIN. The fact that a bank’s records claim that the correct PIN was used usually proves nothing of the sort. We have a series of technical papers and videos on fraud methods available online.

7. But the stream of victims is also frustrating and at times heart-rending, as there is often little we can do. Given current rules on legal aid and costs, and given that he does not speak good enough English to act as a litigant in person, Mr W seems to have little chance of getting his money back.

8. In general the victims who come to us having been given the brush-off by the banks and then by the Financial Ombudsman Service are disproportionately less white, less male and less middle-class than the population as a whole. They are precisely those people who are not in a position to take the bank to court.

9. The police are usually not much help either, especially since an ACPO decision in 2005 to get people to report fraud to their bank in the first instance rather than to the police. The House of Lords Science and Technology Committee examined ‘Personal Internet Security’ in 2008; their Lordships concluded that that decision had been the wrong one. Yet they could not get ministers to change their minds.

10. So the only really dependable fraud figures appear to be those from victim surveys, such as those conducted by the British Crime Survey and Eurostat, mentioned in our original submission to the committee. These suggest that about 4% of the population become fraud victims in any year and about half don’t get their money back. What’s more, the fear of online crime is real and it discourages many people from doing more things online, causing real harm to the economy.

11. Ms Worobec talks of the Financial Ombudsman Service (FOS). Yet this routinely finds in favour of the bank and against its customer, even when this flew in the face of both the law and the facts. FIPR made a submission to this effect to the review of the ombudsman that was conducted in 2008, before the ombudsman became the adjudicator required by the Payment Services Directive.

12. In that submission we included the full papers of a sadly typical case. Donald and Hazel Reddell were intimidated by Barclaycard into paying up £3000 that had been stolen from their account after their card was cloned – on the single occasion when they used it, namely in a Barclays Bank ATM! The bank showed its confidence in the Ombudsman by sending in the debt collectors in while that august body’s formalities were still in progress. Donald and Hazel appeared on “Tonight with Trevor McDonald”; I raised their case with a nonexecutive director of Barclays; I wrote to Bob Diamond after he made a speech saying the bank would have to rediscover its ethics; and I even put their case before the bank’s much-heralded Salz review. Yet despite a complete lack of evidence of any contributory negligence on their part, Barclays have still not given the Reddells their money back. I suggest that honourable members ask Ms Worobec when the Reddells will receive their refund. They can hardly be described as “having practically colluded with the fraudster”.

---

1 Bank fraud resource page, at http://www.cl.cam.ac.uk/~rja14/banksec.html
13. Ms Worobec also talks of the Payment Services Regulations 2009, which transpose the Payment Services Directive. I would like to draw the committee’s attention to article 59.2 of the Directive: “Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56.” The UK banking industry lobbied long and hard to get the word “necessarily” inserted into this text. I invite the committee to ask Ms Worobec why. Was it not so that UK banks could continue saying “Your card and PIN were used so you must have been negligent or complicit”?

14. Indeed as recently as a year ago, complainants to the Ombudsman reported that adjudicators there had not even heard of the Payment Services Regulations. We wrote to the Business Secretary Vince Cable (having discussed the matter with him while he was in opposition); his response was that he could do nothing as the ombudsman was “independent”, but that we might see the FSA who assumed the power to regulate her as of April 1st. We met with the FSA in January but learned that despite the ombudsman’s manifest failings they did not propose to do anything about her at all. Their line is that “the basis for Ombudsman decisions is what is fair and reasonable in all the circumstances of the case, rather than on a strict legal basis’. We disagree; if the ombudsman service does not have to follow the PSRs and the rest of the law (including the Human Rights Act) then the UK does not have an adequate transposition of the Payment Services Directive.

15. NGO efforts towards securing better financial consumer protection in the UK are now aimed at persuading the European Commission to remove the word “necessarily” from the Payment Services Directive in the current review of that legislation, and require explicitly that adjudicators act according to law. The committee might ask Ms Worobec whether UK banks will resist either or both of these changes.

16. Yet, despite its serious flaws, the Financial Ombudsman Service is finding against the bank in tens of thousands of cases per year. In 2012 there were 64,234 complaints to the ombudsman regarding banking and credit; 31% of these for current accounts and 54% of these for credit cards were found against the bank. The figures are not broken down enough to give the phantom withdrawal figures, but it is clear the banks’ system for refunding customers is not working.

17. So I am delighted to see Ms Worobec claim that 98% of fraud victims are reimbursed. I encourage the committee to ask her to provide the data from which this figure was derived. 98% of what, precisely?

18. The committee should be aware that when customers complain of transactions that are “chip and pin” (according to bank records) some banks see these simply as attempted frauds where the bank was the victim, not the cardholder, and record them under another heading. If customers are told to go away as “Our systems are

---

3 Financial Ombudsman Service, Annual review 2011/2; at http://www.financial-ombudsman.org.uk/publications/ar12/about.html#a2 and /deal.html#a5
secure so you must have been negligent or complicit”, a complaint may not be recorded at all. And a third example of non-recording is where the bank claims the dispute is purely between the cardholder and a merchant; the line is that where there was a “willing buyer and willing seller” the dispute does not concern them. A common example is where a British tourist in southern or eastern Europe gets a large card bill after eating in a restaurant where a waiter made a copy of their card and cashed it out in a nearby nightclub. UK banks then hide behind card scheme refund rules (which we understand even the FSA are not allowed to see). UK banks’ unwillingness to file chargebacks even for clearly fraudulent transactions encourages crime gangs in other countries. You might ask Ms Worobec whether eating tapas in Spain amounts to “having practically colluded with the fraudster”.

19. Ms Worobec claims that the burden of proof is on the bank, not the customer. This is somewhat disingenuous. The problem is that the fact that the banks assert that their system provides evidence that carries the day on the balance of probabilities. The ombudsman accepts this; it cannot easily be challenged by an ordinary customer for want of being able to get access to the banks’ systems for expert examination; and the courts do not usually order wholesale disclosure because there is so much of it that such an order would never be proportionate to an ordinary civil case. Where disclosure is ordered in a criminal matter (as in Mr W’s case), or where a fraud victim has the stomach and resources to make a fight of it in the courts, the banks fold. But ordinary fraud victims have little chance.

20. A matter that Ms Worobec failed to mention in her letter is that after colleagues and I revealed how stolen cards could be used by a criminal who did not know the PIN on Newsnight in February 2010, her colleague Melanie Johnson wrote to the University of Cambridge asking for one of our students’ Masters thesis to be removed from the web. The banks claimed it might help the bad guys, but this was nonsense. We had found that vulnerability after studying fraud patterns; the villains knew how to do it already. Ms Johnson appears to have simply been trying to defend the industry line that “Our systems are secure so you must be negligent or complicit”. We made her go away by pointing out to her that section 2 of the Fraud Act 2006 makes it an offence to dishonestly make a false representation to benefit yourself or another, or to put a third party at risk of loss. But perhaps many people who work in the banking industry still imagine that this law applies only to poor people like Mr W, and not to them.

Ross Anderson FRS FREng
Professor of Security Engineering, Cambridge University
Chair, Foundation for Information Policy Research
April 2013
1. Introduction

1.1 The internet has revolutionised society, and provided communities and business with great opportunities, and usage is set for a further prodigious increase over the next few years. The internet has encouraged and assisted new businesses by promoting innovation and the sharing of ideas, which has also boosted both the economy and job growth. It has allowed businesses to lower their costs, promote their brand and increase efficiency, and gives customers immeasurable choice and access to better, cheaper and more convenient services. The UK economy is very dependent on the internet as a basis for business and communications which is exemplified by the fact that in 2010, three quarters of UK consumers shopped online, spending nearly £60 billion, while 42% of all UK adults bank online.

1.2 These benefits, however, also provide opportunities for criminals. It allows them to exploit new ideas for fraud, identity theft, intellectual property theft and other forms of crime on an unprecedented scale through access to victims, data and commodities. They have done this by using a variety of cyber tools, techniques and online services. Criminals also utilise international boundaries to develop inventive and complex infrastructures that enable them to commit e-Crime. They have done this by using a variety of cyber tools, techniques and online services. Criminals are also adopting new technology to enhance their operational security or improve the efficiency of their operations.

1.3 The City of London Police (CoLP) has led the implementation of the National Fraud Intelligence Bureau (NFIB) since 2010. Prior to this, due to its unique relationships with the financial community in the City and the specialist fraud investigations skills and experience of its detectives, the City Police had been designated the National “Lead (Police) Force (NLF)” for fraud since 2003. The force receives additional funding from the Home Office to investigate serious and complex fraud and also to run the National Fraud Intelligence Bureau. These fraud functions come together as the Force’s Economic Crime Directorate (ECD) and are match funded by the City of London Corporation. Within policing, the force leads the Association of Chief Police Officers (ACPO) Economic Crime Portfolio and has been working with Chief Constables across the country over the passed 12 months to define a new model for recording and investigating fraud.

1.4 The NLF provides specialist advice on law enforcement dealing with often highly complicated and detailed criminality. Its objectives are to provide advice to all police forces, industry investigators and other law enforcement agencies to disseminate best practice, deliver training and act in an independent advisory capacity to other forces on request. The NLF provides a national investigative capacity to deal with all types of fraud (subject to agreed case acceptance criteria) and to assist other police forces in local investigations, and act as a single point of contact for anti-fraud advice.

1.5 As a result of the Fraud Review in 2006, the concept of the National Fraud Intelligence Bureau (NFIB) was created along with Action Fraud (the brand name of the National Fraud Reporting Centre launched and run by the National Fraud Authority) to help UK law enforcement agencies and their partners catch and disrupt criminals and to alert
communities to fraud threats. The NFIB gathers a large volume of information on suspected fraud from both public and private sector sources, much of which is not reported to, or made routinely accessible to the police. This is analysed and turned into intelligence such as the identification of the scale of fraudsters’ criminal activities. The intelligence is used to support law enforcement operations and also provide prevention advice to industry.

The Government’s National Security Strategy, published in 2010, ranked UK cyber security (of which e-Crime is an element) as a Tier 1 national security priority. As a result of this threat, the Government has committed £650m to the National Cyber Security Programme (NCSP). The City Police is one of a number of organisations that has received funding to help deliver this programme.

At the end of 2011, the Government published its Cyber Security Strategy, which illustrated how the UK will support the economy; protect national security and safeguard communities by building a secure and resilient digital environment.

What is e-Crime understood to be and how does this affect crime recording?

Types of e-Crime

2.1 The NFIB sees e-Crime (also variously described as internet crime, cyber crime and technology enabled crime) at two levels. At the simplest level, it is crime that exists only because of computer technology, for example hacking of email accounts, denial of service attacks and the production and deployment of malicious software (‘malware’). These offences are largely covered by the Computer Misuse Act 1990. Additionally, there is ‘electronic’ or cyber-enabled crime which can be described as the use of the internet to enable other crimes to be committed. The latter features particularly strongly within the NFIB’s remit as cyber enabled fraud. The most damaging cyber enabled frauds are those where the ease of communications through the internet has allowed an existing type of fraud to be attempted much more easily (for example, advanced fee or ‘419 letter’ frauds have developed and grown into fraud perpetrated by ‘phishing’ emails) or frauds exploiting the methods of genuine e-business such as ticketing fraud using bogus websites or online shopping fraud.

2.2 The bulk of e-Crime data that NFIB assesses is received from Action Fraud. Action Fraud records crime aligned to the Home Office Counting Rules for Fraud and Forgery, which includes crimes committed under the Computer Misuse Act 1990. However the reports it receives at present are limited to individual calls or reports from the public. Police forces still represent the bulk reporting for fraud and the service recognises that through the complex method of cyber crime and also because of jurisdictional issues, victims can receive a very different service depending on how or where they report their crime. Chief Constables have therefore agreed to a new business model lead by the City of London Police which will involve a national reporting and case allocation model to offer victims, a more professional service.

---

1 This type of fraud is a commonly attempted fraud whereby victims are asked to help transfer money out of another country – such as Iraq, South Africa or West Africa – by paying a fee in advance. In return, the victim is promised a percentage of the money that the fraudster says will be transferred.

2 Phishing is attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an email.
2.3 The recording of crime by the police is governed by the National Crime Recording Standard (NCRS) and the Home Office Counting Rules (HOCR). These set out the principles under which reports received from victims are recorded. Crime statistics that are recorded by police are based on a notifiable list of offences. The HOCR set out the classification groups into which offences are managed for statistical purposes.

2.4 However, individual police forces record crimes, particularly those enabled by technology, in different ways. This is because there is no such crime type as an ‘e-Crime’ formally defined in legislation. The use of a computer or other cyber technology is an enabler to the crime, and not a crime type in its own right. Therefore, it is not centrally recorded. This presents difficulties to the law enforcement community in assessing the scale and nature of the e-Crime threat.

2.5 The City of London Police is currently leading a programme of work to introduce Action Fraud reporting to all police forces in England and Wales. This will reduce some of the issues created by the lack of harmonisation that currently exists by creating a national call centre and on line facility to report fraud and cyber crime.

2.6 Over the coming months, Action Fraud, in partnership with the National Fraud Intelligence Bureau, will press ahead with the ‘roll out’ of an improved crime reporting capability with the support of all UK police forces. Within this programme is the development of an enhanced reporting method for businesses who are victims of cyber crime. This will ensure the police, through the NFIB, will have the capacity and capability to analyse all fraud and cyber crime data from one source, allowing for a much better understanding of the extent and nature of the e-Crime threat, and also provide for an enhanced service to victims.

2.7 New crime recording classifications have also been introduced by the Home Office to enable law enforcement agencies to capture specific cyber crime offences as laid out in the Computer Misuse Act (1990), but many crimes committed online are also prosecuted under existing legislation such as the Fraud Act (2006) or the Communications Act (2003).

3. What is the extent and the nature of the threats on which e-crime policy is based?

3.1 The significance of cyber criminals has grown in line with the development of online technology and the proliferation of electronically held data. Although it is difficult to estimate accurately the scale of losses to the UK economy as a result of e-Crime, one report puts the figure at £27 billion per year. Whatever the true cost, its reach is known to be extensive, affecting individuals, businesses and government institutions.

3.2 The Government has expressed the need for partnership with the private sector and academia to combat crime. The City of London Police enjoy close working relationships with the private sector (who are represented at the ACPO Economic Crime Portfolio meetings), through private data sharing agreements with the NFIB and also through industry funded police investigation units such as the Insurance and Cheque Fraud investigation units. There is a very clear common message concerning the co-ordination of engagement with the private sector across government. Whilst government policy has

---

3 The Cost of Cyber Crime, Detica (for The Cabinet Office), February 2011
provided a useful high level perspective, they have only resulted in bespoke isolated programmes of engagement and there are still no clearly identified ‘nodes’ for the formulation of policy, strategic forecasting and operational collaboration with the private sector on a national scale. Given this confused picture, there may be merit in an initial “mapping” exercise to identify the optimal mechanisms for engagement that already cut across different government departments.

3.3 The rapid pace of change in terms of technology and techniques used by cyber criminals make mitigating e-Crime a unique challenge. The ever-increasing amount of public and private data held online and the significant increase of internet usage, both privately and commercially, also allows for an increase in opportunities for criminals to exploit weaknesses. Further evidence of the threat posed was illustrated in a BBC report in July 20124, which shows fraudsters traded 12 million pieces of stolen personal information online between January and April 2012. The figure represents a threefold increase on 2010. Credit-checking company Experian, which produced the figures, said the increase was partly due to consumers having a growing number of online accounts. Consumers now have an average of 26 separate online logins but just five different passwords. Experian said many people were unaware their identity had been stolen until they were refused credit cards or phone contracts.

3.4 Attacks on businesses have risen markedly over the past year, with most UK based companies reporting malicious software infections. The 2010 Information Security Breaches Survey5 found that 90% of “large” organisations and 74% of “small” organisations had experienced a malicious security incident within the last year, including hacking, viruses, data theft and fraud.

3.5 In August 2011, Action Fraud launched the capability to record the enablers of fraud within fraud reporting. Since August to the end of the financial year, the NFIB have received a total of 49,037 fraud and internet crime reports from Action Fraud of which 45% were enabled6 online7. The highest volume of frauds reported to Action Fraud are concerned with online shopping and auctions, many of which are linked to organised crime. As an indication of the scale of only one aspect of e-Crime, over 25,000 “phishing” emails were forwarded by members of the public to the NFIB in less than one week during the Office of Fair Trading’s SCAMNESTY campaign. The majority of traditional frauds have been eclipsed by an internet enabled variant and all forms of legitimate internet commerce are vulnerable.

3.6 In considering the impact of e-Crime, the experience and effect on fraud victims has also to be considered. It is the experience of the City of London Police, that, a large number of victims have found fraud to be as harmful to them as violent crime, with tens of thousands of victims requiring medical intervention for psychological and physical stress related injury each year as a direct result of being defrauded.

5 The Information Security Breaches Survey 2010, PwC, April 2010
6 Reporting consists of both crime and information reporting; either by the nature of the offence i.e. online shopping and auction fraud, hacking, etc or as had been selected by the victim during the reporting process.
7 It is believed the true proportion of internet enabled fraud is higher than this as an accurate assessment depends on the victims correctly knowing, identifying and recording an enabler when reporting the crime
4. What is the effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and what are the potential impacts of proposed organisational change?

Are there any gaps in the response to e-crime and, if so, how should they be addressed?

**Effectiveness of current law enforcement and legislative capabilities**

4.1 The Serious and Organised Crime Agency (SOCA) and the Police Central e-Crime Unit (PCeU), hosted by the Metropolitan Police Service, undertake national e-Crime investigation and international joint investigation. The introduction of the new National Crime Agency (NCA) in 2013, which will replace SOCA, will continue with and expand on this role. Whilst the NCA is not yet operationally effective, the activity and linkage currently being initiated in the build up to the 2013 start date indicates that the operational response will be enhanced. Within the Shadow Command of the NCA, the City of London Police is member of the Economic Crime Coordination Board (ECCB) and also supports the three sub groups; Prevention, Intelligence and Enforcement. Early pathfinder joint operations have targeted criminals who are using the internet to facilitate money laundering and fraud.

4.2 The development of the partnership and coordinating functions of the National Cyber Crime Unit (NCCU) being established within the NCA will also provide a better-coordinated and standardised approach to the e-Crime threat. Many of the concerns and issues will, in part, be addressed by the unit, which draws together and adds to the work currently carried out by SOCA’s Cyber Unit and the PCeU.

4.3 The NCCU will focus its resources and skills on the most sophisticated areas of cyber crime, whilst supporting the NCA and wider law enforcement to take responsibility for tackling cyber-enabled crime. This principle of supporting law enforcement to take responsibility for tackling cyber-enabled crime will underpin the work of the NCCU. Cyber crime that is facilitated by the internet will continue to be investigated by the police.

4.4 The creation of the NCCU is a critical part of the Government’s wider National Cyber Security Programme (NCSP). It will consolidate the national law enforcement response to cyber crime into one unit. The NCCU will work closely with other partners to strengthen the UK’s overall response to e-Crime and ensure individuals and industry can utilise the opportunities presented by the internet. The NCCU is responsible for building the cyber capability of the NCA, across all four operational commands to manage high impact incidents of cyber and cyber-enabled crime.

4.5 An improved response to e-Crime can also be seen with the development of the Cyber Crime Threat Reduction Board (TRB), and of the Fraud Threat Reduction Board. These were established under the Government’s organised crime strategy\(^8\) which provides an operational context in which law enforcement and intelligence agencies can assess operational and intelligence activity against the ‘Stem, Strengthen and Safeguard’ themes of the Organised Crime Strategy. Both of these boards bring together representatives from key organisations to tackle specific issues within their remit, with a partnership-based approach. Whilst only recently established, both TRBs have already made significant

---

progress, assisted by the Threat Reduction Assurance Forum, which oversees and links
the work of both these boards, alongside the other seven TRBs responsible for their
respective crime types. The Threat Reduction Action Plans, identified and implemented
on a bespoke basis by both boards, ensures clarity, effectiveness and coordination for the
first time.

4.6 The ECCB has also produced several significant products in 2012 that have allowed a
greater understanding of the fraud threat, identified gaps in knowledge, and highlighted
key threats and risks. The intelligence gap analysis report and Strategic Threat
Assessment are now being used to inform the formulating of a Control Strategy to
manage economic crime nationally in a coordinated, effective and efficient way. These
products incorporate e-Crime.

4.7 A significant amount of e-Crime is also the responsibility of the NFIB, and the police
service as a whole. This has resource and capability implications as it lands alongside
other priorities as part of the general demand on policing. As an intelligence bureau, the
NFIB assesses the crimes it receives and then distributes them to the appropriate police
force or law enforcement agency for investigation; this can include PCeU and SOCA. In
reality, due to competing priorities, and the complexity and resources often required,
many police forces have difficulty in investigating e-Crime.9

4.8 Police forces across England and Wales are faced with a 20% reduction in national
funding in the period 2011-2014. This means that resources for targeting financial crime,
including much e-Crime are likely to be reduced in some regions. The City of London
Police has proposed a joint funding initiative with the Government and the banking sector
to fund additional police resources in the 10 ACPO police regions to investigate fraud, a
great proportion of which is now conducted through the internet. These resources would
complement the existing regional units that investigate organised crime and asset
recovery, and would also be closely aligned to the NCA build, including the specialist
PCeU resources. Initial first year funding has been approved by the Home Office,
resulting in intelligence officers being deployed in the 10 ACPO regions, to liaise with the
NFIB and assist further in identifying and understanding the associated regional fraud
threats. If further funding for an additional two years is approved, the intelligence officers
will work alongside new regional fraud enforcement teams to provide a comprehensive
intelligence-led response on a regional to national level.

4.9 Whilst individual police forces do provide a local response to e-Crime, this can be
uncoordinated and inconsistent, with many factors impacting on a variable policing
response from region to region. A project has been developed by PCeU to provide
additional regional resources that are effectively trained and equipped. The National e-
Crime Programme has delivered three pilot PCeU ‘hubs’ to address a lack of regional
focus. The ‘hubs’ enhance existing PCeU national operational capability to respond and
investigate cyber crime. The regional ‘hubs’ are based in the North West, East Midlands
and Yorkshire & the Humber. The ‘hubs’ were launched in February 2012 and are already
providing a fast and effective response. The PCeU ‘hubs’ have enhanced the local
policing response but further dedicated resources are still required to investigate the
underlying fraud offences.

4.10 The publication of the Strategic Policing Requirement (SPR) will support national co-
ordination and collaboration between police forces to respond to serious and cross-border

---

9 Due to investigative capacity, the difficulty in identifying the criminals behind e-Crime and the jurisdictional challenges of
dealing with criminals who are frequently located outside of the UK.
criminality. The SPR is also intended to ensure local policing plans account for cyber capability, and that local police forces can access the necessary specialist services required.

4.11 The introduction of Police and Crime Commissioners (PCCs) in late 2012 is intended to provide strong local representation, with the PCCs able to set the priorities for the police force within their force area, respond to the needs and demands of their communities more effectively, set the force budget and priorities, and hold the local Chief Officer to account for delivery and performance. With the extent of internet enabled crime effecting local communities, fraud and e-Crime should be seen as a serious and growing problem that needs to be addressed.

Gaps in response to e-Crime

4.12 The greatest challenge to an effective response by UK law enforcement agencies is the globalised nature of the threat. The most effective e-Crime groups are organisations that operate internationally, separating the component parts of their criminal enterprise across different countries for their utility and selecting jurisdictions for their permissiveness. There are challenges associated with delivering an effective solution in this environment due to the current varying international police response and enforcement. Differences in legislative, regulatory and practical arrangements for managing cyber security have potentially serious implications for all organisations. Whilst there is not necessarily the need for new international legislation, the promotion of standards and norms could help to strengthen the global threat mitigation architecture. Lessons can be learned from examining best practice in some sectors, and from the experiences of international partners. There is also a need to consider intelligence requirements through a global perspective.

4.13 In addressing the issue of e-Crime, the use of terminology needs to be clearer and more consistently used. There is a requirement for a common understanding of some of the general terms and an agreed list of the cyber crime techniques and tools, and the criminal infrastructure that poses the most risk to the UK. Both public and private sectors are the victims of cyber crime, but these are very wide categories and in the first instance prioritisation should be given to specific parts within these sectors that face the most risk and harm. A common understanding of terminology both in terms of threats and mitigation is a vital component of the UK response.

4.14 The current challenges in assessing the scale and nature of the UK e-Crime threat affects both the policy around e-Crime and the operational response to it\textsuperscript{10}. The impact of this is magnified by the tendency of cyber criminals to be highly adaptive and innovative. As a result, they can often be a few steps ahead of the law enforcement community’s ability to respond and are often in the process of exploiting the next criminal opportunity whilst law enforcement is trying to target the previous one. An effective law enforcement response is challenged further by the need for many industries to harness new technology to enable a more efficient and effective service. For example, new payment technologies and alternative banking mechanisms are rapidly evolving both in the UK and overseas. In a highly competitive market, the desire (and need) to generate new products rapidly makes delivering comprehensive security controls for these products a formidable challenge. Many organisations’ decision-making in relation to innovation is heavily driven by market forces and ease of use, with security concerns sometimes taking second place.

\textsuperscript{10} Response tends to be reactive rather than proactive and strategically targeted
4.15 Key risk areas that need to be prioritised for affirmative action include online tax and benefit/tax credit systems (Universal Credit) in the public sector, banking and payments and retail (the UK has the second largest in the world) for the private sector, and personal computers and devices used to access public and private sector systems. The means by which these systems are accessed are often the weak links which cyber criminals attack. Government has a key role to play in working with the private sector to mitigate the threat posed by these systems.

5. **How effective are current initiatives to promote awareness of using the internet safely and what are the implications of peoples’ online behaviours for related public policy?**

5.1 Whilst the UK has seen some recent initiatives to promote awareness of internet safety, it is clear that more needs to be done within this area.

5.2 Through its regional hubs, the PCEU have worked hard to mainstream cyber awareness, capacity and capability since its inception.

5.3 The National Fraud Authority (NFA) as part of the 'Shadow' NCA - ECCB Prevention Sub Group, plays a key national preventative role, in terms of reducing repeat victimisation by advising callers to Action Fraud. This service also plays a vital role for crime victims by offering reassurance and other advice through a bespoke service in partnership with Victim Support. The NFA also initiated and developed the “Devil’s in Your Detail” campaign, a joint initiative between the NFA and private sector organisations from the banking and telecoms industries. The campaign was video-driven and raised awareness of the importance of protecting personal information. The campaign reached over 4 million people through initiatives involving social media. Subsequent analysis of 4,000 people who watched the videos resulted in over 60% stating that they would take more steps to protect themselves from fraud.

6. **What are the options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use?**

6.1 The key to addressing e-Crime effectively is through greater collaboration, effective intelligence sharing, improved engagement with business, and a comprehensive awareness programme. Prevention is a vital theme that threads through all of these areas.

   **Greater Collaboration**

6.2 The Government’s National Cyber Security Strategy makes clear, and this is applicable to information security in general, that it is only through engagement between government, law enforcement and the private sector that the UK will become more resilient from attack, shaping an open and stable environment and developing our skills base. As criminals will target a range of industries it will be vital for all sectors to come together to share experiences and develop common strategies for addressing threats. A particular focus must lie in the security of the millions of personal information records held by both the public and private sector. There is a wealth of intelligence from various sources that this data is being targeted, stolen and traded as a commodity by criminal gangs. A comprehensive approach to the threat is required and collaboration is the key to success. Ad hoc groups promoting collaboration across the sectors do exist however, there is a
need for a stronger coordinated and formalised process across both the public and private sectors.

6.3 Collaboration can come in many forms, and the proposed City of London Police joint funding initiative to provide a national policing capability for fraud would provide a very effective specialist resource, aligned to the national law enforcement picture on a local, regional and national basis, and tackling an area of crime that has had limited resources. Whilst already supported by ACPO and all police chiefs, such a venture needs the financial support of the Government and the banking sector. Whilst the three-year pilot requires investment, the benefits to potential supporters, and the UK as a whole, are expected to be commensurately higher.

6.4 Criminals may target third parties, partner companies and other industries to access data. Advances in technology, such as the development of Cloud Computing, are also a source of new risk as well as opportunity. There is a wealth of expertise and information across all sectors in the UK that could greatly enhance protection against such wide-ranging threats, and collaboration must be co-ordinated across the wider private sector and government. To facilitate such comprehensive co-ordination and collaboration, there is a need for a point of focus around which stakeholders can rally.

 Improved intelligence sharing

6.5 An improved and more effective intelligence sharing protocol between law enforcement agencies would also have a great impact on preventing e-Crime. There is still much to be done in this area, and many agencies could collaborate and share their intelligence more effectively. The fact they are not is due to many reasons, including cost, culture, and their respective regulations, but none are insurmountable, and a greater effort is required from all agencies to share the intelligence they possess.

6.6 The National Fraud Intelligence Bureau (NFIB) is an example where intelligence sharing can lead to an effective preventative response. It disseminates products, including alerts, as a result of analysing intelligence provided by a range of organisations and industry sectors. This collaborative approach has been extended further with some also providing staff to work within the bureau. The NFIB works with private sector partners to close down criminally managed websites. Between January to April 2012, 261 websites were sent for suspension request. Between April to August 2012, 52 websites have been confirmed as suspended. In September 2012, 152 have been sent for suspension, with 143 being confirmed as suspended. Between January to August 2012, 248 telephone numbers were identified for suspension. The submission of bank account alerts was instigated from April 2012 and since this date 221 account details have been disseminated to the banking industry in 177 alerts. These are sent to the banking industry for intelligence purposes, and an example of the impact that these alerts provide was when a single customer had £70,000 prevented from being defrauded in September 2012. These timely actions are calculated to have saved the finance sector millions of pounds.

6.7 In May 2012 alone, the NFIB developed and disseminated 449 crime investigation packages, 28 tactical intelligence products and 112 alerts via a new partnership with the British Bankers Association. Whilst the work of the NFIB encompasses all areas of fraud, this approach should be expanded upon, and further supported, to encourage greater intelligence sharing of e-Crime related threats.
**Engagement with business**

6.8 The majority of victims of banking and plastic card fraud are protected by compensation from the finance and banking industry. Whilst much is done within this sector, the industry needs to continue to be supported and encouraged to provide enhanced and effective security to mitigate the ever-changing and often innovative exploitation by criminals and criminal finance. A robust coordinated approach by Government, law enforcement and business will ensure a better understanding of the true level of crime and raise public awareness to the threat and how to reduce it.

**Education**

6.9 The safe use of the internet requires a continuous, pervasive and constantly updated approach to education. This needs to be mainstreamed throughout an individual’s lifetime education. This would need to be on the scale of other public safety education, such as road safety and ‘stranger danger’, with initiatives seeking message adoption and understanding through all sectors of society. Although public awareness of “cyber enabled fraud” has greatly improved (for example the significant amount of education built into the school curriculum to manage children’s online behaviour by the Child Exploitation and Online Protection Centre), increasingly sophisticated attacks continue to target home computer users, and much more coordinated work is required.

*October 2012*
Written evidence submitted by EMC and RSA [EC 08]

Introduction

1. EMC welcomes the opportunity to contribute to the Home Affairs Select Committee’s important and timely enquiry into e-crime. This response begins with an executive summary followed by a short introduction to EMC, its global reach, and its expertise and capabilities in cyber security, before addressing the committee’s specific questions.

Executive Summary

- EMC is one of the world’s major IT infrastructure and services providers and has a significant presence in the cyber security market through its RSA division.
- The cyber-crime threat is sophisticated, complex, and rapidly evolving. There is a thriving criminal ecosystem that mirrors the legitimate IT market where criminals can freely buy and sell malicious software and services. This rapidly maturing online black market has led to a tenfold reduction in the cost to access cyber crime tools and services and an increase in the volume and sophistication of attacks seen.
- If the UK online environment is to remain safe for citizens, as well as the public and private sectors, there must be continued and increasing efforts to raise awareness of the extent and rapidly evolving nature of the e-crime threat, both in terms of the actors involved and the new threat vectors they are developing. Intelligence must also be shared and best practice spread in a two-way process involving both the public and private sector.
- In this era of tight budgets and rapidly evolving threats, new regulations stipulating particular technologies or practices to address cyber threats are not necessarily required, or indeed appropriate. Instead a dynamic, outcome based and technology neutral approach should be encouraged, requiring sectors to collaborate and individual organisations to conduct risk assessments and put appropriate controls in place that are commensurate with the identified risk. In this way organisations will be able to develop and maintain more flexible security programmes, processes, and technologies that can evolve ahead of – or at least alongside – the threat landscape.

About EMC and its security division RSA
2. EMC was founded in 1979 and is today one of the world’s major IT companies. It has annual turnover of around $20bn and employs over 54,000 people worldwide, including around 1,650 in the UK.

3. EMC is a global leader in enabling organisations in both the private and public sector transform their operations and deliver IT as a service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping organisations store, manage, protect and analyse one of their most valuable assets – information – in a more agile, trusted and cost-efficient way.

4. This journey to cloud computing supports improved information security because organisations are able to replace the disparate and piecemeal legacy IT systems that are so common today with centralised monitoring, management, compliance, and security solutions. In addition, security is being built into the information infrastructure that makes up the foundation for cloud computing including virtualisation and data storage platforms.

5. Another key priority for EMC is “big data” analytics, which refers to the ability to analyse and gain real time insights on vast data sets of unprecedented scale and formats gathered from various sources. EMC’s big data division Greenplum provides this capability to leading organisations including T-Mobile and Skype, enabling them to gain real time insights on their business and provide a better service to their customers. EMC is increasingly leveraging its expertise in big data to support information security by providing organisations with real-time access to the entirety of information relevant to the detection of security problems.

6. EMC’s security division, RSA, provides security, compliance and risk management solutions for organisations worldwide. RSA helps the world’s leading organisations succeed by solving their most complex and sensitive security challenges so they can safely benefit from the tremendous cost and productivity gains of digital technology and the internet.

7. RSA has been driving innovation in the information security industry for over 25 years. Today, RSA protects the identities of over 250 million people around the world, including, in the UK, the online banking customers of nine out the country’s top 10 retail banks, more than 800 public sector organisations, and 30 defence and aerospace companies. RSA’s technology can be found in BlackBerry devices, PlayStation games consoles, and checks more than 5 billion URLs per day for malicious activity.

Response to specific questions

- What e-crime is understood to be, and how this affects crime recording
8. To successfully defend against cyber security threats it is important to understand the actors involved better. The attackers can be categorised into three major classes of cyber adversaries: criminals, non-state actors, and nation states. Each has distinct motives and modus operandi but may, at times, collaborate if their goals align. For the purposes of the committee’s enquiry, this response focusses on the criminal element.

9. Whether loosely affiliated or tightly organised, cyber criminals are out to steal personal information for financial gain. This information can range from an individual’s credit card details and web or corporate logins, to an organisation’s highly confidential plans or data. Indeed the value of personal data to a cyber criminal is much higher than a credit card or bank account number alone. For example, the average selling price of a US credit card on the criminal black market is around $1.50. But when that card is sold with a full identity profile, the value can be up to ten times greater.

10. It is typical to see cyber criminals auctioning “on-demand” access to large numbers of infected computers under their control, and knowledge of “zero-day” exploits of previously unknown software vulnerabilities, on the black market to the highest bidder for use in automated cyber-attacks. Indeed criminal groups are able to purchase all manner of malicious software and services online, including “do-it-yourself” kits to create networks of compromised computers (“botnets”) that then can be used for the mass distribution of “malware” (malicious software) and benign “bulletproof hosting” environments from which to undertake their activities. Today’s malware is incredibly sophisticated — capable of sitting undetected on a user’s machine and stealing personal and financial data, taking over accounts, and sending spam emails to proliferate and infect other users.

11. Unfortunately, as the criminal ecosystem matures, the cost of entry for cyber criminals to access these capabilities continues to fall. Research published by RSA in June 2012 found that the rapidly maturing online black market, which mimics functions seen in the legitimate IT supply chain including manufacturing, purchasing, outsourcing, partnerships, development, sales, distribution, performance optimisation, and customer support, has led to a tenfold reduction in the prices being charged for malicious software and services.¹ In 2011, RSA found that roughly one in every 300 emails in circulation contained some element of “phishing”, whereby cyber

criminals attempt to acquire sensitive information by posing as a legitimate entity, with 50 per cent of these attacks focussed on financial institutions.²

12. Although the tools available to cyber criminals are becoming increasingly sophisticated, the preferred method by which they exploit these capabilities centres on people. Security professionals have long understood that IT users will click on links they should not and unwittingly install malware hidden through simple ruses. Security professionals have traditionally deployed multiple perimeter controls, such as anti-virus software, firewalls and intrusion detection systems, to help deal with this threat. This process may work well for generic attacks, but not for the most sophisticated malware or zero-day exploits. For example, the Zeus Trojan, the malware most widely used by criminals to target financial institutions, is detected less than 40 per cent of the time by anti-virus software.

13. Similarly, attackers are increasingly gathering intelligence on their targets, sometimes months in advance of an attack, using social media and other means to understand which individuals possess the assets they want, and crucially how to tailor, or “socially engineer”, their attacks to increase their likelihood of success. Indeed cyber attackers prefer using social engineering in this way because in so doing they are able to evade traditional perimeter controls more easily.

- The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers
- The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

14. The tripartite distinction to the cyber threat outlined above appears to be well understood by policy makers and is reflected in the UK National Cyber Security Strategy published in November 2011. However RSA’s experience dealing with both the public and private sectors suggests that, while recent policy initiatives such as last year’s National Cyber Security Strategy have advanced government’s understanding of the cyber threat and how best to respond to it, the private sector remains ahead in terms of understanding its scale and maturity, and implementing appropriate measures to deliver advanced security.

15. Research published by RSA’s Anti Fraud Command Centre (AFCC) in July 2012 found that the global volume of phishing attacks seen in the first half of 2012 had increased by 19 per cent compared with

the second half of 2011, costing organisations an estimated $687m in total losses. The UK was among the top 10 countries experiencing phishing attacks over this period.³

16. The AFCC, based in Herzliya, Israel, is one of the most advanced facilities in the world dedicated to fighting international cyber-crime. Established in 2005, the AFCC combines counter-intelligence, threat monitoring, and threat analysis capabilities to neutralise attempts by cyber criminals to steal money and information. Nearly 150 analysts work around the clock, 365 days a year at AFCC, protecting nearly 15,000 private and public sector customers in over 180 countries from cyber security threats and are able to shut down attacks in an industry-record time of five hours.

17. In the first seven years of its operation, AFCC shut down more than 500,000 cyber attacks. But in the first six months of 2012, AFCC shut down an additional 150,000 attacks, at a rate of 1,000 attacks per day. Clearly, the cyber threat is increasing significantly and it is now crucial for all sectors to recognise the dangers involved and respond.

18. If the UK online environment is to remain safe for citizens as well as the public and private sectors, there must be continued and increasing efforts to raise awareness of the extent and rapidly evolving nature of the e-crime threat, both in terms of the actors involved and the new threat vectors they are developing, among senior and mid-level policy makers. Intelligence must also be shared and best practice spread in a two-way process involving both the public and private sector.

19. One successful example of this from the United States is the Financial Services Information Sharing and Analysis Centre (FS-ISAC), which was formed in 1999 and brings together the public and private sector to enhance cooperation and information sharing to combat cyber and physical threats. It is entirely funded by its membership of over 4,200 organisations which include commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 30 trade associations representing the majority of the US financial services sector, and works closely with relevant federal, state, and local agencies. It acts as a trusted third party, providing anonymity to allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so that information that would normally not be shared, is able to be provided, thereby benefiting the whole of the sector.

20. In this era of tight budgets and rapidly evolving threats, new regulations stipulating particular technologies or practices to address cyber threats are not necessarily required, or indeed appropriate. Instead an outcome based, technology neutral approach should be encouraged, requiring sectors to collaborate and individual organisations to conduct risk assessments, and then put controls in place that are appropriate and commensurate with the identified risk.

21. It is necessary, however, for the government to start taking a more proactive approach to tackling e-crime, rather than the largely reactive structures currently in place. One notable exception is the highly successful Child Exploitation and Online Protection Centre which actively seeks to prevent the sexual abuse of children and catch those involved perpetrating these crimes. The government should consider expanding this pre-emptive policing framework to confront other forms of cyber crime head on.

22. The establishment of the National Crime Agency (NCA) next year provides an opportunity to put such pre-emptive structures in pace. As the government prepares for its formation, it must ensure that NCA’s remit, and the boundaries and inter-relationships with other agencies involved with e-crime, are well understood by all. Furthermore, it is imperative for the agencies currently involved in the response to e-crime to continue functioning at their optimum level throughout the transition process to prevent criminals taking advantage of any potential lapses in effectiveness or increased vulnerability.

- whether there are any gaps in the response to e-crime and, if so, how they should be addressed

23. In light of the increasing volume of attacks and rapid pace of change associated with the cyber threat, it is a given that organisations will be in a state of persistent, dynamic, and intelligent threat and disruption. In these circumstances the security dogmas of the past, which rely on an uncoordinated line up of static perimeter defences, can no longer be seen as adequate. Indeed many of the security technologies in common use today across the public and private sector, such as anti-virus software and firewalls, are no longer fit for purpose and offer diminished value in today’s world of advanced threats.

24. Security must evolve to a new more agile, risk-based, and contextual paradigm, that takes advantage of the latest advances such as cloud computing and big data analytics, and is able to meet the challenges posed by today’s dynamic threats and “hyper-extended” world where information is exchanged in more ways and more places than ever before, and people are using the same devices for their work and personal lives, all enabled by technologies such as smartphones and tablets, cloud computing, and social networking.

25. By doing this, organisations will be able to develop and maintain more flexible security programmes, processes, and technologies that can evolve ahead of – or at least alongside – the threat landscape – and not simply protect themselves against “known bad” threats.
• options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use

26. A key barrier hampering the response to e-crime is the fact that organisations that have been targeted by cyber criminals are often reluctant to admit this publicly. This is partly because many organisations fear that doing so will undermine their corporate reputation and the trust placed in them by their customers and stakeholders. Organisations also perceive that the Data Protection Act and other statutes hamper the sharing of effective actionable intelligence with partners, which as outlined above, can be one of the most effective means of combating cyber crime.

27. RSA recently gained first-hand experience of the importance of both these points, and in particular the importance of transparency and sharing information.

28. On 17 March 2011, RSA publicly disclosed that it had detected a targeted, socially engineered, cyber attack on the company’s systems and that certain information related to the RSA SecurID® product had been extracted. RSA immediately developed and published best practices and remediation steps, and proactively reached out to thousands of customers around the world across the public and private sectors to help them implement those steps. Furthermore, RSA worked with the appropriate government agencies and industry bodies in the United States, the United Kingdom and other territories to ensure broad communication of these best practices and remediation steps as well as information about the attack.

29. The attack on RSA has become a valuable lesson that has redoubled the company’s commitment to leading industry efforts to increase understanding of today’s advanced threats while also collaborating with a broader community of stakeholders to better prepare for and mitigate advanced cyber attacks.

30. To counter these challenges, RSA would urge policy makers to consider legislation providing a safe harbour or similar protections for organisations that voluntarily share sensitive threat information with the government and/or the extant industry information sharing and analysis infrastructure. Such an approach could help improve situational awareness and cyber readiness for many organisations while reducing serious concerns about legal risk. Policy makers should also consider the work being undertaken by the insurance industry to provide innovative means of addressing this issue.

31. In relation to the personal data held by social networking sites, as discussed above it is clear that the preferred method of exploitation for cyber attackers centres on people. With social engineering now the number one avenue of attack, the new security perimeter is in fact the human being.
32. In addition to reinforcing the need for better and increased efforts to share best practice and actionable intelligence on the latest threats and how they can be mitigated, this also demonstrates the need for a shift in corporate culture from the old IT security paradigms towards a more agile, risk-based, and contextual approach that is able to cope with the reality of today’s “hyper-extended” world described above.

- the effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples’ online behaviours for related public policy

33. EMC believes consumer education initiatives such as www.getsafeonline.org are crucial to combating e-crime by raising awareness and sharing the latest information on e-crime threat vectors, and how to combat them, as they evolve. EMC has been heavily involved in developing and driving similar initiatives in other countries, notably www.staysafeonline.org, the US equivalent of Get Safe Online, of which EMC was a founding member. The company’s global experience of such initiatives suggests their effectiveness is maximised when they are inclusive and involve the broadest possible range of public, private, and third sector partners. EMC would therefore encourage Get Safe Online to enable a broader range of stakeholders beyond the current list of established sponsors and partners to contribute to the initiative, including voluntary groups with established links into the youth sector such as The Prince’s Trust. Other private sector partners should also be encouraged to contribute via non-financial means such as by donating staff time and expertise.

34. Finally, the government should consider the tone and positioning of the messages communicated by such educational programmes. Ultimately, the aim should not be to frighten the public or make them think nothing can be done about the cyber threat, and thereby discourage them from enjoying the benefits of today’s digital world. Instead the goal should be to convey a simple and positive set of steps that both adults and children can follow to protect themselves, in a same way as was achieved by previous public information campaigns such as the “Green Cross Code” or “Clunk click Every Trip” campaigns to promote road safety. The US Stop.Think.Connect campaign, of which RSA is a founding partner, is a good example of attempting to educate the public on internet security with a clear and engaging set of messages. 

EMC/RSA
August 2012

4 http://www.staysafeonline.org/stop-think-connect/about
Written evidence submitted by the Communications Crime Strategy Group [EC 09]

1. The Communications Crime Strategy Group currently draws its membership from the following telecommunication companies:

   British Telecom
   Hutchinson 3G
   Vodafone
   EverythingEverywhere (Orange and T Mobile brands)
   Carphone Warehouse
   Phones 4U
   Cable Wireless Worldwide
   B Sky B
   Verizon Business
   O2 Telefonica
   Virgin Media

The Group objective is to set the strategic crime agenda for the industry member’s it represents and part of this strategy is to identify risks associated with e-crime.

**What E-Crime Is Understood To Be And How This Affects Crime Recording**

2. For the purpose of this submission e-crime is defined as crime that is committed by use of electronic means and incorporates the term cyber crime, those crimes which can only be committed through the use of cyber techniques, and cyber enabled crimes, those crimes which are escalated or assisted by the online electronic environment.

3. The telecommunication industry and its customers find major challenges in both the reporting and recording of crimes, to law enforcement, that fall under the e-crime umbrella. There is little, if any, knowledge at the front end of policing as to how such criminality should be addressed and recorded and invariably, because the perpetrators reside outside local police boundaries; all too often the response of front desk officers at police stations is to push the problem elsewhere under the guise that the “crime” needs to be reported where the crime took place. This approach often causes such crimes to go unreported.

4. 2011/2012 has seen the expansion of “Action Fraud” as a web site/call centre to which most types of fraud can be reported and whilst this is to be commended it still has some way to go to be a one stop shop for the reporting and recording of all types of e-crime related fraud. There is also recent evidence that some Police stations are now using this central reporting/recording process as a means of yet again passing victims of e-crime on and therefore not recording and/or investigating criminality that falls within this area.

It is our view that a clear distinction needs to be made between the recording for, statistical and intelligence purposes, for which Action Fraud was established and the role of police to investigate such criminality.

**The Extent And Nature Of The Threats On Which E-Crime Policy Is Based And How Well They Are Understood By Policy Makers**
5. The widespread expansion of the internet, along with the extensive uptake of new technologies, including smart devices such as mobile phones, has extended the reach of e-criminality beyond those technically capable criminals to a much wider audience due to the easy availability of tools and scripts that enable amateurs to proliferate crimes that previously were only available to the more technically capable.

The explosion of forums and other peer to peer areas where tools are available to download has seen the establishment of a culture and marketplace which is lacking in the normal oversight by authorities and law enforcement leading to an almost total lack of policing/regulation of what is in fact a public place.

This has left policy makers un-prepared and unable to have any real influence on how such places are operated/policied due to the nature and cross jurisdictional aspects that transcend national and international boundaries.

**The Effectiveness Of Current Law Enforcement And Legislative Capabilities, Including Local And Regional Capabilities And The Potential Impacts Of Proposed Organisational Change**

6. For all but the most serious crimes, terrorism and child exploitation, the effectiveness of law enforcement, both at the local and regional levels, to tackle everyday e-criminality is to say the lease patchy and in most cases non existent.

E-crime, by its very nature, transcends regional and national boundaries whilst often manifesting itself through local victims who are often left without any support at local level.

Where specialised e-crime units do exist they are often overstretched to the point that only the most pressing of cases can be properly investigated or pursued.

Legislation is often a barrier to such investigation due to its inadequacy to keep abreast of threats as well as lack of detailed understanding by both investigating officers and crown prosecutors of how the legislation can or should be applied.

Levels of proof are often set so high as to prevent any possibility of a successful prosecution of offenders, leaving law enforcement officers having to revert to lesser charges for more serious offences.

7. Whilst the impact of organisational changes can only be implied, based on the experience of changes to date, in day to day policing, there appears to be every likelihood that the services and resources necessary to keep abreast of the ever increasing threat from e-crime will be even more overstretched or non existent at all but the most senior regional or national level.

**Whether There Are Any Gaps In The Response To E-Crime And, If So, How They Should Be Addressed**

8. Response to e-crime needs to have cohesion at local, regional, national and international level. Currently the way e-crime is handled is often down to a “local” enthusiastic officers and the overall approach to e-crime lacks structure and any real strategic direction. Major forces such as the Metropolitan Police Service have high levels of expertise in tackling e-crime however this expertise is often centered on specialist units and is very quickly dissipated at regional and local levels of policing.
There is an obvious need to have some form of top down approach until such time the necessary levels of knowledge and expertise can be established at local levels.

9. The two areas that require better cohesion and consistency are that of reporting and investigating. In terms of reporting there needs to be clear direction at local police level as to how e-crime is reported and recorded and this needs to be in conjunction with the ability to extract local reporting/recording to a national level so as to enable an overall national picture to be better formed.

10. Investigation of e-crime requires specialist skills sets that are scarce at local level as are the necessary resources. Therefore there needs to be regional centres of expertise and resource that can act on behalf of local policing in this area with the ability if necessary to call on national resources when these are required. Whilst the victims of such crimes are often at the local level the perpetrators very rarely are.

**Options For Addressing Key Emerging Issues That Will Affect The Public Such As Liability Over Personal Computer Security, Personal Data Held By Social Networking Sites And Its Vulnerability To Criminal Use**

11. By their very nature the methods used by criminals to commit e-crime can change rapidly and new threats materialise with very little or no warning. Add to this mix the explosive take up, by the public and business, of modern communication devices giving a myriad of ways to access the internet and in so doing potentially increasing the risk of becoming victims of the e-criminal.

12. The importance of personal data and its role in the commission of e-crime is only just becoming recognised by the public and businesses, especially as it relates to access via a mobile device and it is imperative that this education process of the community continues.

13. The Government have a major role to play in ensuring that the right security messages, for the use of these devices and social network sites, are communicated to as wide a demographic as possible. This activity is a trinity of efforts between Government, Business and the Public and no one community can act on its own but there is a clear leadership role to be played by Government.

14. The Government, as advised by the expert agencies, needs to balance public awareness against letting criminals become aware of methodology and techniques that will enable the criminal to circumvent security or use systems in a way not intended. Greater exposure of sources of information for the user such as Get Safe On Line (www.getsafeonline.org) and Action Fraud (www.actionfraud.police.uk) and educational messages such as “The Devils In Your Details” (www.thedevilsinyourdetails.com) need to be built upon and constantly refreshed and targeted toward at risk groups.

15. Business has a role to ensure that customers are made aware of their responsibility in respect operation of devices and how best they can protect themselves. Whilst the public requirement is to have transparency in the security of the devices they operate this is not always practical or advisable and the public must be made aware of how they can and must assist in the war against this type of criminality. There are also major challenges when the business that are marketing devices, systems and applications are international in nature and have operations based outside UK jurisdiction.

16. ISPs and service providers are increasingly – and rightly – expected to do more to support their users to have safe online experiences and where reasonable remove criminal content from the services. However for e crime to be tackled effectively there needs to
be more effective mechanisms for members of the public to report interactions or content that they believe is criminal. Some mechanisms exist, for example in relation to images of child sexual abuse, or grooming, but it is not clear how a members of the public should report others such as online harassment or racist content. Some police forces have online report forms but these are lengthy and detailed and not applicable as they are written for victims, when often the person reporting has observed behavior and merely wants to report it for investigation. Police forces urgently need to review their online presence to check and assess whether the existing reporting mechanisms are fit for purpose on the age of social media and always on communications.

17. Finally the public MUST become more engaged to take on their responsibilities in securing what is in fact the front line and soft under-belly of e-criminality. Car security and home security are examples where the public are much more engaged than they are with mobile or static electronic devices and there may be lessons to be learned from such areas.

The Effectiveness Of Current Initiatives To Promote Awareness Of Using The Internet Safely And The Implications Of Peoples’ Online Behaviours For Related Public Policy

18. Recent campaigns such as “The Devils In Your Details” and “The Rough Guide To Staying Safe On Line” are examples of using modern communication channels to communicate out to the at risk demographics however, like anything in the fast and changing world of communication, messages quickly become stale and therefore less effective in getting the message out to those at risk. The other major challenge is the plethora of sites, some Government endorsed/funded and other put there by “concerned parties” that offer a confusing range of advice, some good, some bad and some downright confusing to the average user.

19. There is a clear need to rationalise from where the authorised messages come from. For example I have referred in paragraph 14 to 3 sites that have government backing there are also many others such as www.staysafeonline.org/ , www.saferinternet.org.uk/ and many more. This leads to a great deal of confusion in the mind of the public when seeking advice on this subject.

20. Peoples on line behaviour confirms that one size does NOT fit all. This presents many challenges to the trinity partnership when trying to engage on security and personal privacy issues as the late teen early twenties user is totally different in their risk taking than say the “silver surfer” however all are exposed to some degree to the same risk from e-crime.

Public Policy therefore MUST take on board the variance there is in personal behaviours of the on line community and tailor any awareness initiatives to reflect this, not an easy task!

J A Wraith MBE, Secretary
Communication Crime Strategy Group
August 2012
Written evidence submitted by Get Safe Online [EC 10]

I write to you in my capacity as Chief Executive of Get Safe Online.

As you are probably aware Get Safe Online is part of the Governments supported national major public-private sector initiative to raise awareness of online security. It is aimed at consumers and micro-businesses. It is a not-for-profit organisation and relies on contributions from private and public sector organisations. Current sponsors are: Cabinet Office, BIS, Home Office, Association of Chief Police Officers, The Serious Organised Crime Agency (SOCA), HSBC, Cable & Wireless, PayPal, Gumtree, VeriSign, Symantec, Ofcom and the National Fraud Authority (Action Fraud), Cable and Wireless, creative Virtual, Trend Micro and Microsoft. It has a board of directors and an active steering group that meets on a bi-monthly basis to set both the strategic and tactical aims and objectives for the initiative on an on-going basis.

The Get Safe Online initiative is largely Internet based. The website at (www.getsafeonline.org) is a one-stop-shop for reliable, independent and easily understood up-to-date information about online safety. It gives home users and small businesses the advice they need to use the Internet safely. It includes information on protecting your PC, yourself and your business as well as advice on topics such as Internet shopping, social networking sites, data theft and identity fraud.

The key messages of the initiative are that online sales and transactions are increasing at an incredible pace. Get Safe Online wants people to be able to continue using the Internet, enjoying the many benefits it has to offer, but also to be aware of the risks and take the steps necessary to protect themselves and their families online. In addition, people are increasingly opting to use the Internet when transacting or interacting with Government and it is important they are online safely and securely.

The Get Safe Online initiative provides a significant contribution to helping computer users and small businesses to take steps to protect themselves, not least because the Get Safe Online name and branding has significant potential and is easy for consumers to remember and therefore access. Government and the private sector will need to continue to work together to ensure that the potential of the Get Safe Online initiative is maximised.

Having outlined the work that Get Safe Online is doing in the area of Internet Security we would welcome the opportunity to give evidence to select committee and to suggest a number of our active partners are also well place to provide significant information to assist you.

Tony Neate, Chief Executive
Get Safe Online
August 2012
Given Symantec’s position as one of the world’s leaders in internet and information security we welcome the opportunity to provide the following information to the Committee in this important inquiry.

Executive Summary

- Today more than ever cyber security incidents have become headline news given the increasingly complex, sophisticated and organised nature of cybercrime which is determined as crime committed using a computer, network, or hardware device.
- Online attacks that were once conducted solely for fame and notoriety are now conducted by organised professionals motivated by economic gain.
- Information continues to be a key target with cyber criminals seeking access to data that can be used to conduct further online attacks or sold as a commodity on the underground economy.
- Cyber criminals tactics continue to evolve by increasing targeting mobile devices and social networks where users may be less aware of cyber security threats and where criminals may be able to avoid detection for as long as possible.
- Recognition by the UK Government that cyber incidents are a tier one level threat is welcomed but given the rapidly changing nature and extent of the threat addressing cyber security must remain a long term overarching public policy objective.
- Neither government, industry, law enforcement, individual citizens or Parliamentarian can solve the problem of cyber crime alone.
- Recognition by UK law enforcement of the need to work together and in partnership with industry is a key factor in the effective leadership by the UK in this area.
- But cyber crime is not just a problem for the UK but a global problem that requires a global approach. The involvement of UK law enforcement in international efforts is welcomed and should continue. The rise in data loss incidents has resulted in data protection issues become front page news.
- With personal data a valuable commodity for cyber criminals a sector wider data breach notification requirement should be introduced as part of the current review of the EU data protection legal framework.
- Technology has an important role to play in building and maintaining UK citizens online trust and confidence in the online world. But technology alone is not the answer.
- Raising awareness initiatives that increase understanding of the online threat environment and educate individuals of all ages how to protect their information and identity from the threat of cyber criminals must continue to be supported and funded by both government and industry.

What e-crime is understood to be and how this affects crime recording?

1. To answer this question it is necessary to first define what is meant by e-crime. For Symantec e-crime is included in the term cyber crime defined as any crime that is committed using a computer, network, or hardware device. The computer or device may be the agent, facilitator, or the target of the crime.

2. The broad range of cybercrime can be divided into two categories defined as either a single event or an ongoing series of events. An example of a single event would be where a victim might receive an e-mail containing what claims to be a link to known entity but in reality is a link to a hostile website controlled by a cyber criminal. Once the victim is sent to the hostile website the criminal is in control of a users machine and may take advantage of this control to commit fraud and/or steal individual’s information.

3. The second category is an on-going series of events. This can be where there are repeated interactions between the cyber criminal and the victim. For example, the target is contacted in an online chat room by someone who, over time, attempts to establish a relationship. Eventually, by using such use tools as social engineering, the criminal exploits the relationship to commit a crime.
4. When considering what is understood by the term e-crime it may be useful for the Committee to consider the definitions of cybercrime within the Council of Europe Cybercrime Treaty. The Treaty (which the UK government has ratified) is the most comprehensive legal instrument in the fight against cyber crime. In the Treaty cybercrime refers to a number of offences perpetrated using electronic means ranging from criminal activity against data to content and copyright infringement.

5. Overall however it should be remembered that e-crime is not a new phenomenon it is simply traditional crimes conducted using electronic means. For example fraud, harassment and theft has always existed but the new technology is simply the latest tool being used by criminals to conduct their illegal activities. Although clearly depending on what type of crimes are included in the term e-crime this will affect the way in which such crimes are recorded.

The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers

6. For the last eight years Symantec has produced its Internet Security Threat Report\(^1\) which provides an overview and analysis of worldwide internet threat activity and a review of known vulnerability and trends in areas such as phishing, botnets and spam. The report is based on the most comprehensive sources of internet threat data which is gathered from Symantec's Global Intelligence Network. Information on the key finding of the latest Internet Security Threat Report published in May 2012, can be found at the end of this submission.

7. The findings of the latest report indicate the extent and nature of current cyber threats with Symantec blocking more than 5.5 billion malicious attacks in 2011 which is an increase of more than 81% from the previous year. The number of unique malware identified also increased by 41%. The number of web attacks blocked per day also increased dramatically by 36% as cyber attacks become increasingly complex, sophisticated and targeted.

8. The report shows an increasingly high volumes of malware\(^2\) attacks along with an increase in sophisticated targeted attacks, where the user may not know they are being attacked due to the ability of the attacker to slip under the radar and evade detection, as well as a rise in advanced persistent threats and attacks on the infrastructure of the internet itself. Also identified was an increase in the number of data breaches of individuals and business information with more than 232.4 million identities worldwide exposed overall during 2011. Information remains a key target for cyber criminals who can use personal and business information to conduct other attacks through phishing or social engineering.

9. While the volume and sophistication of cyber attacks globally increased in 2011 the overall level of spam a popular vehicle for conducting cyber crime fell from 85.5% of all email in 2010 to 75.1% in 2011. This reduction is largely seen as due to law enforcement action which shut down Rustock a massive worldwide botnet responsible for sending out large amounts of spam.

10. Cyber criminals are not only continuing to use existing vulnerability but are also increasing in their use of social networks as a propagation vector for attacks. Due to social engineering techniques and the viral nature of social networks it is unfortunately much easier for threats to spread from one person to the next.

11. The growth in viruses and malware attacking mobile devices was also seen with the 2011 report being the first year that mobile malware presented a tangible threat to users. Attacks being seen included malware that sends premium SMS text messages from a users phone. This can earn the cyber criminal $9.99 for each text sent but unfortunately costs the victim dearly when their mobile phone bill arrives. As the take up of mobile phones and tablets continue to rise Symantec expects that cyber criminals will continue to explore ways to attack mobile devices and once they find something effective and money making they will exploit it ruthlessly.

12. Individuals continue to be a key target for cyber criminals according to the findings of the latest Norton Cybercrime Report published on 5\(^{th}\) September. One of the world’s largest

---

2 Malware is malicious computer code that can be classified into four main threat types: viruses, backdoors, worms and Trojans.
consumer cybercrime studies the report is based on the findings of a survey of more than 13,000 adults across 24 countries.

13. According to the report there are 556 million victims of cyber crime per year, which is more than the entire population of the European Union. In the UK it’s estimated that more than 12.5 million people fell victim to cybercrime in the past twelve months. The cost of cyber crime to the UK was £1.8 billion with an average cost of £144 per cybercrime victim. This means that cybercrime costs UK consumer more than a week’s worth of food for a family of four.

14. The 2012 report showed cyber criminals are targeting users of social networking and mobile devices which is further evidence of how the tactics of cyber criminals are changing based on the popularity of particular technologies and online platforms and networks. It is estimated that two thirds of adults use a mobile device to access the internet. One in five adults globally (21%) has been a victim of either social or mobile cyber crime. In the UK 30% of adults have fallen victim to cybercrime on social networking platforms. Although 63% of adults are accessing social network accounts and 24% access their bank accounts over free or unsecured Wi-Fi connections, around 53% of the adults surveyed were concerned about the security of these Wi-Fi connections.

15. While the 2012 report revealed that internet users are taking basic steps to protect themselves and their personal information, such as deleting suspicious emails and protecting their personal information online other precautions are still not being taken. For example 40% of UK adults don’t use complex passwords or change their passwords frequently. More than a third of adults do not check for the padlock symbol in the browser before entering sensitive personal information such a online banking details.

16. The recognition of the cyber threats as a tier one level threat to the UK in the National Security and Defence Strategy and the subsequent Cyber Security Strategy are seen by Symantec as evidence that policy makers recognise the extent and nature of the threat being faced in the UK. The focus on the economic and social impact of e-crime in the strategy document indicates an understanding of the impact of cyber threats not only to the ongoing resilience and stability of the internet but to the societal and economic stability of the UK. Going forward as the online threat environment continues to evolve there is a need to ensure policy makers up to date on the changing nature and extent of the threat to the UK from cyber crime and that cyber security remain a long term overarching public policy objective.

17. However, addressing cyber threats is not a responsibility of policy makers alone but a responsibility that is shared by all those using the Internet. The nature of the internet and IT technology is such that no single person can be held accountable and we all share a collective responsibility to protect ourselves and our customers whether they are businesses, users or citizens. Public and private sector co-operation and collaboration are a key factor to assisting not only the policy makers but also businesses and individuals to understand, assess and evaluate the level of seriousness of cyber incidents and their level of risk from cyber crime.

The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

18. The UK continues to be seen by Symantec as among the best placed countries in countering cybercrime; particularly in comparison to several other EU Member States. The UK’s Police e-Crime Unit and SOCA’s e-crime task force and the work of CPNI on cyber threats all play an important role in addressing cyber crime issues facing UK businesses, organisation and individuals.

19. A particular element of the effectiveness of UK law enforcement is the strong collaboration with the private sector. Coordination and cooperation between the public and private sector on addressing the spread of cyber crime are an important component to a cyber security strategy not only in the UK but also globally. The UK’s understanding that it is the private sector that has most knowledge about cyber threats and the need for law enforcement and industry to work together in collaboration, where appropriate, should be seen as a key success factor of the UK approach. However, it is also suggested that providing more training and resources to UK police, particularly at a local and regional level to fight cyber crime would be welcomed.
20. Given that the proposed organisational changes have not been implemented yet, it remains to be seen how the establishment of the National Crime Agency (NCA) will affect enforcement activities in this area. The proposals outlined by the Home Office in June 2011 point towards a continued focus on cyber crime as there currently is within SOCA and the Police e-Crime Unit. The creation of a National Cyber Crime Unit that it is understood will sit within the NCA is also welcomed as by Symantec. This step forward points the way forward for law enforcement capabilities already in place to be enhanced and bolstered going forward. Before the NCA is in place the emphasis in the Home Office document s on the importance of the continued cooperation between SOCA and the Police e-Crime Unit before the NCA is established is supported.

21. However, it should also be remembered that cyber crime is not just a local, regional or even national problem for the UK. Cyber crime is a global problem that requires a global approach particularly as threats and attacks can travel around the world at the click of a button. It is suggested that a move towards a more European wide approach by law enforcement to cybercrime issues could support and enhance the effectiveness of current UK efforts. Symantec has welcomed the recent announcement of the establishment of a Europol Cybercrime Centre. It is hoped that this initiative will continue to develop cooperation and coordination by law enforcement and that UK law enforcement will play a key role in supporting the Centre’s activities.

22. In terms of legislative capabilities the UK’s legal framework for addressing cyber crime is supported by Symantec. The Computer Misuse Act is a key legislative tool and provides the capability for prosecutions related to cyber crime offences. However, as explained above new forms of cyber crime emerge as new technologies develop. Given the rise in online threats since the Computer Misuse Act was last amended in 2007 it is suggested that the Committee should consider whether there are aspects of cyber crime seen today that remain unaddressed within UK’s legislation. For example while unauthorised access to a computer is criminalised under the CMA the actual theft of confidential information is not specifically addressed. In light of the significant number of UK citizens being affected by identity related online fraud it is suggested that a discussion is held on whether this offence should be specifically addressed within UK law. Also given the take up and use of cloud computing by both businesses and citizens increases a legislative gap currently exists in both UK and EU law given that the use and also misuse of computing resources delivered via the cloud without right is currently not covered within either UK or EU law. These offences are suggested as areas that the Committee could considered to ensure that the UK’s legislative capabilities are sufficient to address current and possible future online criminal activity. Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use.

23. As the Committee’s question highlights the findings of Symantec’s latest internet security threat report shows that information continues to be a key target for cyber criminals as well as a rise in the use of social networks by cyber criminals to conduct attacks. With hundreds of millions of people on social networking sites it is inevitable that online criminals would look to attack users there. However according to Symantec’s findings more than half of all attacks identified on social networking Web sites were related to malware hosted on compromised blogs or communication sites rather than the theft of information from social networking sites. It appears that a key threat from social networking is where a hyperlink for a compromised website is shared to a large number of users on a social network. Users then click on the link and are sent to the website where malware, which may include threats such as key loggers that seek access to personal information such as passwords, can then attack their machines.

24. Given the rise in data breaches and the threats seen to personal information Symantec has welcomed the European Commission review of the current European data protection legal framework in place in Europe since 1995 which is proposing the introduction of a sector wide data breach notification requirement. The review of the current Data Protection Directive (95/46) from which the UK Data Protection Act 1998 derives, is an opportunity to ensure the legal framework, first introduced in 1995 is appropriate and relevant today; particularly in an era where information has become the digital currency for users but, unfortunately, also a focus for e-crime.
25. Gaining and maintaining the trust and confidence of individuals that their information is protected and secured given the level of cybercrime being seen is a challenge that must be faced and addressed by organisations. Introducing a requirement to notify if data has been lost or stolen in the legal framework not only ensures data is fully protected throughout its lifecycle but also that users are informed if a serious incident occurs that may impact them, thus creating a sense of empowerment and individuals’ confidence in taking action if they want or need to. However, any breach requirements introduced needs to be appropriate and non burdensome to either organisations or citizens.

26. While ensuring the data protection legal framework in Europe is appropriate and relevant to the way information is being processed, accessed, shared and managed online, there is also a responsibly of individual users to ensure that they protect their information particularly when sharing personal information online.

27. The computer security industry has an important role to play in developing technological tools and solutions that are appropriate to deal with cyber threats and can help individuals to protect their identifies and information online. Symantec will continue to develop and offer solutions that enable users to put in place appropriate measures to protect their systems, networks and information. However it should be recognised that software companies cannot and should not be held responsible for what they do not effectively controls such as how a users may install, configure, use and update (or perhaps even chose not to update) security software. It is also difficult to see how a technology provider would measure the responsibly of the consumer in the way it has selected, installed, configured and users the software when ascertaining liability.

28. Factors that would need to be considered in measuring and determining possible liability would include whether the software being used by an individual user is fitness for the purpose it is being used. For example is the software being used in line with its intended purpose. Also whether the software being used is up to date and properly maintained by the user. For example a user may have decided to turn off the automatic software updates provided by the provider when the user configured the software. This is a decision that the provider of the software will not be aware of nevertheless this action could result in the user being left unprotected whilst online and suffer a cyber incident. In such a scenario the individual user may suffer cyber attack not because the software failed but because of a decision made by the user.

29. If such an approach was taken for it to be workable it is suggested that software vendors would need to be able to gain the necessary control over the way that users are using their technology. This could include the ability to monitor and control the behaviour and actions of people for example to ensure that the software, or tool, is being used for only the purpose for which it was supplied or sold. Moves in such a direction would not only raise political, privacy and legal questions but it is not clear whether such a evolution in the way in which technology interacts with users is a journey that users would be willing to embark on and potentially cover the costs of.

30. An approach where the liability burden is placed on the provider of software products alone could lead to a situation where companies would not be prepared to take liability for their products unless they can assume a level of control over the way it is being used in order to avoid or limit liability. This could lead providers to using more privacy invasive technological to provide the ability to monitor and control the behaviour and actions of users for example to ensure that the software is being used for only the purpose for which it was supplied or sold.

31. An approach along these lines could not only impact the control users have on their PC’s but could also stifle technological innovation and competition in the marketplace by promoting particular business models. A move towards more closed platforms or a situation where one dominant technology provider could dictate what can, or cannot, be installed on its system due to liability concerns may limit consumer choices to only sites or online content that are approved by PC providers based on a level of risk.

32. Moves towards liability in this area could not only raise political and legal questions but it is not clear whether such a evolution in the way in which technology is provided and interacts with users is a journey that users would be willing to embark on and potentially cover the costs of its development and implementation.
33. As the online threat environment continues to evolve and cyber criminals tactics adapt and change it is only right that we continue to consider options for addressing current as well as emerging issues. However in light of the rapid speed in which cyber threats and attacks evolve it is important that legislation and law makers should not try to run behind technology but rather support the market to develop the appropriate tools and solutions to current and future online threats. Also it is also important that users continue to be educated about online threats and understand the value of their personal data and the importance of having protection measures in place that are appropriate to their online activities.

The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples’ online behaviours for related public policy

34. Having appropriate technological solutions and tools in place can support citizens to have the confidence that their activities and information and identity online are being protected. However, Symantec believes that technology alone is not enough to address the online security challenges we all face today. An effective cyber security approach is one that combines appropriate technology, the development of policies, procedures particularly for reporting, responding and recording cyber incidents and raising awareness initiatives to ensure people have the necessary skills and knowledge to protect themselves from cyber criminals.

35. Symantec continues to be a supporter of initiatives around the world that promote awareness of internet security and safety issues to different online users from children to silver surfers. In the UK Symantec has been a long term supporter of Get Safe Online the government-industry campaign aimed at raising greater awareness amongst citizens and small businesses of the importance of online security. We are also members of the UK Council for Child Online Safety which is another example of how industry and government are working in partnership to increase understanding of online safety by both children and parents.

36. At a time when public and private sector organisations continue to look to online platforms and networks to interact and provide goods and services directly to citizens, it is important that internet security and safety remains on the public policy agenda. Initiative and activities that can raise awareness of the online threat environment and the importance of online security and safety have a key role to play not only in protecting individuals information online but also creating greater trust and confidence of internet technology. This will remain important if we are to ensure UK citizens can gain from the full opportunity and advantages offered by the internet and have confidence to enjoy the connected world safely and securely.

37. As mentioned earlier in this submission addressing cyber crime threat facing the UK is not something that industry, government, individuals or law enforcement can do alone. Users also have a responsibility to protect themselves by installing and using available internet products and tools effectively to ensure they remain secure. Education on online security and activities that raise awareness will continue to be vital to ensuring users are aware of not only the constantly evolving online threat environment but also what they can do to be safe and secure online.

38. While the current economic climate presents many resources challenges, it is important to continue to invest in ensuring individuals are aware of cyber security issues if the full social and economic opportunities and benefits offered by online networks and platforms are to be fully realised.

Symantec is a world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. Further information can be found at www.symantec.com. Symantec appreciates this opportunity to submit comments to the House of Commons Home Affairs Select Committee.

Symantec
October 2012
2011 IN NUMBERS

5.5 Billion
TOTAL ATTACKS BLOCKED IN 2011

- WEB ATTACKS BLOCKED PER DAY: 4,595
- VS. 3 BILLION IN 2010

- ESTIMATED GLOBAL SPAM PER DAY: 62 Billion in 2010, 42 Billion in 2011

- 1 MILLION IDENTITIES EXPOSED PER BREACH

- 1 IN 299 OVERALL PHISHING RATE
8 NEW ZERO-DAY VULNERABILITIES

4 MON 5 TUE LAUNCH DAY

403 MILLION UNIQUE VARIANTS OF MALWARE VS. 286 MILLION IN 2010

OVERALL SPAM RATE

2010 86%

2011 75%

NEW MOBILE VULNERABILITIES

2010 163

2011 315

OVERALL EMAIL VIRUS RATE 1 IN 239

55,294 UNIQUE MALICIOUS WEB DOMAINS VS. 42,926 IN 2010
Introduction

1. Local Authority Trading Standards Services (LATSS) enforce a wide range of consumer protection legislation across the UK. In the past this has been focussed on the traditional 'high street' where a physical premise could be visited and problems could be addressed in a much more tangible way. However, the internet has brought a whole new market place to consumers in the UK which has led to Trading Standards having to adopt new and innovative approaches to ensuring adequate protection for consumers carrying out their transactions online. As more and more consumers and businesses now routinely use technology (be that internet, e-mail or mobile/smart phones), Trading Standards faces further challenges in ensuring internet scams are properly tackled.

2. Trading Standards has a vital role to play in an overall strategy of e-crime enforcement. The security and integrity of the internet is key to the future economic success of the UK. Consumers need to feel they are adequately protected when carrying out their business online and equally, businesses need to be confident that rogue traders operating online are robustly tackled. Trading Standards takes the leading role in ensuring both these priorities are met and welcomes the opportunity to submit written evidence in relation to this inquiry.

What e-crime is understood to be and how this affects crime recording

3. The terms e-crime and cyber crime are often used interchangeably but are, broadly speaking, one and the same. The ACPO definition of e-crime is; “The use of networked computers or internet technology to commit or facilitate the commission of crime”. This is a perfectly reasonable definition but can cover a wide range of offending and there is often a lack of clarity as to the types of criminality that fall within that definition. Indeed, there is (in law) no such crime as an ‘e-crime’. This in itself can lead to problems in the effective reporting and recording of e-crime, as outlined later in this section.

4. The UK Cyber Security Strategy and previous discussions on the subject of e-crime have tended to focus, quite reasonably, on the higher level criminality such as hacking, Distributed Denial of Service (DDoS) attacks, cyber terrorism and large scale data/identity theft. However, in relation to consumer and business impact, there are a number of areas that whilst individually may be perceived as low level criminality, they can often have a disproportionate effect on the individuals concerned. These are often crimes that are not specifically dependant on technology to facilitate the crime, as would be the case for DDoS for example. However, the proliferation of technology has made the commission of the offences far easier and allowed the offenders to target a much wider audience than they would previously
been able to using ‘traditional’ methods. For example, the sale of counterfeit goods or websites set up to encourage consumers (and businesses) to part with their money without the product or service ultimately being provided. In terms of the National Intelligence Model (NIM) much of this would appear at first glance to be Level 1 criminality. However, when the scale of offending is assessed it can quite often become apparent that this in fact Level 2 (and in some cases Level 3) criminality.

5. In relation to the recording of e-crime, in practice the ACPO definition and most other definitions fail to provide for the successful recording of all instances of e-crime. This is primarily because the e-crime element is often a sub-element of the actual mischief of the crime. For example, a trader using a website to commit some sort of advance fee fraud might be classified as a fraud offence, when the principal mechanism to facilitate the crime is the internet. Furthermore, there is a proliferation of mechanisms by which consumers and businesses can report/record instances of e-crime. This in itself leads to an inaccurate picture as to the true scale of e-crime (see paragraph 16).

The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers

6. Broadly speaking, Central Government would appear to have a good understanding of the higher level threats posed by e-crime. However, there is probably less of an understanding of the threats posed directly to consumers and businesses when going about their normal day to day business, for example; websites offering fake job opportunities, companies offering to provide a service with up front fees that then fail to deliver the service (advance fee fraud) and websites selling counterfeit, dangerous and/or illicit products. The Federation of Small Businesses believes e-crime is having a serious detrimental impact on their economic success.

7. The creation of the National Trading Standards eCrime Centre (NTSeCC) (see paragraph 15) has gone some way to begin to address this issue. However, there still remains a lack of recognition amongst policy makers as to how that may fit within an overall approach to tackling e-crime. The priority thus far, as one would expect, has been tackling the high level threats to national security. From a local policing perspective, the policy has tended towards tackling the spread of child pornography. As a consequence, the very real threat from general scams that are targeted at UK consumers has tended to be poorly understood. Anecdotal evidence suggests that, what appears to be relatively low-level criminality can have a disproportionate impact on those individuals affected. To someone on a relatively low income, losing £100 through some form of internet scam could be extremely detrimental to their well-being. As an economy we are increasingly reliant on e-commerce so policy makers need to fully understand the impact of this type of criminality and the detrimental effect it has in creating a trusted online environment.

8. As outlined above, policies are often considered and devised based upon serious and organised criminality (e.g. Home Office Guidance and Implementation of RIPA Notice for use with Facebook, Charles Miller April 2010 – which focused primarily on SOCA/Police access to Facebook). Much more detailed consideration needs to be given to the impact e-crime has at Level 1, particularly from a Trading Standards perspective as this often forms part of much wider Level 2 and Level 3 criminality. If one considers the Home Office guidance referred to above, the process was considered and is only relevant for SOCA/Police, as a result the disclosure process can only be accessed by SOCA/Police Single Points of Contact (SPoC). Even then
the disclosure process does not go far enough to assist with localised law enforcement issues faced by Trading Standards.

9. Purely from a Trading Standards viewpoint current legislation in relation to e-crime is often a case of applying square pegs to round holes. For example, obtaining disclosure from a hosting company should ordinarily be a straightforward Data Protection Act request. However, quite frequently hosting companies will refuse on the grounds the information is telecommunications data. Another example would include obtaining disclosure from social networking sites, for example Facebook, as referred to previously. The inability of regional law enforcement officers to obtain data pertinent to a Facebook account, whereby the account holder involved in criminality has closed privacy settings, is in effect giving the criminal fraternity an open passport to trade illegally.

10. These examples highlight the gaps between policy makers and law enforcement agencies which have a duty to enforce e-crime at Level 1. Unfortunately, the difficulties posed by these gaps often result in little or no action being taken to identify and apprehend individuals involved in e-crime, let alone anyone connected to organised gangs. Furthermore, this fundamental lack of enforcement ability at Level 1 fails to provide the information necessary to deliver the intelligence building blocks which are required to carry out successful enforcement at Level 2 and Level 3.

The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

11. Recent organisational changes would appear to have been successful in having an impact in tackling the serious, national e-crime threats that we are faced with. The creation of PCeU, SOCA Cyber and others is certainly a step in the right direction. Clearly, it remains to be seen what impact the creation of the National Crime Agency (and in turn the National Cyber Crime Unit) will have in tackling e-crime.

12. In respect of Trading Standards, changes to consumer protection enforcement that have led to the creation of NTSeCC are a welcome move in recognising the importance of tackling all forms of e-crime and not just those at a high or serious organised crime level. However, there still remain some fundamental issues which need to be tackled:

a. Resource issues/training: hindering the appropriate investigation into e-crime, impacting on appropriately trained staff and the ability to keep up to date with technology and the ever changing techniques of the e-criminal.

b. Localised political agendas: the level of e-crime enforcement within Trading Standards at a local level is very much at the discretion of local political priorities and their views of the requirements of the communities they represent. For example, a rural local authority may have more interest in animal feed enforcement than investigating intellectual property crime on the internet. This factor has even more impact given the public sector cuts in recent times which have forced local authorities to review their priorities which inevitably has removed resource from enforcement functions.

c. Central Government: the continued need for policy development to prioritise local/regional law enforcement. This often results in the tools (resource & legislation) not being provided for law enforcement officers to deal with e-crime effectively. The
recent changes to RIPA are a point in case whereby LATSS staff will now have to seek magistrates’ approval in order to gain access to subscriber data. Although it is recognised why policy makers sought to restrict isolated disproportionate use of RIPA, for Trading Standards enforcement, this appears to be a wholly disproportionate change that will severely impact on the ability of local officers to tackle e-crime.

With reference to resources and training, NTSeCC is about the undertake a programme of work to ensure Trading Standards enforcement staff are suitably trained to carry out e-crime investigations at a local level. This will include improving their knowledge of open source research, online investigation techniques and the capture of digital evidence. Allied to that is a programme of equipment procurement to ensure local staff have the correct tools (both software and hardware) to help them further their investigations.

### Whether there are any gaps in the response to e-crime and, if so, how they should be addressed

14. The Consumer Landscape Review, commissioned by the Government in 2011, set out a vision to, amongst other things, improve and simplify the way in which consumer protection legislation was enforced locally, regionally and nationally. Traditionally, the majority of this work was split between the Office of Fair Trading (OFT) and individual LATSS. With the differing remits (and geographical boundaries) of the two bodies, this often led to ‘enforcement gaps’, particularly when dealing with cross-region and national issues. In recognition of this, the National Trading Standards Board (NTSB) was formed to oversee the transition of responsibilities from the OFT to LATSS, with particular emphasis on putting in place an infrastructure to tackle cross-region and national issues and/or cases of a particularly complex nature (Level 2 and Level 3 criminality).

15. As part of this process, the provision of e-crime enforcement in relation to scams and rip-offs directed at consumers and businesses was indentified as a key priority. Whilst there are a number of officers in individual LATSS who take an active role in e-crime enforcement, there was no coherent approach to tackle a problem which, by its very nature, is a cross-region issue. It was also recognised that e-crime enforcement is a specialised area, requiring specific expertise and skills. Furthermore, for reasons already identified, this area of e-crime has not always been seen as a priority by other enforcement agencies. As a result, the new NTSeCC has been formed to tackle the problem of internet scams directed at consumers and businesses.

16. Consumers and business are faced with a bewildering array of options when reporting e-crime. The local police force, LATSS, Citizens Advice, Crimestoppers and Action Fraud are just some of the reporting mechanisms available. As a result, it is sometimes difficult to build up a complete and accurate picture of the current and emerging threats faced. NTSeCC has recognised this as a key issue and therefore the collection and analysis of intelligence in relation to e-crime is core to its business. This will allow us to monitor current and future trends so we can direct our limited resources in a way that is likely to have the most impact. However, it is felt that greater clarity needs to be provided as to where to report instances of e-crime. If this is through a central point (for example Action Fraud) then this needs to be backed up by clear, simple processes that allow for the rapid dissemination of reports to the appropriate agencies for action (i.e. NTSeCC, LATSS etc.)
Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use

17. NTSeCC is currently undertaking a National Strategic Assessment with a view to identifying emerging threats faced by consumers that are specific to areas that Trading Standards has a duty to enforce. However, as part of the wider Trading Standards role, we have a duty in terms of safeguarding vulnerable people. In line with this, Trading Standards would look to support any activities through its links with Citizens Advice and their wider Consumer Empowerment Projects.

The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples' online behaviours for related public policy

18. There are a number of initiatives aimed at raising awareness such as Know The Net, Get Safe Online and Action Fraud. Whilst these are worthy attempts to give the public a greater awareness, there doesn’t seem to be a coherent response to tackling this issue. Frequently consumers and businesses put themselves in positions whereby they are easy prey for online criminals. This is often as a result of being poorly educated in the potential dangers of the internet and being unaware of the personal and financial risks they undertake whilst using the internet/computers.

19. One could question whether this should be the sole responsibility of Government or whether the industry (ISPs, search engines etc.) should take on a more pro-active role in educating their customers to some of the pitfalls of using and trading on the internet. Whilst we recognise that steps are already being taken by some parts of the industry, there are elements that seem to ‘turn a blind eye’ to both their moral (and in some cases legal) responsibilities.

National Trading Standards Board
National Trading Standards eCrime Centre
Association of Chief Trading Standards Officers
Trading Standards Institute

November 2012
Written evidence submitted by Paul Miloseski-Reid [EC 13]

I am the UK Lead Trading Standards Officer who provides regulatory compliance advice to eBay, Gumtree and PayPal on their obligations under consumer protection law. I initiated the Internet Auction Working Group in 2009, a sub-group of Local Government Regulation, to strategically review the crime affecting emarketplaces, which make up 36% of UK eCommerce.¹ Members of the group included my equivalents who advised the other 80 UK emarketplaces eg. Amazon and CQ Out.

I have not had the opportunity to obtain views from the Internet Auction Working Group, which I Chaired, and so the following should be considered as my own personal view. I have no problems with any of the information being published. However, the information within the Annex should not be published.

Due to the pressures of investigative work within my role I have been unable to dedicate much time to presenting the following information to the standard I would have liked, but I hope the content will prove helpful to the Committee nevertheless. I have further background information and reports that I can refer the Committee to should they have an interest in some of the particular points raised below.

Prevention better than cure

According to Ofcom 91% of 5-15 year olds have internet access at home and this age group spends an average on 90 minutes per day online.²

Only 32% of parents say they actually monitor their child's social networking activities every day, and 28% of parents admit they only occasionally, rarely or never monitor their child's social networking activities.

Many children have more IT skills that their parents, and parents are not au fait with ‘parental locking’ software etc etc etc so important to get the message to our kids from early age the dangers of the internet

56% of 851 children and young people aged 5-18 years thought that all illegal or inappropriate things should be blocked automatically, so may be lot of support from parents for the idea of ‘safe’ internet provision which adults have to unblock

Internet is dominating every part of our lives: professionally, economically (retail, price comparison sites etc) and socially, particularly in the youth. It continues to grow:

¹ In 2012, Amazon and eBay made up 36% of all online traffic to UK shopping sites. In 2012, eBay have a 19.2% share of all UK online retail visits
² Ofcom (2011) 'Children and parents: media use and attitudes report'
Professionally
Note the likes of Knowledge Hub, LinkedIn

Economically
- UK is the world’s leading country for ecommerce, with 79% of consumers buying online - we each spend around €1333 each year on the Internet
- £47.2bn was spent online in the UK alone in 2009. It was forecasted that sales would reach £56bn by 2014, but they already reached £68bn in 2011
- UK represents over 30% of European online sales
- 37 million shoppers spent £12.9bn in the 2011 Xmas period
- online shopping now accounts for 17% of the total UK retail market
- UK eCommerce to represent 12.4% of GDP by 2016
- Note the rise of Group-buying sites. UK list and issues which may surround them

Socially:
Facebook has hit the biggest milestone in the company’s eight-year history: 1 billion users.

Along with Money Advice (making good financial decisions), I recommend that online safety should be an essential life skill which young people learn at school. The evidence/surveys demonstrates that parents feel out of their depth and are in need of support in this area.

EDUCATION FOR SMEs
Consideration ought to be given how Government gets its “online safety” message across to businesses from day 1 of trading. There could be a role for Companies House to desiminate information at the point of company registration, however this would leave some 2,412,000 non-Ltd businesses without access to this advice
I believe that business registration would realise a number of government policies...
- The government agenda is to reduce burdens on business and regulators. Although there would be an initial burden on business this is balanced by the reduced burdens for the business in obtaining advice. Imagine a website which acted as a business advice one-stop shop. In return for registering, they would obtain comprehensive advice on the range of legislation applicable to them along with e-newsletter updates on new Regulations and scams that may affect their business/locality.
- Such a website is almost in operation already. Under the Transformational Government programme businesslink.gov.uk will be the main web portal for businesses accessing government information – see 33(3). It would only

---

3 Pg 47 Innopay’s Online Payments 2012 Report
4 at the start of 2010
http://www.bis.gov.uk/analysis/statistics/business-population-estimates
require some tweaking for it to be in a more user-friendly format where a trader can simply enter their profession and be provided with the various advice required, whether it be taxes, licensing or planning. Business Link already have a registration process for their email updates. Ideally, registration with BL would link in with Government Gateway - www.gateway.gov.uk to provide a true one-stop shop for a trader’s relationship with Government.

- Businesses spend at least £1.4 billion each year on advice about how to comply with regulations. The suggestion above may help to dramatically reduce this expense.
- Should the above option be explored can we also suggest including in any such registration form a requirement to provide a contact for alerts...Government could then alert SMEs to the latest scams affecting businesses

**EDUCATION FOR CONSUMERS**

1. Currently consumers have too many options:
   - http://www.adviceguide.org.uk/index/your_world/consumer_affairs.htm
   - http://www.communitylegaladvice.org.uk/gateway/consumer.jsp
   - http://www.getsafeonline.org/

   Along with sites, specialising in certain aspects of consumer advice: www.no-ur-rites.com; www.ca.co.uk/default.aspx?catid=125&pagetype=90

   There must be ONE ‘Government central advice’ site for pre-shopping and post-contract advice. This ought to include an eCommerce page with a forum for questions and answers (eg. http://forums.moneysavingexpert.com/) and template letters of complaint. This should collaborate with private/third sector sites which already have useful resources eg. Which?, MoneySupermarket, by signposting to the sections of those sites

2. Awareness of customer supporting bodies like the Financial Services Compensation Scheme and the Financial Ombudsman Service is low, therefore the majority of consumers are reliant on the business to inform consumers. A) this should be included in consumer education, but also a legal duty on all eMoney providers to make a statement about the Financial Ombudsman Service scheme in their promotional material just as UK banks must.

3. Move Howard online shopping assistant - www.ukecc.net/sub.asp?id=209 - to the ‘Government central pre-shopping advice’ site and then improve upon it.
The concept of Howard online shopping assistant is great, however it is somewhat restricted in which sites you can research and could possibly be more user friendly. A few suggestions to perhaps provide a more comprehensive series of online background checks for consumers:

A. The website search to utilise some of the following sites which have greater number of domain names registered or if not possible links to them:
   - Allwhois
   - Internetters
   - Internic
   - Network Solutions
   - samspade

B. Provide details of **EU VAT number check**

C. Most consumers would not have company number and so provide details of company registrars - **European Business Register**

D. Google search can sometimes provide useful information, however it would be very helpful to also refer them to the country’s most popular Consumer Complaint Forums eg. in the UK we have:
   - [www.grumbletext.co.uk/](http://www.grumbletext.co.uk/)
   - [www.clik2complaints.co.uk/](http://www.clik2complaints.co.uk/)

E. Information on the country’s equivalent of the following that we have in UK would assist:
   - [Check CCJs, court orders and fines](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [OFT EA Injunctions / Undertakings database](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [Disqualified Directors Register](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [Insolvency Register for Bankrupts](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [Liquidation and legal notices](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [BBC Rogue Traders](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [Watchdog reports](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [Referenceline](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)
   - [Checkatrade](http://postcode.royalmail.com/portal/rm/addressfinder?catId=400145)

**Encourage consumers to report problem sites**

Quick reporting button included in IE, google chrome etc which sends report to that country’s central repository eg. Action Fraud for UK. We suggest you publish the best cases showing how an individual’s report led to a conviction – pushing the angle ‘one person makes all the difference’. Consider a Name & Shame policy as ASA does so consumers see action is being taken.

**Challenges for Enforcement**

There are over 4000 ISPs worldwide. Contactability is a huge problem. Some ISPs have no contact details on their sites or only details of other departments which do
not always know who deals with takedowns. At an EU (Europol, DG SANCO) or International (Interpol) level, a central body should collate the ‘takedown’ contacts for all of the 4000+ ISPs, social networks and search engines on behalf of the enforcement community.

SPECIFIC ECRIME CONCERNS

COUNTERFEITS
I would highlight www.brand-i.org/. It is hoped that this can aid the fight against the influx of Chinese websites selling counterfeit, using co.uk domains to pretend to be a UK business.

REDRESS AFTER SCAMS
No matter the comprehensiveness of education some will always be victim to scams or illegal ‘business’ practices. Court is not an option due to costs and the international nature of scams. Credit cards are used for 40% of online transactions; debit cards 35%, with PayPal being the third most popular. More people are opting to use an eMoney provider, as it masks their financial details and it saves time at the checkout, so we are seeing a continuous increase in the market share of eMoney providers.

One would normally make a claim with a debit or credit card provider under the Chargeback rules or s75 of the Consumer Credit Act 1974. Further details on both of the Chargeback and s75 provisions is set out in the FOS advice page.

BUT The Financial Ombudsman Service position is that section 75 protection does not apply where PayPal or any eMoney service becomes involved in the credit card transaction. This leaves consumers with no recourse to pursue their complaint with the Financial Ombudsman Service. They only have recourse with the courts. I would EMPHASISE – this is not just an eBay or Amazon issue. This said, with over £3bn in sales annually and these two sites representing a significant portion of UK ecommerce the issue would be worthy of our attention even if it did only affect eMarketplaces.

A growing number of UK retailers are including an eMoney payment option in their checkouts:
- PayPal used by 976 of the UK and 572 of the US major stores.

5 pg 57 Innopay’s Online Payments 2012 Report
6 pg 75 Innopay’s Online Payments 2012 Report
• Skrill (Moneybookers) used by over 135,000 merchants
When 52% of the adult population have a PayPal account, UK online retailers naturally feel obliged to offer PayPal on its websites.

The key issues which determine the applicability of section 75 are identified very clearly in Office of Fair Trading v Lloyds TSB Bank Plc and others [2006] EWCA Civ 268 and the Bank of Scotland v Alfred Truman (a firm) [2005] [EWHC] 583 (QB). This is legal authority that section 75 protection does exist where one has paid on credit card for a product, via an eMoney service.

Similarly, the majority of consumers using debit cards can rely upon chargeback protection where there is a breach of contract:
- There has been unauthorised use of the buyer's card.
- The buyer didn't receive the item that was paid for.
- There were errors in processing the transaction.
- The buyer is dissatisfied with the item as it does not match the description.

As per Truman, where section 75 applies this in turn means that the chargeback scheme will operate

Empty parcel scam
Some sellers and buyers (returning products) ‘play the system’ by simply sending an envelope or empty box which is recorded delivery or has a certificate of posting from their Post Office. It is difficult for recipients to dispute this as the sender has evidence of posting/delivery. No weight is recorded with post office receipts which now act as a certificate of posting and IF weight is recorded with recorded delivery, this information is not included in the details posted online. This can cause issues for eBay millions of users as PayPal only accepts online proof of delivery. It is also an issue for UK ecommerce as consumers have the legal right to return products without reason, thus it is a route for rogue buyers to purchase products and return ‘empty’ boxes.

We recommend exploring whether postal services could include weight of package on a certificate of posting AND for recorded delivery this information is made available online to 3rd parties, so they can identify such scams and provide a more equitable service to the recipients.

Theft of financial details by rogue sites
Best countered by eMoney Services which hide consumer financial details. This market needs to be competitive. I am of the opinion that the market is not competitive

---

8 Paragraph 49: An important element of the firm’s case is founded on the submission that the card-holders had no valid claim against the card issuers under s 75 of the 1974 Act. That in turn meant that the chargeback scheme should not have operated and therefore the bank has no claim against the firm.
9 Consumer Protection (Distance Selling) Regulations 2000
due to eBay tying users to its own PayPal eMoney service. eBay is 95% of the world online auction market. Forcing its users to use PayPal has likely contributed to PayPal gaining 20% of global ecommerce sales.

The market must be competitive if eMoney services are to work to their benefit. Portability between eMoney services is something to consider so consumers can easily change service where they get a bad deal. Improving the market will encourage more consumers to opt into using these services and thus benefit from the security of masking their financial details.

Note that Alipay (700 million registered accounts) is being rolled out globally, which may have an effect on which eMoney provider non-eBay sites include in their checkouts. This will have no effect on eBay sites (which will continue to push users towards PayPal) nor Amazon sites (which will continue to push users towards its own Amazon Payments). However, it is argued that most consumers would be reluctant to change eMoney provider once they have chosen one due to the burden of registering all of their personal and financial details with another provider. Thus, a new entrant to the market will have to offer great incentives for consumers to change provider.

**SPAM**
There is an ever increase in scam spam emails, offering wonder drugs, cheap degrees and other cons. Most email providers allow you to block a spam email AFTER you have identified that type of email as spam or email sender to be a spammer. Spammers use countless email addresses so you will never overcome the issue that way.

Consumers ought to be provided with the right to positively discriminate which emails they will accept eg a list of their trusted email addresses. Anyone else emailing them will be informed that they only accept emails from known associates.

I recommend the promotion of white lists, primarily for vulnerable internet users, which block all emails except those from named friends/family.

It is likely that there is some cross-over with criminals using spim (unsolicited text messages) as well as spam for their frauds. This is only going to become a larger problem, as there is an ever increase in mobile users - 77% mobile users in 2002 compared with 43% 1999\textsuperscript{10}. Also, more people are opting for pre-paid (81%) rather than subscription mobiles (31%)\textsuperscript{11}.

The volume of "spim" was set to triple in 2004, according to a report from the Radicati Group, a technology market research firm in Palo Alto, California. The company projected that 1.2 billion spims would be sent, 70 per cent of which are

---

\textsuperscript{10} Monitoring European Telecoms Operators EC report

\textsuperscript{11} Telecoms services indicators 2002 for EC
A survey conducted by QQ.com, one of China’s largest news portals, showed 98.1 percent of people received spims every day, with about 20 percent getting three to five in 24 hours.

The European Council recommended in May 2003 that Member States consider a set of appropriate requirements for tracing the use of prepaid card technology in connection with organised crime.

Recital 43 of 2002/58/EC [Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector Directive] provides:

>To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes

As prepay mobiles can be used to send unsolicited text messages (“spim”), effective enforcement is currently hampered in EU countries due to the lack of appropriate recording of mobile prepay subscriber details. Whilst this Directive is generally aimed at the use of mobiles by businesses, how are Communication Service Providers to know what use will be made of a mobile once sold?

It is clear from the EC’s Report, Regulatory Framework & Market Developments concerning Directory Services in EU and EEA member states, that a lot of effort is required by EU member states alone. The report highlighted that EU “mobile operators often know little about their prepay customers, not even their name and addresses”.

‘Spam’ regulations (2002/58/EC) and part of the Consumer Protection from Unfair Trading Regulations 2008 (para 26, schedule 1 - persistent and unwanted solicitations by telephone) are almost unenforceable.

‘To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes’ (Recital 43 of 2002/58/EC)

In the US, one in six mobile phone users report receiving unsolicited text messages on their phones from advertisers. The US legislated Businesses can set up numerous different pay-as-you-go mobile accounts to use for sending unsolicited messages. It is practically impossible to identify the owners of these mobiles as the phones need not be registered as is the case with contract phones. Pay-as-you-go mobiles are always the preferred choice of criminals and scammers. Without subscriber details, the Directive cannot be effectively enforced and it is very difficult to pursue other offences where these mobiles are used.

13  chinadaily.com.cn/china/2009-06/13/content_8280507.htm
18  http://en.wikipedia.org/wiki/Mobile_phone_spam
This is a larger problem for all law enforcement. It’s arguable that the UK Police are now capable of overcoming this problem by using Triangulation techniques (a method of pinpointing a mobile’s location), however with Triangulation costs ranging up to £2500 a time this may be disproportionate to the crime. Trading Standards do not have access to Triangulation techniques under RIPA, and may have no other method to trace an offender. We do not have stats for the UK but of the 80,000 identity-requests in Switzerland 30,000 were prepaid mobile phones. I note that 130,000 users of prepaid mobile phones refused to register their phone.

Examples of countries that have legislated registration:
- Australia – legislated mandatory registration in 2000
- Japan’s Vodafone K.K – registration in 2004
- India, Switzerland and Brazil all have registration requirements for prepay phones and/or phone cards

It is worth noting that there were discussions within the E-Money Directive Consultation on a requirement for mandatory registration of prepay mobiles, with regards to the Money Laundering aspects of the Directive, however we understand that industry argued strongly against this.

In June 2009, three major Chinese carriers—China Mobile, China Telecom and China Unicom—imposed limits on text messaging in order to crack down on spam SMS. Under the restrictions, a phone number can send no more than 200 messages per hour and 1000/day on weekdays²¹

I recommend:
- an exploration into the links between spammers and spimmers
- the implementation of a low limit eg. 10, for the number of messages any mobile may send in a day UNLESS the user registers the mobile.

SPAM 2
As with SPIM, I recommend the implementation of a low limit eg. 10, for the number of emails that may be sent daily from unregistered/unverified email addresses eg. Hotmail. There would be no, or a lesser, restriction for verified email addresses. You

21 reuters.com/article/idUSTRE55B1RU20090612 & chinadaily.com.cn/china/2009-06/13/content_8280507.htm
may explore the average number of emails sent from a typical business email account to identify what may be a ‘reasonable’ number to set this higher restriction at.

**FAKE MEDICINES**
50% of medicines purchased from websites concealing their address are fake say World health Organisation (WHO\(^\text{22}\)).

Obviously there are benefits for those who are house bound to shop online and have medicines home-delivered. **I recommend** the use of one logo used by all EU online medicine retailers, along with a licence number that can be easily verified online. One logo will increase consumer awareness and lower barriers to cross-border purchasing. It is preferable if web crawlers are capable of automatically verifying misuse of licence numbers on such websites.

**NOTICE AND TAKEDOWNS**
Government has been slow to provide national, strategic leadership in dealing with the practicalities of the legislation (regulation 22 of the Electronic Commerce (EC Directive) Regulations 2002). Regulators, law enforcement and industry have been left to devise their own Notice and Takedown templates. The lack of guidance has left the majority of Council Trading Standards Officers uncertain as to powers available for Notice and Takedowns and what wording they could use in any such notice.

**eg of issue.** An IAWG member took around 1 week of research and phone calls to identify the relevant host of a fraudulent website; sent 3 emails to two different email addresses over a period of 5 months. A year later the website was still operating unchanged. With no victim and no financial loss the Council Trading Standards Officer did not pursue it any further and is now reluctant to become entangled in further Notice and Takedowns for other cases.

**Issue re: Takedowns -** Deleting illegal sites is more efficient than blocking them says Eco, the Association of German Internet Economy.\(^\text{23}\) The opinion of one IAWG member who considers himself moderately IT skilled is that it is simple to locate and use proxy websites. There are 400,000 pages of guidance on how to ‘Access Blocked Websites using Proxy Servers.\(^\text{24}\)

**I recommend** one EU-wide Notice and Takedown template for use by law enforcement and industry to provide a consistent approach to ISPs and assist those Council Trading Standards Officers who may lack the knowledge of such procedures.


\(^\text{23}\) EDRI-gram Number 8.17 - [www.edri.org/edrigram/number8.17](http://www.edri.org/edrigram/number8.17)

\(^\text{24}\) [http://tinyurl.com/2v2j362](http://tinyurl.com/2v2j362)
and powers. EU should engage international partners to explore an international template.

ISPA recommended that a code of practice should be developed for Notice and take-down procedures, underpinned by statute – paragraph 2.62

UK has the most deregulated system for domain registration in the EU
Foreign based companies hide behind a .uk domain name, leading consumers to believe they are dealing with a UK company and enjoying all the protections they expect from their ‘home’ jurisdiction

A .co.uk domain name says the information available on the web site is local, relevant and most of all trusted. “The most popular way of checking whether a site was in the UK was to see if the website address was ‘co.uk’ (cited by 41 per cent). Likewise, most participants in our consumer focus groups assumed that a ‘co.uk’ in the address indicated a UK site, although they also looked for clues like language, prices in pounds, and a UK address or phone number.25

This trust has led to:
• Police has this week shut down 1,219 bogus websites.htm
• Police have suspended 2,000 .co.uk domains.htm

There are 600,00026.uk domains registered to foreign registrants. Nominet have consulted on changing the requirements to prohibit a foreign registrant registering a .uk domain, however this would not prevent foreign businesses from owning/using that domain and so the above criminality will continue.

SUGGESTION: A number of businesses27 provide details of the legal entity at the bottom of every page so any user can clearly identify the contracting party at any given page that they are accessing. I do not propose such ‘disclaimers’ on every page, but consider that a statement on the homepage is a reasonable and proportionate step that is necessary to avoid any confusion. An effective disclaimer stating that the business is a Chinese or German etc Company would be required on the homepage.28

TRAINING
Must be more regional internet forensic specialists to assist each agency. These regional experts should be available to all Law Enforcement Agencies & regulators.

26 CHECK this figure within Nominet Domain_name_industry_reports
28 a French company prominently disclaim that they are not a UK businesses on their .uk homepage
SPECIFIC EMARKETPLACE CONCERNS

EMARKETPLACES
Online marketplaces, or eMarketplaces, are websites that provide the facility for consumers and/or businesses to sell products, whether this is fixed-price or auction style listings. These sites are used by consumers to sell their unwanted household goods and national companies as an additional online presence. Online marketplaces in the UK are a multi-billion pound industry. There are at least 309 million registered users worldwide that may list on UK sites and over 40% of active internet users visit eMarketplaces at least once a month.

eMarketplaces play a major role in consumer shopping. In 2012, Amazon and eBay made up 26.2% of all online traffic to UK shopping sites. eBay alone has a 19.2% share of all UK online retail visits with 22.2 million unique users per month.

Most users are honest, however there is a significant element of criminal activity. I would want to encourage eMarketplaces to share data on banned users (counterfeiters, fraudsters etc) with each other. A criminal can defraud eBay users; eBay ban them, they then go on to defraud Amazon users. They can hop from one eMarketplace to another until they go through all 80 UK eMarketplaces. At which point (after perhaps 12 months or so) they may be able to start over again with eBay using new financial and IP address details, making it very difficult for eBay and other eMarketplaces to identify that they are the same banned offender.

I also enclose at appendix 1 some stats on the level of eCommerce, eMarketplaces and eCrime in the UK.

APPENDIX 1
eCommerce in the UK
- £47.2bn was spent online in the UK alone in 2009. It was forecasted that sales would reach £56bn by 2014, but they already reached £68bn in 2011
- UK is the biggest country in Europe for business to consumer online spending, with 79% of consumers buying online - we each spend around €1333 each year on the Internet
- UK represents over 30% of European online sales
- 37 million shoppers spent £12.9bn in the 2011 Xmas period
- online shopping now accounts for 17% of the total UK retail market
- UK eCommerce to represent 12.4% of GDP by 2016

eCommerce worldwide
- By 2012 it is expected that more than 1 trillion will be spent online by B2C consumers
- UK, Germany, France and Italy – represented 69% of the estimated $122 billion online retail spending in Western Europe in 2010.
- 40% of EU consumers buying online

eMarketplaces in the UK
- 40% of active internet users visit eMarketplaces at least once a month
- Amazon and eBay made up 36% of all online traffic to UK shopping sites.
- eBay have a 19.2% share of all UK online retail visits
- eBay took 9.8% (the highest) and Amazon 8.6% of 96 million UK Internet visits on Boxing Day alone
- 190,000 SMEs on eBay; achieved £446m sales in 2010
- Amazon.co.uk, with 5 million customer accounts, was responsible for 16.6% of all UK e-commerce in 2002
- 93 eMarketplaces serving UK consumers
- Amazon went from 4.7 million transactions in Nov/Dec 2001 to 3 million transactions in one day in 2011
- Amazon is no.1 and no.6 in the top 100 e-retailers by site traffic and generated sales of more than £3.3bn in 2011
- 70% of the adult population already use eBay, with 17 million unique users per month
- 159 million-pound businesses trading on eBay
- over 100 high-street retailers, including Tesco and Argos, use eBay as an additional sales channel
- over 81 million product listings at any one time
- eBay predict sales of $10 billion just via a mobile device in 2012
- Amazon.co.uk, Britain's biggest online retailer, generated sales of more than £3.3bn in 2011

eMarketplaces worldwide
- 12.5 million transactions are completed on eMarketplaces daily
- 25 million entrepreneurs and SMEs on eBay

29 60 million on eBay, 6.5 million on eBid, Amazon has more than 15 million product lines
• In 2004, $54.3bn was spent on US auctions across 1 billion listings. In 2010, the total value of goods sold on eBay alone was $62 billion.
• eBay is the World’s 2nd largest online retailer with 16% share of the online retail space; commands 95% of the global auction listings market; 97 million active users; 100,000 new buyers joining their network across the world every day; 200 million live product listings.
• 50 million downloads of eBay apps in the past year.
• In Q4, 2010 Amazon sales were $12.95 billion. In 4 years they doubled from 76 million active customers accounts to 152 million.
• Amazon has 144 million active customer accounts; 2 million active seller accounts, which represent 29% of all sales. Amazon is growing at around 50% year on year.
• eBay revenue rose 29% to $3.28 billion for the first-quarter of 2012.
• Taobao (owned by Alibaba) - 370 million registered users; 800 million product lines; 50 million unique visitors a day in 2010. Taobao's sellers are behind 70% of the China’s $80bn of online transactions. Taobao made up 71% of Chinese consumer online purchases in 2011.

**eMoney in the UK**

52% of the adult population have a PayPal account.

**eMoney Worldwide**

867 million amongst just 4 providers.

<table>
<thead>
<tr>
<th>eMoney Provider</th>
<th>Stats</th>
</tr>
</thead>
<tbody>
<tr>
<td>PayPal</td>
<td>2.6 million customers in 2000. Now 26 million accounts in the UK - equivalent to about 52% of the adult population. 95% of eBay's 32m listings on the site already offer PayPal. eBay's Profit Jumps 20% on PayPal Gains. PayPal accounts for 20% of the global eCommerce sales of which 33% occur via a mobile phone, with more than 117 million active accounts in 190 markets. Accepted by over 165,000 sites in Europe alone.</td>
</tr>
<tr>
<td>Moneybookers</td>
<td>30 million customers worldwide, 135,000 merchants</td>
</tr>
<tr>
<td>Google Checkout</td>
<td>20 million Google Checkout in US. No global figures available</td>
</tr>
<tr>
<td>Alipay</td>
<td>700 million registered accounts and being rolled out globally</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>867 million users</strong></td>
</tr>
</tbody>
</table>

**eCrime in the UK**

• around £800m worth of counterfeit goods, and often unsafe items such as medicines and electrical goods, pass through online shopping and auction sites in the UK each year.
• 12 million UK users of counterfeit software.
• estimated £5 billion worth of stolen goods are ‘for sale’ in the UK at any one time.
• 80%-90% of crime on the internet is believed to be fraud-related.
• 45% of the 49,037 fraud and internet crime reports to Action Fraud were enabled online.
• UK ranks 2nd only to the USA for the number of cybercriminals worldwide.
- **UK ranks 2nd** for financial losses due to phishing and pharming attacks
- Cyber crime **costs the UK £27bn** per annum - £21bn affecting business; £3.1bn affecting citizens
- UK consumers spending over **£740,000** on fake medicines per annum
- 100 active fake escrow websites globally at any given time, with UK losses estimated at $10 million annually
- 6% of broadband subscribers had a botnet on their machine in 2010
- 21,377 websites were taken down in 2011 by the PCEU Internet Governance Team
- UK worst record in Europe for **identity fraud**
- eCrime costs e-retailers **£205 million** annually

**eCrime Worldwide**
- **Over half** of Europe’s electronics retail sites break consumer protection laws.
- Similar issues 2 years on - **57% sites** not reimbursing original delivery costs
- 81% of counterfeiters purchase their fakes online, with 41% of those purchasing from other online marketplaces (2008)
- **33%** increase in internet fraud in US
- 50% of medicines purchased from websites concealing their address are fake (WHO)
- Up to **560,000** people victims of phishing sites annually
- **Four-fold increase** in companies reporting security incidents with a financial impact between 2007 and 2010.
- Taobao Marketplace removed 63 million pirate products in 2011

**‘Auction’ crime in the UK**
- eBay alone removed 2.21m potentially counterfeit listings and suspended 30,000 sellers in one year
- On a given day, there are over 5 million illegal listings on UK eMarketplaces which attempt to restrict consumer rights, which quote to an estimated consumer harm of **£349.6 million** per annum

**‘Auction’ crime Worldwide**
- Online auction fraud was the **most reported ‘internet’ offence** in 2007, accounting for 35% of all reports
- There were **250,000 victims** of auction fraud daily during 2004

---

30 Not printed.
Written evidence submitted by Professor Peter Sommer [EC 14]

1. I am currently a Visiting Professor at de Montfort University and a Visiting Reader at the Open University. For 17 years I was first a Visiting Research Fellow and then a Visiting Professor at the London School of Economics. I have acted as an expert witness in many trials involving complex computer evidence; many of these would probably be regarded as E-Crime. They include: global hacking, terrorism, “phishing”, software piracy. But my instructions have also included criminal matters where digital evidence was crucial although the substantive crimes, including murder, large scale illegal immigration, art fraud, state corruption, money laundering, insurance frauds, theft of gold bullion and paedophilia which would probably not be classified as E-Crime.

2. I have provided advice for the UK's National High Tech Crime Training Centre, was the external evaluator and then external examiner for the MSc in Computer Forensics at the Defence Academy at Shrivenham which is widely used for police training and while it existed I was the Joint Lead Assessor for the digital element in the Home Office-backed Council for the Registration of Forensic Practitioners. I currently advise the Forensic Science Regulator on matters of digital evidence.

3. As an academic I have had a very long-standing interest in the issues of the definitions and statistics of computer-related or “cyber” incidents. In March 2009 I carried out a literature review, including statistics, of Internet crime for the National Audit Office as a contribution to a value-for-money review of Government initiatives in reducing the impact of such crimes.

4. From time to time I have been asked to contribute to a variety of government-sponsored inquiries into the policing of e-crime, starting with Project Trawler in 1999 which lead up to the formation of the National High Tech Crime Unit.

5. My practical work as an expert witness has brought me into frequent and direct contact with successive specialist police units, starting with the original Metropolitan Police Computer Crime Unit.

6. In February this year the House of Commons Science and Technology Select Committee published its report Malware and Cyber crime (HC1537) for which I provided both written and oral evidence. Both appear in their printed report. There is some slight overlap with the concerns of your Committee’s current inquiry and this is reflected in my submission to you, though of course the two Committees proceed on different bases.
7. I attach a CV.¹

Definitions of E-crime

8. There is no generally-agreed definition of E-crime and this lack directly impacts assessments of extent. We can illustrate the diversity of definitions. The Council of Europe CyberCrime Convention², also known as the Treaty of Budapest, covers in Articles 2-6 as “substantive offences”: “illegal access”, “illegal interception”, “data interference”, “system interference”, and “misuse of devices”. It adds as “computer-related offences”, articles 7 and 8, “computer-related forgery” and “computer-related fraud”. It further adds, articles 9 and 10; “offences related to child pornography” and “offences related to infringements of copyright and related rights”. Articles 4 and 5 more-or-less correspond to s 3 of the UK Computer Misuse Act, 1990: “Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.”

9. If we now turn to a report produced in February 2011 by the BAE subsidiary Detica in partnership with the Cabinet Office’s Office of Cybersecurity and Information Assurance (OCSIA), The Cost of Cyber Crime³, this covers: “identity theft and online scams affecting UK citizens; IP theft, industrial espionage and extortion targeted at UK businesses; and fiscal fraud committed against the Government.” “Industrial espionage” is not a criminal offence in the UK⁴ and the report excludes any direct reference to malware or to child pornography.

10. A recent paper by academics at Cambridge and Cardiff Universities Measuring the Cost of Cybercrime⁵ has the great virtue that it carefully discusses the various elements that might go into “cybercrime” and estimates of associated loss. At the very least the reader can see the workings and assess whether to accept their particular decisions. A similar earlier and slightly less thorough exercise was carried out by the Oxford Internet Institute in 2010: Mapping and measuring Cybercrime.⁶

11. The ACPO E-Crime Strategy⁷ dated August 2009 uses a much simpler definition: “The use of networked computers or Internet technology to

¹ Not printed.
commit or facilitate the commission of crime”. This definition appears to exclude, for example, the use of computers to carry out frauds which don’t involve networks, the acquisition of illegal material such as child or extreme pornography and the deployment of techniques to generate forged documents.

12. The previous ACPO Strategy, dated January 2005 and signed off by Trevor Pearce, then Acting Director General of the National Crime Squad and now Director Designate of Operations at the National Crime Agency (NCA), referred to “For the investigation of Computer-enabled Criminality and Digital Evidence” and did not limit itself to “networked computers or Internet technology”.

13. It needs to be recognised that by 2011 PC ownership was 77% of the population and household internet take-up was 78%. When the term “computer crime” first came into popular usage in the early 1970s the proportion of the population that had access to computers was tiny. For that reason, right through to the end of the last century it was possible to see computer/cyber/e-crime as distinct purely in terms of the demographics of potential offenders. But today large numbers of crimes are likely to have a “computer” element simply because for most of the population distinctions between their “non-virtual” and “cyber” selves are increasingly difficult to make.

14. The computer and the network may not be central to a crime or its investigation but the role of some form of digital evidence may be crucial.

15. A question for the Committee, therefore, is whether the current ACPO definition of E-Crime fully addresses the range of policy issues facing police investigatory capability.

Impact on Crime Reporting

16. Most official forms of crime recording in the UK are on the basis of specific offences prosecuted. But in relation to “E-crime” there are particular difficulties as a result of policies of the Crown Prosecution Service. It sees the 1990 Computer Misuse Act as designed to fill in gaps in other forms of legislation and in framing charges will concentrate on what it sees as the substantive offence rather than a modus operandi. Thus, if some-one infiltrates a program to monitor the keystrokes on a computer and then subsequently uses the passwords thereby obtained to access a computer from which to carry out a fraudulent transaction, the offence will probably be recorded as a breach of the Fraud Act 2006, despite the fact that both s 3 and s 1 Computer Misuse Act offences took place. A phishing attack would probably also be charged as fraud or

---

8 I have been unable to discover a current online source for this, but retain my own copy
10 Statements frequently made by CPS officials in public and private
money laundering, a Distributed Denial of Service attack (which also tends to involve offences under s 3 Computer Misuse Act when computers are remotely taken over by “back doors” or “Trojans”) would probably be charged as an extortion as this is the most common way in which criminals can make money. A botnet is simply a more extensive form of Distributed Denial of Service attack. In every year since the Computer Misuse Act came into force, prosecutions have seldom exceeded 100 per year.

17. From a broader policy perspective many criminal activities can be classified in several different ways – as the "substantive" offence such as fraud, sexual exploitation of children or extortion - or as a “computer crime” (involving computers to some degree) or as an e-crime (on the current ACPO definition as involving networked computers).

Impact on Policy Formation

18. The main justification for collecting statistics and arguing about categorisation is to see that resources are available to meet the needs of law enforcement, a matter which I consider below.

Gaps in legislation

19. There are no significant gaps in terms of substantive law, as a combination of existing conventional criminal offences, principally the Fraud Act 2006, and the deployment of the Computer Misuse Act meet most likely eventualities. There are however problems with the law covering investigators, which consists of a hotch-potch of powers, the product of historical evolution. Seizure and subsequent examination of computer hard-disks and other physical data media depend mostly on the Police and Criminal Evidence Act, 1984. Communications data is covered by the Regulation of Investigatory Powers Act, 2000 and subsequent laws and orders about data retention, currently the subject of the Draft Data Communications Bill. Interception evidence is, under RIPA, inadmissible and can only be used for intelligence purposes. The law covering access by the police to suspect computers is particularly complex and I attach a copy of my article Police Powers to Hack which is in Computer and Telecommunications Law Review (2012 CTLR, Issue 6 pp 13-19)\(^\text{11}\). There, and also in my evidence to the Joint Committee Draft Data Communications Bill, I suggest that a more radical review of police powers, including the circumstances in which warrants are issued, is required in order to achieve an appropriate balance between providing the police with adequate investigatory powers and ensuring that the public are not subject to unnecessary intrusion.

\(^{11}\) Not printed.
20. Interception evidence, currently excluded by s 17 RIPA, 2000, will need to be admitted in the same way as all other forms of technical evidence and the distinctions between “communications data” and “content” are now almost impossible to make within the technical protocols used on the Internet.

21. The Committee also ought to consider the position of the means by which evidence is obtained from cloud computing services, the vast majority of which are not based in the UK either jurisdictionally or physically. There are many forms of cloud computing, from consumer-orientated services like Google, Facebook, Drpbox, Twitter and web-based email, to business facilities in which companies substantially reduce their own local computing resources and pass their processing and storage requirements to large international entities.

22. Although there are a number of legal procedures and Mutual Legal Assistance Treaties which give the UK courts the ability eventually to obtain evidence from the cloud, they are lengthy and expensive. Swifter results can be obtained by seeking the co-operation of cloud companies, but the UK government seems slow to realise that the cloud companies will strongly prefer adherence to international legal norms of recognition of privacy rights, transparency, strict application of necessity and proportionality tests, and proper judicial process. In that connection, UK use of law enforcement-issued production orders and permission to intercept in the hands of a politician, is significant handicap.

**Issues in investigation and law enforcement**

23. Apart from the matter of investigatory powers, the very wide range of circumstances in which digital evidence may play a part creates significant difficulties for determining a police response. A criminal event may be local, national or international; it may be semi-opportunistic or highly organised; it may or may not, be linked to other forms of organised crime; its primary focus might be fraud involving banking and financial services, or retail fraud, or the sexual abuse of children, or the theft of copyright materials, or something else entirely. And the digital evidence may be central to a trial or simply peripheral but essential.

24. It is not enough to think in terms solely of specialist units. Every detective needs to know the basics of digital evidence – where it is likely to be located, how it can be safely collected and preserved without being contaminated in the process, and the core techniques that are used in analysis. The front-line detective needs to be able to interact and work with forensic technicians. Because of the ever-changing nature of computer hardware and software, and the rapid development of new criminal methods, basic training for all detectives
cannot be a one-off exercise but requires relatively frequent refreshment.

25. In effect the **police response needs to be tiered** – a level of knowledge for all, higher levels of skills for detectives within particular specialisations such as child protection, fraud, terrorism. And a single elite leadership unit to tackle the most complex and innovatory crimes and also provide research, advice and training for the rest of the law enforcement community.

26. The first attempt at setting up such a unit was the National High Tech Crime Unit (NHTCU) and which disappeared when the National Crime Squad was dissolved and the Serious Organised Crime Agency (SOCA) created. NHCTU staff were then absorbed in to “SOCA e-Crime”, now “SOCA Cyber”. But SOCA was separate from UK policing and the leadership role was lost until PCEU was set up from within the Metropolitan Police Service. It is to be hoped that with the development of NCCU within NCA does not repeat the same mistake – the unit must have a solid clearly articulated on-going relationship with the rest of UK law enforcement.

27. Thought must also be given to how digital forensic expertise is made available. The expertise has to extend to assisting in making decisions about what potential evidence to seize and what to examine in detail. Because of the quantities of digital material available – numbers of computers, mobile phones, tablets etc plus the ever-increasing storage capacity each holds, selections have to be made. Police refer to this process as **triage** but insufficient thought has been given to how it executed – and by whom. There seems a very good case for the development of specialist Digital Scenes of Crime Officers (SOCOs) as the skills required are outside those routinely available to regular SOCOs or police officers attending a crime.

28. There is also a very good case for regional hubs of digital forensic expertise as opposed to each police force having its own unit. This consolidation is already happening. However it is also essential that regular police investigators have easy access to digital forensic technicians so that they can work together when required.

29. A particularly productive route to the investigation of organised groups which deploy cyber techniques appears to be the Covert Internet Investigator (CII). There are a number of courses in CII, for example from Skills for Justice 12 and NPIA13 but there is as yet no published Code of Practice, which would seem important in developing public confidence in the ethicality and robustness of the methods

---

13 http://www.npi.police.uk/en/578.htm
30. The use of **private sector out-sourcing of digital forensic services** needs to be deployed with care. There are a number of highly competent companies and individuals, many former police officers and law enforcement agency employees. But there is danger in current practices of aggressive competitive tendering – if a OIC (Officer in Charge) lacks the knowledge fully to formulate his requirement, all that the tendering forensic service provider will do is respond to that tender. If, as now often happens, the OIC and the successful forensic service provider are geographically separated, police and technician will never work properly together and opportunities are missed.

31. Another often-neglected aspect of law enforcement is the role of the **Crown Prosecution Service**. For some time the CPS has had specialist prosecutors who have enjoyed a certain level of training – indeed I have done a small amount myself. But if my experience is anything to go by most CPS caseworkers lack much knowledge of digital evidence and in particular evidence derived from hard disks. All too often one sees the “particulars” on an indictment that make little or no sense. The fear is that mistakes in the framing charges both generates expense elsewhere in the criminal justice system – showing up in defence criminal legal aid and in court costs – and can sometimes result in the guilty going inadequately punished.

32. As with many issues within law enforcement response to digital evidence the problem is not a total absence of activity but that the extent and quality of resource made available is not keeping pace with the rates at which digital evidence in its various forms of growing throughout society.

33. See also my remarks about evidence from the cloud – paragraph 21 above.

**International Dimensions**

34. Although getting further international support and sign-up for the CoE Cyber Crime Convention (The Treaty of Budapest, 2001) is an obvious ambition, the Committee needs to be alert to the possibility that in some parts of the world it is perceived as too orientated to the conditions of Western Europe and North America. Alternative initiatives are being developed by the International Telecommunications Union. The Committee, in talking to UK government officials, may want to probe the UK government’s stance.

35. At a practical level much appears to depend on the quality of personal relationships between UK law enforcement specialists and their opposite numbers in other countries. I note the role of SOCA in this regard.
36. A further issue the Committee may like to consider is the position where, although an offence may have been committed within the jurisdiction of the English courts – the Computer Misuse Act, ss 4-5 are quite widely drawn – there are significant difficulties in successful UK prosecution where the vast bulk of the evidence is outside UK jurisdiction. The Crown Prosecution Service currently has a consultation:

Promotion of public awareness

37. The investigation of crimes in which digital evidence is an important component will always be expensive. Whatever arguments one has about definitions of e-crime it is unquestionably true that many are transborder in nature. For both of these reasons it is unrealistic to expect successful law enforcement action in anything other than a very small proportion of overall criminal acts. For these reasons prevention and mitigation are critical. It is disappointing that the National Cyber Security Programme placed so little emphasis on helping individuals and businesses help themselves. In the end the best people to apply protection to computers are those who immediately use them. One of the big concerns in E crime is the extent to which social engineering methods are deployed and education is the principal means by which it can spotted and thwarted. I notice that out of a total of £650 million for the overall programme get safe online has received just under £400,000.

38. I hope the committee will consider the virtues of extending the notion of "public health" to the cyber domain. We surely need much more frequent Government-sponsored official advice. Inevitably commercially sponsored advice pushes the public towards the specific products and services of the sponsors.

Professor Peter Sommer

November 2012
I write in relation to the Home Affairs Committee Inquiry on e-crime and, in particular, the evidence given by Professor Ross Anderson at your hearing on 20 December 2012. We are concerned over the accuracy of several of Professor Anderson's comments and would like the chance to put a more informed view before your Committee's members.

Financial Fraud Action UK is the name under which the financial services industry across the UK co-ordinates its activity on fraud prevention. FFA UK works in partnership with The UK Cards Association which represents credit cards, debit cards and charge cards in the UK. Its members are the leading retail banks and financial institutions in the UK who issue payment cards and extend credit to their customers (the card issuers), and those who process card transactions on behalf of merchants (the merchant acquirers).

During the hearing, Professor Anderson suggested that:

"... banks often find it easy to blame their customers for fraud... The banks certainly claim that they will blame people if there was gross negligence. In practice, they often blame people as a routine matter, even when it is not clear there was negligence at all"

The position of the banks is, and always has been, very clear. The innocent victims of fraud can expect to receive full protection against any losses - provided in the form of a full and timely refund, While both banks and cardholders share responsibility for the security of the card, it is only in circumstances where customers have been grossly negligent in protecting their PIN and card that they sustain any loss - which is a high threshold to overcome. Processes embedded by the banks ensure that all customers who are genuine victims of fraud will be refunded and will suffer no loss with the burden of proof on the bank to demonstrate otherwise. The cross-industry picture is that 98% of cases are resolved with a full refund being delivered for the customer. The remaining 2% is made up of a combination of the following scenarios: firstly, fraudulent claims, and secondly where the customer has been found to have acted with such gross negligence as to have practically colluded with the fraudster.

Banks are required to refund the victims of fraud immediately and, as a recent Which? study clearly showed, the vast majority are refunded within a week. On the rare occasions when the situation is not clear cut and the bank needs to investigate further, most card companies ensure that the available balance and interest payments are unaffected whilst the transaction is investigated, which provides support and respite to customers.

The regulatory framework is overseen by the Financial Services Authority, while cardholders have recourse to appeal the decisions of banks to the Financial Ombudsman Service (FOS). All are able to use this additional route to redress where they are unsatisfied with any decision.

While we are confident in the processes in place, we are always open to representations from FOS, where the organisation feels there are systemic industry-wide issues that require extra attention. To this end, we are hoping to meet with the Chief Ombudsman later this year.

Professor Anderson cast doubt, as part of his evidence, on the banks' observance of the Payment Services Regulations 2009, but the figures set out above make clear that the proportion of customers receiving prompt redress is overwhelming. This is backed by research into the customer experience when it comes to fraud refunds: According to an independent study conducted by Accenture in 2012, less than 10% of respondents rated the service from their banks as anything less than good or excellent.
I would be delighted to give you a more in-depth briefing on FFA UK and the impact we have had. If you would find this helpful, I will ask my office to contact your team and arrange a suitable time.

Katy Worobec
Head of Fraud Control

Financial Fraud Action UK

February 2013
I write to thank you for inviting me to appear before the Home Affairs Committee this week, and for the opportunity to discuss the work of Financial Fraud Action UK with your members.

**Refunds for fraud victims**

During the evidence session I promised to provide further information to the Committee on the figures I cited during my submission concerning the number of refunded fraud claims. Financial Fraud Action UK and our partner organisation, The UK Cards Association, conducted a survey of our major UK retail banking members (list below) in advance of this session. The survey ran between March 13 2013 and April 12 2013 and collected data on the length of time taken to process fraud refunds during 2012. Our study found that between 96% and 98% of all fraudulent transactions were refunded on either the same day or the following day. On the basis of these findings, no more than 2% of customers receiving refunds have had to wait longer than two days. These figures corroborate that of the Which? survey published in January which found that 98% of fraud claims were refunded, but gives a more up to date picture of the landscape than the Which? survey, which included cases as long as up to five years ago.

*Members surveyed:*
- Bank of America
- Danske Bank
- Bank of Ireland
- HSBC
- Bank of Tokyo Mitsubishi
- Lloyds Banking Group
- Barclays
- National Australia Group
- Capital One
- Nationwide Building Society
- CitiBank
- Royal Bank of Scotland Group
- Co-operative Banking Group
- Santander
- Coventry Building Society
- Tesco Bank

**E-Crime**

I would also like to take this opportunity to reinforce some of the other statistics I shared with you during the session on the changing pattern of e-crime in the UK, from the perspective of e-commerce and online banking.

E-commerce fraud losses (that is, losses on cards used fraudulently over the internet) peaked in 2008 at £181.7m, a year when total online card spending reached £41 bn. During 2012 e-commerce fraud losses stood at £140.2m, a year when total online card spending reached £68bn. Fraud losses for e-commerce have therefore dropped 23%
since their peak in 2008, despite a 66% increase in online card spending.

Online banking fraud losses peaked in 2009 at £59.7m, a year when there were 22.4m registered users of online banking. During 2012 online banking fraud losses stood at £39.6m, a year when there were 26.8m registered users of online banking. Fraud losses for online banking have therefore dropped 34% since their peak in 2009, despite a 20% increase in the number of registered users of online banking.

The National Fraud Authority (NFA) estimates that all types of fraud cost the UK £73bn in 2011, of which less than 1% consists of banking and card fraud. Total plastic fraud stood at £388m in 2012, down 36% from its peak at £609.9m in 2008. Fraud accounts for just 7p in every £100 spent on cards in the UK, against the backdrop of a total of 9.9bn card transactions in 2012.

Solutions

I feel these figures demonstrate that the broader picture is that we are winning the fight against fraud, notwithstanding a constant need for vigilance in the light of changing modus operandi and developing technologies both on the provider side and in relation to the ‘attack tools’ used by fraudsters.

The banking industry has invested heavily in fraud prevention and detection activity, including £1bn spent on the roll-out of Chip and PIN and full sponsorship of the Dedicated Cheque and Plastic Crime Unit (DCPCU) which has prevented fraud to the value of £433m over 10 years. The banking industry has also pioneered new ways of working with the public sector to address fraud, including work with government on public-private fraud intelligence-sharing, and with the National Fraud Authority on consumer campaigns.

The figures around financial fraud, despite progress, remain higher than we would wish and, as the Committee has heard in previous evidence sessions, there is a real concern among our law enforcement partners that stolen funds are being used to bank-roll terrorist groups and support organised criminal gangs involved in the trafficking of people and drugs.

I’d like to reiterate the point I made about the need to streamline ways to share intelligence between law enforcement and the banking industry, and for data to be shared more effectively across borders. If we are to be even more effective in the fight against financial crime then intelligence-sharing across industries and between public and private sector (as well as internationally) is crucial. This should be reflected in the decisions taken around the new data protection regulations stemming from Europe, as well as decisions to be taken on existing Justice and Home Affairs measures.

There is also a need for a greater and more concerted effort from government, the police, and the private sector on consumer education and awareness raising to encourage small changes in consumer behaviour so that we are not "leaving doors and windows open" to online fraudsters, to use the analogy of ACPO’s DAC Martin Hewitt. To this end, having successfully run a number of campaigns jointly with the NFA and other sectors, we would ask for the Government to help in bringing other players to the table.

Chip & PIN

Finally, I would like to supplement my response to Dr Huppert's questions on Chip & PIN to state for the record that the use of PIN to authorise a transaction will not in itself preclude a cardholder from receiving a full refund. Victims of card and banking fraud benefit from a legal and regulatory guarantee of being refunded for any losses in a timely manner, irrespective of the nature of the transaction. In general, card payments are a
safer way to do business, attracting much greater protections than traditional payments such as cash or cheque.

We are confident in Chip & PIN as a system and believe it is largely responsible for the substantial decline we have seen in card fraud. While we would never be complacent enough to claim that any system is infallible, the evidence our police colleagues are seeing is that cards most commonly become compromised when consumers unwittingly reveal their PIN, for example through common ‘shoulder surfing’ and distraction thefts at ATMs, or by telephone frauds where a criminal posing as a bank staff member or police officer dupe the customer into disclosing his or her details.

I look forward to reading the Committee’s e-crime inquiry report, and please do not hesitate to contact me if I can be of any further assistance.

Katy Worobec
Head of Fraud Control

Financial Fraud Action UK

April 2013
Introduction

Nominet is the internet registry for the .uk country code top-level domain (ccTLD). With over ten million registered domain names, we are the second largest country-code top-level domain. We are an SME with a turnover of around £25 million and we employ around 140 people. Nominet operates on a not for profit basis with a constitution that requires that we act for the public benefit.

We interpret our public benefit constitution as requiring us to provide a secure and resilient internet service to ensure the smooth running of the .uk namespace. More broadly, working with others, we seek to raise awareness of risks to the internet and promote measures to reduce these risks. This means in practice:

- Monitoring the large amount of traffic we process for signs of abuse such as Distributed Denial of Service (DDOS) attacks, or distribution of malware and spam and where appropriate sharing these indicators of abuse with other industry partners.
- When asked to do so by law enforcement authorities, suspending .uk domains associated with criminal activity.
- Raising awareness amongst businesses and end-users through targeted promotional campaigns and education initiatives, in particular through our dedicated information portal, ‘Know the Net’.
- Through our charitable foundation the Nominet Trust, providing funding for community-level partnerships and initiatives such as the e-Crime reduction partnership in South Wales.

What do we mean by ‘e-Crime’?

e-Crime covers a broad territory and some of the confusion in the debate results from people using the term to mean different things which present different enforcement challenges and require different combinations of actors to work together to address the issue. For us e-Crime is a subset of cyber-crime and distinct from issues such as espionage, ‘hacktivism’ and cyber-terrorism. On this definition, the key feature of e-Crime is that the attacker receives some direct monetary benefit. Therefore in this response we focus on the common forms of criminal conduct that we encounter falling within that definition, and not on issues such as cyber-terrorism or mass infringement of private rights through, for example, online copyright infringement.

Very little e-Crime constitutes entirely novel forms of criminal behaviour. In most cases, e-Crime is the adoption of new technology to perpetrate types of crime with a long history. For instance, Nominet is called upon to act where .uk domain names are associated with sale and distribution of counterfeit goods and illegal pharmaceutical products.

An area of increasing concern is the use of new technology to distribute viruses and malware. The purpose of distributing viruses and malware is often to facilitate other forms of crime, such as to harvest personal data with a view to perpetrating large-scale identity theft or to facilitate fraud.

How well is the ‘e-Crime’ problem understood by policy-makers?

In general the UK Government has been in the forefront of nations seeking both to identify e-Crime risks and respond to them effectively. The National Cyber Security Strategy published in November 2011 was in our view a thoughtful and comprehensive overview of the issues and the actions for both Government...
and others that it contained were reasonable and realistic. In particular we welcome the Government’s recognition that, because the nature of e-Crime itself can change very rapidly (for instance as a result of technology shifts), a partnership approach with members of the internet industry is critical to ensure flexibility to address future threats.

However, at the level of policy-making below this an on-going concern for us is the ownership of responsibility for e-Crime (in all its different manifestations) within Whitehall. Despite the best efforts of Ministers and officials to create a coherent and joined up approach, Nominet has not always found it easy to determine where policy leadership on specific questions lies. This problem has been exacerbated by the transfer of some aspects of internet policy from BIS to DCMS.

Over the past 12 months we have had e-Crime and cyber security related interactions with each of DCMS, BIS, Home Office, Ministry of Justice, Cabinet Office, the Foreign Office and Department for Education, as well as GCHQ, CPNI, CSOC, Ofcom, the Intellectual Property Office, Information Commissioner’s Office and the Law Commission. Each of these interactions has arisen from laudable and important policy objectives, but simply keeping track of the plethora of policies and initiatives is a significant task.

This busy policy environment is becoming further complicated by the steady accretion of powers and responsibilities in e-Crime related fields by EU institutions. E-Crime is by nature a cross-border phenomenon, so in principle more effective collaboration at EU and indeed global level is to be welcomed. However, the full nature and extent of EU competence in this area, and how this interleaves with national efforts, remains somewhat unclear. There is some risk of duplication of effort and there is further risk regarding the EU’s more mandate-focused approach compared to the UK’s cooperative and voluntary approach.

This is a particular issue in relation to the reporting of security incidents and the sharing of information and intelligence across Member States. Commissioner Kroes has made clear that she will seek to introduce mandatory incident reporting requirements on a range of industries, but we would agree with the position taken by the Government that legislating in this way should be a last resort and that a cooperative non-regulatory approach may produce better results in the long term. In particular we believe in the importance of embedding risk management and preparedness in corporate culture rather than a compliance based approach which will always tend towards minimised standards.

### Effectiveness of current law enforcement, legislative capabilities, gaps

As regards UK-specific enforcement capabilities, the agencies that have been most active in pursuing e-Crime include SOCA, PeCU, the MHRA and Trading Standards. We welcome the proposed formation of an e-Crime specialism in the new National Crime Agency which should build on the useful experience in tackling e-Crime already gained by these existing agencies.

For our part, consolidating e-Crime enforcement in the NCA is an opportunity to establish a clearly-specified crime reduction strategy. This should include identifying which forms of e-Crime cause the greatest harm, what tools are appropriate to tackle the problem and how partnerships with other actors to take effective joint action should be structured.

Nominet is particularly interested in this because of the rising volume of requests we are receiving from law enforcement agencies to suspend .uk domains associated with criminal activity. At present we will typically be asked to suspend a domain based on evidence held by the agency concerned that the domain is associated with a criminal activity – for example, counterfeiting or sale of unlicensed medicines. The
Agency in question does not need to have proven in a court that a crime has been committed in order to notify Nominet that it believes that the domain name is being used to commission a crime.

The making of these requests, and our response to them, is a purely administrative arrangement that has no statutory underpinning. In effect Nominet is being asked to co-operate with law enforcement as an administrative matter, and to assess whether for instance a domain name complies with our terms and conditions. Law enforcement agencies may however point out to Nominet that were we to refuse to act when in receipt of actual knowledge that a crime has been committed on a .uk domain, we could ourselves be committing a criminal offence under the Proceeds of Crime Act.

In practice, the level of information presented to us varies. We encourage agencies to channel requests through a handful of law enforcement agencies with whom we have an established working relationship. In principle though, any body with law enforcement responsibilities could approach us with a request, based on minimal evidence, and expect us to comply with it. Hitherto such requests have generally been made in relation to relatively straightforward cases of criminal conduct, and we have generally found that the domain holder is indeed in breach of Nominet’s own terms and conditions. However, in theory we could be asked to suspend domains on the basis of criminal conduct whose nature is inherently more problematic, for instance where freedom of expression issues are engaged.

In response to this, Nominet has been seeking to develop an abuse policy which codifies the approach that we will take when we receive such requests. We hope to publish this for consultation in the coming year. Obviously such a policy cannot constrain the behaviour of the agencies themselves but can only describe how Nominet will seek to act. Hence in our view the need for the NCA to seek to develop its own matching processes for making such requests, and then applying these processes across the board in a consistent fashion.

Many stakeholders would go further and suggest that the law itself needs to be amended so as to create a clear legal framework for the making of suspension requests, possibly including court oversight of the process. It is hard for Nominet to determine the materiality of this issue from a wider perspective because we do not know what level of requests the NCA and other agencies might make in the future. It is worth noting though that domain suspension or seizure is an increasingly popular mechanism for US law enforcement agencies, who have ‘seized’ multiple thousands of domains in single operations. Were the Government and/or the NCA to come to the view that domain name seizures are an essential mechanism for preventing or disrupting e-Crime, then the legal basis for these requests should be placed on a more robust footing than it is at present.

**Information sharing**

As noted, we make efforts to share information with other parts of industry and the UK Government on cyber-crime threats. Increased government involvement with trusted parties involved in network and information security – in particular in sharing information – would be welcome. Such involvement is best through cooperation and partnership. The speed of innovation, the transnational nature of the internet and the number of organisations involved in assuring the successful operation of what was designed as a distributed network requires a cooperative, rather than a centrally coordinated, approach.

It is important to note however that the overriding consideration in making information sharing networks work is the ability of participants to trust each other. It is for this reason that the ‘CERT’ (Computer Emergency Response Team) model has resulted in a plethora of CERTs for different industries, and indeed, different parts of government. We believe that the Government’s approach to CERTs has
demonstrated a good understanding of the role that trust plays in making them work. The European Commission’s occasional suggestions for an EU-wide CERT and mandatory information sharing would in our view encounter some problems in creating the necessary levels of mutual trust and confidence. Private sector participants in particular will need very robust assurances about the use to which incident data is to be put by others in any pan-EU CERT network.

Online safety and awareness-raising

The National Cyber Security Strategy rightly focuses on the need for promotional effort to be expended on raising awareness of risks and of empowering businesses and communities to protect themselves against e-Crime. We welcome the steps the Government has already taken in this direction, but it will be continuing challenge over a number of years as the public and businesses develop a culture of technology and information security.

In 2008 Nominet established the Nominet Trust, an independent charity which supports initiatives that harness the internet to stimulate positive social action at a grass-roots level. To date Nominet has contributed £26m to the Trust. The Trust has funded a number of projects relating to e-Crime including a significant piece of research by Professor Mike Levi and Dr Matthew Williams from Cardiff University’s School of Social Sciences which was published last September.

As well as supporting research and community action through the activity of the Trust we have also sought to develop accessible online resources that help raise public awareness through our ‘Know the Net’ website. Given the need for long term cultural change in how we think about our privacy and security we believe it is important to avoid an alarmist approach to consumer education and awareness. Headlines about cyber criminals victimising millions of people can make it seem that the ordinary consumer is powerless thereby encouraging apathy rather than sensible precautionary measure.

Our Know the Net campaigns use engaging materials to educate users about simple practical measures that they can take to lower the risk of them becoming a victim of e-Crime. Three specific examples are worth mentioning:

Online scams: ‘ThreatTest’

Based on findings that suggested that more than half of UK population has been targeted by online scams, we commissioned research to better understand the profile of online scam victims. We found that women between the ages of 25 and 34 were most at risk. In response we launched an online ‘ThreatTest’ tool, which has to date been used by more than 28,000 people. It provides some important common sense tips to help reduce personal exposure to online scams.

Obeying the law online: ‘Accidental Outlaw’

Our research found only 44% of people could correctly identify what online activities were illegal. The top risks identified were misuse of copyrighted content (particularly music), discussing or publishing details relating to a super injunction and defamation of other people using social media.

In response we launched the ‘Accidental Outlaw’ test – more than 22,000 have taken it already. This allows users to check their own understanding of how the law applies online and learn about areas they are unsure of.

Mobile Security: ‘In The Dark’
Recognising that many people now use smartphones and tablets everyday as their principal means to access the internet, our research showed that only 54% could correctly answer questions on device security. The research also showed that 43% of users do not have basic security measures such as anti-virus software, remote wipe facilities in the case their device is lost or stolen, or the latest version of their operating system installed, and 31% did not know how to protect their mobile device. 21% of 16-24 year olds reported that they had been ‘phone jacked’ putting them at risk of data and ID theft.

In response, we launched ‘In the Dark’ tool for users to test their own mobile security knowledge – almost 5,000 have used it already.

**Security of the Domain Name System**

Although this is not a specific line of inquiry in the Select Committee’s call for evidence we thought it would be useful to provide some background about Nominet’s primary responsibility, the functioning of the .uk Domain Name System (DNS).

*How the DNS works*

The DNS system goes back to the establishment of the internet as a distributed network of connections between geographically diverse computers. Internet addresses are written as a string of numbers known as ‘IP addresses’ which tell computers the location of the data they are trying to find on the internet. The DNS system was created to replace the IP address with letters and words in order to make the system usable. For example, it is much easier to remember www.bbc.co.uk than 212.58.244.68 which is the IP address of the BBC’s website.

However, in order to allow a computer to know that the domain name of www.bbc.co.uk relates to the IP address 212.58.244.68 there has to be a place where this can be looked up. All top level domains (e.g. ‘.uk’ or ‘.com’) are incorporated in the ‘root zone file’ the ultimate, authoritative database of the global internet, which is managed by the Internet Corporation for Assigned Names and Numbers (ICANN) which operates this function under an arms-length contract with the US government. A DNS search comprises of two stages of looking up. Firstly the domain name is looked up on the ‘registry’. Each top level domain on the internet has a registry where domain names can be looked up. Nominet is responsible for running the registry of all domain names that end with .uk. The registry does not actually contain the IP address of each domain name, instead it holds the IP address of the ‘nameserver’ used by the user of the domain name. This allows a computer to contact the nameserver and identify the IP address of the server it is looking for.

**Potential vulnerabilities of the DNS**

The DNS system was developed for a small network of trusted connections between computers. The benefit of the system is that it is easily scalable and has extended to cover the hundreds of millions of domain names that are now registered around the world, however the system does have some potential points of vulnerability.

One feature of the DNS is that the servers of registries have to handle millions and sometimes billions of requests to identify nameservers and the nameservers have to handle large numbers of requests to turn domain names into IP addresses every day. This requires a significant amount of computing power and highly robust systems to ensure that a response is always provided and that it is provided in a fraction of a second. The DNS system can be exploited by hackers, criminals and ‘hacktivists’ to launch Distributed Denial of Service (DDOS) attacks. A DDOS attack attempts to flood the victim IP address or server with
so many requests that the servers become overloaded and slow down or fail to provide a response. The result is that no one is able to use the system, for example to view the website or get email through to the domain name under attack.

Another weakness of the DNS is that it relies on the veracity of the information provided in response to a DNS query. ‘Cache poisoning’ attacks take advantage of the fact that internet service providers will use a server on their own network to cache common queries such as facebook.com or bbc.co.uk from their users rather than repeatedly send a DNS request to the registry every time the address of bbc.co.uk or facebook.com is requested. This caching mechanism manages the amount of traffic the ISP and the registry have to contend with and provides faster response times for users. Unfortunately there is no validation of who has provided the information in regular DNS so in a ‘cache poisoning’ attack the incorrect information is inserted into the ISP’s cache server in order to direct traffic to another source than the intended source for example to obtain log in credentials or to cause reputational damage to an organisation.

**Defending against these vulnerabilities**

As outlined above, the most important response to these types of attacks on the DNS is to take steps in advance to prevent or limit the effectiveness of such attacks. Nominet’s systems are highly robust and resilient, utilising physically diverse and geographically diverse infrastructure to maintain the reliability of the .uk DNS. We also have sophisticated monitoring techniques to identify patterns of traffic that may indicate an attack or malicious activity. In addition there is clear value in the sharing of information and cooperation between businesses and governments. When an attack is identified, swift action by registries, ISPs and other network providers can limit or mitigate the threats.

We have also been active in the encouragement of the deployment of the DNSSEC security standard which is designed to prevent cache poisoning by embedding an encrypted digital signature in the response from the registry to the DNS cache by signing all messages between systems with an encrypted digital signature to create a ‘chain of trust’. DNSSEC is not a silver bullet to solve e-Crime issues but it does mitigate a vulnerability in the original architectural design of the internet that has been exploited by attackers in the past. Particularly for high-risk domains such as those for governments, financial institutions and large-scale e-commerce websites it can add an additional layer of security.

**Potential developments in the .uk DNS**

Nominet recently conducted a consultation exercise on the introduction of a new domain name service in the .uk domain space. At present, .uk is organised under a hierarchical structure in which consumers and businesses register at the third level, such as example.co.uk or example.org.uk. From time to time, Nominet has been asked why it is not possible for consumers or businesses to register at the second level, such as example.uk. This would mirror the simpler structure of .com and most other country code Top Level Domains.

Our consultation proposed the introduction of a new, second-level structure that we referred to as direct.uk, sitting alongside the existing .co.uk, .gov.uk and so on. We proposed the inclusion of additional security features into the new service that would enhance end-user trust and hence make the product particularly attractive to those wishing to trade online. The security features we proposed included an obligation to implement the DNSSEC security feature, the provision of a malware scanning service, stricter procedures for validating data provided by registrants at the point of registration, and a ‘Trustmark’ that the registrant could use on their website. We also proposed to restrict eligibility to
companies with a UK presence, as this gives the customer some comfort that UK consumer laws would apply to transactions from the site in question.

Our consultation has received a very high response rate with around 1,000 responses alongside many views submitted by phone, email and in public meetings we held around the country. It was clear from the consultation responses that there was not a consensus of support for the direct.uk proposals as presented. Although shorter domains (e.g. nominet.uk rather than nominet.org.uk) were considered desirable, many respondents felt that the proposed release mechanism did not give enough weighting to existing registrants, and could lead to confusion if they could not obtain the corresponding domain.

The objective of raising trust/security was welcomed, but many disagreed with the proposed approach, suggesting that standards should be raised across the whole of the namespace. There was significant support for the introduction of address validation for registrants; though some would like us to go further than that and others would like us to carry out the validation process differently. We have published a summary of the consultation responses and analysis of the consultation data on our website.¹

Based on the feedback we received we are going to explore whether it is possible to present a revised proposal that meets the principles of increasing trust and security and maintaining the relevance of the .uk proposition in a changing landscape for domain names. The Nominet Board plans to review progress at their June meeting, where they would consider whether there is an alternative option that addresses the concerns raised in the consultation. Any alternative options would be subject to further consultation prior to any final decision being made.

**Conclusion**

Nominet remains committed to making the UK internet a safe and trusted space for business and consumers. As there is not and will never be a silver bullet to tackle e-Crime and cyber security issues our approach is rooted in providing a robust and resilient service which is enhanced by co-operation across the public and private sectors, supplemented by awareness raising activities to empower businesses and consumers to take practical steps to ensure their own safety and security.

The task of developing a culture in which people’s online behaviour is appropriate to the risks that exist is not one that can be achieved by government action alone, nor can it simply be left to the private sector. We therefore welcome initiatives such as this inquiry that help to raise awareness and, we hope, best practice.

Nominet

March 2013

I am writing to you to follow up on questions you raised during my evidence session to the Committee as part of your inquiry into E-crime.

**YouTube**

YouTube provides a forum for people to connect, inform, and inspire others across the globe. Every day, hundreds of thousands of videos are uploaded to YouTube. In fact, 72 hours of video is uploaded to YouTube every minute. Because of the massive scale of YouTube, it is simply not possible to pre-screen all of the content.

As I explained during the evidence session, to ensure that our Community Guidelines are followed, we have developed an innovative community policing system that involves our users in helping us to enforce YouTube's standards. Every day, thousands of users report potential violations of our standards by selecting the "Flag" link while watching videos. Once a user flags a video, a manual review is triggered, and content that breaks our guidelines is promptly removed. Our global policy enforcement team reviews flagged content 24 hours a day, 7 days a week, routinely removing material that violates our policies.

Once a video that violates our policies is removed from YouTube, it will be blocked from ever being uploaded to YouTube again. Our systems prevent the re-uploading of videos by creating a unique "fingerprint" of every video we remove. If a user tries to upload an identical video again, it is automatically rejected, regardless of whether the user is using a different user or file name. In addition, our policies ensure that users who repeatedly upload material in violation of YouTube's Guidelines have their accounts suspended.

As for the specific content policies that relate to terrorism, our Community Guidelines clearly prohibit videos that promote terrorism, contain hate speech and videos that are posted with the purpose of inciting others to commit violent acts including bomb-making, sniper attacks, or other terrorist acts. We also remove all videos and terminate all accounts known to be registered by a member of a designated Foreign Terrorist Organization (FTO) and used in an official capacity to further the interests of the FTO.

We take this matter very seriously. Hundreds of videos that use the term 'Awlaki' and violate our policies have been flagged by the YouTube Community and subsequently removed from the site by our Removals team.

But we are constantly looking to new ways to improve YouTube, most recently by introducing a programme called 'YouTube Deputise' where we invite a small set of users who flag policy-violating content regularly and accurately to access more advanced flagging tools. Initial feedback from piloting this programme suggests that it has resulted in a fivefold increase in flagging from these users without diminishing the accuracy.

We have invited the Counter Terrorism Unit, CEOP and SOCA to become part of this new system to assist them in flagging videos to us at scale. We think this will ensure that UK law enforcement bodies are even better equipped to alert us to policy-violating content as and when it is uploaded onto YouTube in the future.

There does remain, however, some videos that cite Awlaki or include his words on YouTube. While we will continue to remove content that incites violence according to our policies, material that is newsworthy or that does not promote violence will remain on the site. Our policies aim to draw a careful line between enabling free expression and religious speech or political speech while prohibiting content that incites violence. We strongly believe that YouTube is a richer and more relevant platform for users precisely because of the diverse range of views it hosts.

**Use of Google Ad Grants by UK charities**
Google Ad Grants is a programme whereby any not for profit can apply to receive up to $10k per month of free advertising on our platforms. You can find out more about the programme at www.google.co.uk/grants.

By the end of 2012 we had donated over $33m to over 11,000 UK charities through giving them this free advertising (including the Samaritans).

Sarah Hunter
Head of UK Public Policy
Google
March 2013
Thank you for your letter of March 25th following my evidence session to the Committee in February. The issues raised in the session itself were addressed in my letter of March 19th. To address your additional questions in turn:

**Q:** The default setting on Google+ accounts appears to be public. Would there be any merit in changing this so that information is initially only shared with contacts and altered if the user wishes to make their profile public?

**A:** On the desktop, the initial default for G+ is to share with no-one. The user has to choose which circles, individuals, or broader choices - public and extended circles – they want to share with. Then their selection is sticky, so that next time they go to share something, those same people, circles, and original choices will appear. So if you wanted to always post to friends, you could just select "friends" the first time you post and then that will remain your default until you change it. For mobile, the first time sharing default is with “your circles”, so you do need to change this if you want to share otherwise.

**Q:** Google's data use and privacy policies state that it collects data about the web pages that service users visit. How long does Google store this information for and how does it make sure it is secure? Does Google share it with third parties? If so how does it vet the security of their systems and personnel?

**A:** Like most websites, our servers automatically record the page requests made when users visit our sites. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons, the most important of which are to improve our services and to maintain the security of our systems. We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months). None of this data is shared with third parties.

**Q:** Does Google support Do Not Track technology? Do you think it's important that users should be able to choose privacy above a personally tailored service?

**A:** Our top priority is to protect our users’ privacy and security, and to give them easy ways to control their information when they use our services. We are constantly innovating to find new ways to assist that effort. We added a Do Not Track option into Chrome, and we'll continue working with industry on a common approach to responding to the Do Not Track feature. Over the past year we have introduced a number of other features that seek to ensure users have more control:

- Introduction of a Cookies Consent Mechanism to users in Europe.
- We published information about how Google uses cookies, the types of cookies used by Google, how we use cookies in advertising and how to manage cookies in your browser.
- We added a feature in Chrome that lets you easily manage cookies — just click on the page/lock icon in the left corner of the omnibox to view and control any website’s permissions.
- We implemented the AdChoices icon in the interest-based ads we show in Europe.

**Q:** How many successful hacks have been made against Google in the last year and what types of data were stolen?

**A:** None that we know of, and we look really hard. Our security teams and systems are highly effective at fending off attacks—we have actually detected real attempts that failed. Our security team runs frequent tests to estimate how well we're doing at this detection. We also care about and seek to
prevent attacks against our users, through phishing or other means, even when the attack is not directed at Google.

Sarah Hunter
Head of UK Public Policy
Google
April 2013
E-CRIME ON SOCIAL NETWORKS AND SOCIAL MEDIA SITES

Apologies for the lateness of this information, but I hope the below is of interest to your Committee’s inquiry into e-crime and in particular the increase in the use of the Internet by counterfeiters and pirates.

Established in 1998, the Alliance for Intellectual Property (IP) is a UK-based coalition of 24 trade associations and enforcement organisations interested in ensuring intellectual property rights are valued in the UK and that a robust, efficient legislative and regulatory regime exists which enables the UK to draw the greatest benefits from those rights. With a combined turnover of over £250 billion, our members include representatives of the audiovisual, music, video games and business software, and sports industries, branded manufactured goods, publishers, authors, retailers and designers.

Crime on the internet is affecting our members in a variety of ways:

- Fake and potential dangerous goods are being offered for sale on the Internet via websites or over social media platforms
- Search engines are enabling fraudsters to attract Internet users to illegal sites that offer products for sale or download
- Illegal peer-2-peer filesharing of copyright protected content is continuing
- Online sites are hosting or facilitating the online distribution of protected works without the consent of the rights holder

While copyright holders and brand owners do all they can to protect their products online, assistance is required from others in the online community to ensure that the internet is a fair and safe trading environment for consumers and businesses.

This is especially the case in instances where intermediaries can stand to gain from online IP crime, for example, through the sale of advertising on infringing websites, or from increased web traffic driven to certain sites. We are concerned that such incentives may lead to behaviour that is harmful to consumers and legitimate businesses not being correctly addressed.

An indication of the problems we face – and the assistance we believe is required – is outlined below.

SOCIAL MEDIA SITES: Over the past two years we have seen an increase in the use of social media platforms such as Facebook to advertise and trade in counterfeit goods with thousands of fake items being made available on a daily basis. For example, a recent case in Scotland saw suspected counterfeit goods estimated to be worth almost £20,000 seized by trading standards officers in Moray. The joint operation with Police Scotland came after a trading standards investigation into sales of allegedly fake goods through a local social networking group.

Trade in such fake merchandise is often done via the publication of ‘albums’ (images of the goods available) on Facebook pages set up by counterfeiters. Alternatively, traders can operate a ‘closed’ Facebook page with interested buyers needing to make a ‘friend’ request in order to gain access. Once accepted as a friend, a customer can browse, comment on and purchase fake goods using various payment methods including credit / debit card, Paypal, postal order and cash. The items, in most instances, are then being posted to customers. During investigations of traders engaged in this activity, some brands have found albums containing in excess of 2000 images of counterfeit items available for purchase from a single source.

FACT (the Federation Against Copyright Theft) has also seen a dramatic increase in reports of activity on Facebook where pages or individual profiles are being used to promote pirated content online for streaming, download or access via file-sharing networks.

These social networks allow counterfeit traders and their customers to recommend a trader to other friends and contacts. As a result, many traders have in excess of 1000 ‘friends’ to whom they can ply their trade, gaining, in effect, free advertising.

While Facebook does have a reporting and take down process, it is generally too slow and sometimes takes several weeks to remove offending items, while creating such a page can take a matter of minutes.
DOMAIN REGISTRIES: While it is relatively easy to identify the ISP used to host an infringing website, problems often arise in finding out who is actually responsible for the site itself. This is because as a registrant you can pay for your information to be hidden and to register as a private individual when in fact you are running a business. Inadequate checks are undertaken by domain registrars to confirm that the registration information, personal and financial, is correct. This means that taking action, for example serving legal notices or warnings, against these businesses is very difficult.

Information as to the identity of those behind infringing websites can also be found by doing a WHOIS (ICANN) search. However, again, the effectiveness of this is reliant on the information being correct and up to date.

SEARCH ENGINES: The appearance of infringing sites in search results is of growing concern to rights owners as search engines are increasingly consumers’ first port of call when looking for a product or service. The BPI, which represents the recorded music industry, reportedly sends approx. 3.9 million requests to Google per month of URLs which point to infringing content. FACT also sends notices to Google and other search engines. These search links are subsequently delisted by Google. Whilst Google and other search engines do remove links there is still a reliance on rights owners to proactively find the links.

However, as these URLs only relate to around 150 sites, rights owners believe search engines, as responsible companies, should not only delist the individual URLs but de-rank the actual sites. Google announced last summer a change to its search algorithm which would take into account the number of Notice and Take Downs it received against a particularly site. This information would then be used to de-rank sites against which Google had received a large number of reports. Disappointingly, rights owners report that this change has had little impact. Google’s own transparency report1 demonstrates that they have received over 3.5 million URL removal requests against illegal site filestube.com from over 2400 copyright owners in the last year, yet this site still appears high up in search results.

As these examples demonstrate, the manner in which social media networks, search engines and domain registries operate can create significant challenges. While these issues are not insurmountable, they do require commitment and co-operation from these businesses. If there is greater co-operation, we believe the Internet would be a safer place for consumers to engage in legitimate e-commerce activities, increasing confidence and ultimately allowing for an overall increase in e-commerce.

I would be delighted to discuss these issues further. I will contact your office to see if a suitable time can be found.

Susie Winter, Director General

Alliance for Intellectual Property

February 2013
I am writing to you and your fellow Members on the Home Affairs Select Committee in my capacity as director of the Initiative for a Competitive Online Marketplace (ICOMP). As an organization which is interested, *inter alia*, in promoting privacy and security on the Internet, we have followed your recent hearing on E-crime with a lot of interest. However, we believe that a number of responses from Google’s Head of UK Public Policy, Sarah Hunter were misleading. In order to allow your committee to carry out its important work on the basis of a correct assessment of the factual situation I am writing to you to provide our point of view on these matters.

As you may know, ICOMP is an industry initiative for businesses and organisations involved in Internet commerce. Our mission is to encourage widespread support for principles that are essential to a healthy and competitive online marketplace. To this end, we take a keen interest in data privacy and security as do our members.

During the hearing, it was put to Ms Hunter that Google has faced criticism by 10 Information Commissioners over its attitude to user privacy and had been fined by the United States Federal Trade Commission for bypassing security settings on Apple’s Safari browser. When asked what impression this gave of Google’s respect for user privacy, Ms Hunter expressed “deep regret” for the incidents, saying they were “mistakes and as soon as we identified them, we owned up; we were very public about it.”

We think it is important to point out that Google’s “workaround” was first brought to light by the Wall Street Journal in an article of 17 February 2012 before Google had been “public about it”. The following day, it emerged that, far from owning up and going public, Google had in fact tried to hide the evidence of its misrepresentations by removing cached versions of the opt-out page from Google’s search engine, so that the old opt-out page could no longer be found by means of a Google search. Google responded to these revelations by claiming that the ad cookies “do not collect any personal information.” Chairman Eric Schmidt later distinguished the Safari incident from the “mistakes” over the Wi-Fi data grab, describing the former as “industry practice.” Neither of these claims was accurate and neither, as I’m sure you’ll agree, quite constitutes the immediate and public admission of guilt that Ms Hunter described.

These instances are serious enough in themselves but we believe they are also symptomatic of a broader, far more important and indeed very worrying issue: Google’s attitude towards privacy and its conduct towards the institutions which are tasked with holding them to account.

In recent years, Google has committed a litany of privacy transgressions including the aforementioned Safari and “Spy-Fi” incidents, and more recently the unilateral changes to its privacy policies in contravention of privacy legislation in the UK and the other EU member states. I enclose a copy of ICOMP’s analysis of both the investigation on behalf of the European privacy enforcers including the Information Commissioner into Google’s privacy policy change. I also enclose the response given by Google to the Information Commissioners Office in relation to the ICOs investigation into the above-mentioned Spy-fi incident. These detail the infractions in more detail but in short, Google’s response to each of them has been worryingly consistent. First it attempts to cover-up the facts, next it issues a denial either that the instance occurred or that it had any impact and finally it attributes the breach to a “mistake” on the part of one single “rogue” member of staff. Once each of these statements has been debunked, Google then responds to the ensuing investigation with a calculated strategy of obfuscation and prevarication.

What is so worrying about this attitude is the fact that it shows a deep disrespect for users’ privacy. Such an attitude can only lead to further privacy violations and there is abundant evidence that intrusions into people’s privacy are becoming the order of the day at Google. Indeed almost every privacy watchdog which has investigated Google in recent years has found cause to comment on its unwillingness to cooperate and, in some cases, deliberate efforts to impede proceedings.

---

5 Both not printed
In this regard one can only wonder what the value is of Ms. Hunter’s statement that “user trust is at the heart of our business model”. She went on to claim that “if you think about our businesses, they’re free and there is a lot of competition out there – there are a lot of alternatives – so if our users don’t believe we’re keeping their data safe, they’ll go somewhere else.”

As you may know, the European Commission is currently investigating Google for allegations across Europe that it has abused its dominant position in the market to the detriment of European citizens and the online ecosystem at. Those investigations are based in part on a complaint by ICOMP in which we have claimed that Google’s dominance has partly been created by illegal exclusive agreements to the detriment of what Ms. Hunter called “a lot of competition”. Thanks in part to those agreements Google currently controls over 90% of the search market in Europe.6

It is precisely because there is not that much competition and thus not “a lot of alternatives” that Google is able to continually flout the legitimate privacy concerns of consumers in a way which would destroy any other company operating in a healthy and competitive marketplace. The sad truth is that Google has taken steps to ensure that if, as Ms Hunter says, “users don’t believe [Google is] keeping their data safe” there is nowhere else for them to go and nothing they can do about it. Because of comments such as those at your hearing last week they do not even realise that there is a problem.

We would hope that these comments help your committee see through Google’s attitude towards public authorities and would very much welcome a chance to meet with you on this issue.

Auke Haagsma
Director of ICOMP
March 2013

6 http://gs.statcounter.com/#search_engine-eu-monthly-201108-201207
Thank you for your invitation to provide evidence to the Home Affairs Committee on 16th April. I welcome the opportunity to brief the Committee on the work of the BBA and our member banks to address cyber enabled financial crimes. To inform the discussions, I thought it may be helpful to provide some advance information to the Committee on:

- Supporting bank customers and victims of cyber enabled frauds
- The evolving nature of cyber threats
- The challenges in responding
- The strategic industry approach to financial crime
- Issues for future consideration

**Supporting bank customers and victims of cyber enabled frauds**

BBA members have put in place highly sophisticated security and prevention measures to safeguard customers from online frauds. Banks have also invested in intelligence and analysis systems, recruitment of skilled staff and firm wide training and policies to ensure the most effective strategic defences against financial crimes, as well as working closely with UK law enforcement. These efforts have been essential for driving down online banking fraud losses but also important for maintaining confidence in online banking, particularly given that many customers now use this channel.

Our members see supporting the innocent victims of fraud as a crucial priority. The vast majority of customers that have been defrauded are refunded in accordance with regulatory requirements and banks also provide practical advice and support as appropriate. At the industry level, the BBA works closely with our members to promote best practice for addressing financial crimes including through the guidance materials that we publish.

BBA members are highly committed to raising customer awareness of fraud risks and the “self protection” measures that can be taken. Many banks provide fraud prevention advice on their websites and a number of firms hold awareness raising events for customers. At the industry level, Financial Fraud Action UK (FFA UK) lead fraud prevention efforts on behalf of retail banks and card issuers and have managed a number of awareness raising campaigns including:

- A national campaign, led by FFA UK and supported by the BBA, to raise awareness of the risks posed by criminals that coerce or dupe members of the public into acting as “money mules”.
- A partnership1 between the National Fraud Authority (NFA) and FFA UK that highlighted how cyber criminals steal and use personal information for the purposes of fraud.
- Advice sheets produced jointly by the BBA, FFA UK and the Police, to raise customer awareness of the risks posed by Investment Fraud and a leaflet setting out advice for visitors to Britain.

**The evolving nature of cyber threats**

BBA members have achieved good success in driving down the losses from online banking fraud. However, given the size of the British banking sector and the ever growing number of people who conduct their banking and everyday business online, we recognise that our customers will continue to

1 “The Devils in your Details” campaign
be targeted by cyber criminals. For example, criminals use stolen genuine card details to make fraudulent purchases over the internet via a PC, smart phone or tablet. Criminals also use malicious software and/or ‘phishing’ emails as a means to compromise or steal customers’ sensitive banking credentials to enable fraud and money laundering. Criminals also communicate with each other online to trade data and to share knowledge on offending methods.

As banks have strengthened their controls against cyber enabled financial crimes, the criminals have sought to develop new cyber techniques, such as online social engineering, to dupe or coerce people into divulging personal information or making payments. There is also evidence that criminals are targeting other sectors and businesses that may have weaker controls than banks, to access customer information that can be then used for fraud offending.

Cyber techniques may also be used for attacks against banks that are not financially motivated including:

- **Subversion** (often known as “hactivism”, this is generally carried out as part of a protest. The attackers seek to expose perceived injustice, bad practise and/or exploitation by banks in order to damage their reputation or force changes in policies)
- **Sabotage** (to disrupt the availability of banks online services and content thus eroding customer trust and damaging the organisations reputation)
- **Espionage** (to steal and exploit sensitive information or intellectual property)

**Challenges in responding to these threats**

Whilst BBA members have developed some of the strongest financial crime controls anywhere in the world, there are significant challenges that remain in responding to the cyber criminals including:

- **Rapid evolution in criminal techniques** - Criminals are adopting new cyber offending techniques in response to the counter measures that are put in place, quickly spotting new opportunities and often operating through organised global networks. Highly advanced analytical capabilities are needed in banks, alongside effective intelligence arrangements with law enforcement, to keep up-to-speed with this rapidly changing threat picture.

- **Balancing customer service and financial crime prevention** - There is a challenge in balancing effective measures for spotting and stopping financial crimes with good customer service, as some necessary control measures can cause delays. Our members are constantly striving to ensure that they have the most effective policies and practice in this respect, as well as providing as much information as possible to customers.

- **Conflicting policies and laws** - Compliance with financial crime obligations can at times conflict with other legal obligations on banks. For example, data protection requirements pose challenges to the efficient sharing of information by banks that is needed to spot and stop financial crimes. Similarly, banks are required by the Proceeds of Crime Act to ensure that they do not “tip off” customers that an investigation is taking place whilst also meeting customer demands for detailed explanations when actions have been taken on accounts.

- **Enforcement capabilities** - Often the investigation and prosecution of criminal cases involving cyber crime can be complex, lengthy and expensive, especially where offenders are located outside the UK. Adequate resources are therefore needed to ensure law enforcement is able to provide an effective response to cyber crime cases reported by banks and their customers. This is vital not only for ensuring that justice is served to victims but also to deter potential future offenders.

**The strategic industry approach to addressing cyber enabled financial crimes**
The role of the BBA

The BBA, as the leading association for the banking and financial services sector, supports our members’ efforts to address all forms of financial crime by coordinating strategy and policy, providing guidance, promoting best practice and facilitating operational interaction between banks and law enforcement. The following are some examples of our work in 2012 on fraud matters:

- **Thought Leadership**: We provided a report to the NFA in April 2012 setting out an industry perspective on international fraud threats and challenges, including recommendations for enhanced cooperation between banks and HM Government in this area. The Chief Executive of the NFA in his written response described our report as “well written” and “an example of where work conducted by one sector can highlight wider issues and identify joint working opportunities between other sectors and organisations…..”

- **UK Policy**: In August 2012 the BBA responded to the FSA Guidance Consultation on “Banks defences against investment fraud”. Since our response we have agreed a programme of work with our members to follow up on the FSA recommendations and we are also liaising with the Financial Conduct Authority on this matter. Through 2012 we also provided views to the Home Office on the fraud intelligence arrangements for the National Crime Agency and to the Department of Work and Pensions on the financial crime controls for the Universal Credit.

- **International Policy**: As well as responding to a number of EU level consultations, the BBA supported United Nations work on financial crime in 2012. This included participation in the UN Experts Group on Economic Crime and Identity Fraud and support for an initiative to promote financial crime compliance in the EurAsia region.

- **Industry Analysis**: In December 2012 we provided a report to BBA members setting out analysis of cyber threats and challenges as a basis for strengthened industry collaboration in this area (more details on work in this area are set out below).

- **Operational/practical support**: In early 2012 the BBA established a mechanism with the Metropolitan Police to ensure the most efficient exchange of information with BBA members to prevent financial crimes during the Olympics. Later in 2012 we agreed a new arrangement for the National Fraud Intelligence Bureau to provide fraud alerts to investment banks and smaller banks through an online system managed by the BBA.

The BBA Financial Crime Strategy 2013-2014

Our members recognise the importance of collaboration across the industry on financial crime. With this in mind, the BBA Board in October 2012 agreed a two year strategy to address financial crime comprising the following priority initiatives:

- **An Annual BBA Financial Crime Report** to publicly outline how the industry is responding to financial crime, the challenges we face and our future priorities.

- **A review of industry intelligence arrangements** for financial crime, to enhance industry knowledge of emerging financial crime risks.

- **Dialogue with the Home Office** on BBA proposals for improvements to the legal and policy framework for financial crime and on bank partnership with the National Crime Agency.

---

2 Our portfolio includes work to tackle bribery, corruption, fraud, money laundering, terrorist financing, cyber crimes and physical crimes.

3 BBA report titled “Defining the cyber threats and challenges to the banking sector”
• **Proactive engagement with the Financial Conduct Authority** to support our members to understand and meet Regulatory expectations on financial crime.

• **Intensified BBA led engagement with EU and international bodies**, to promote public/private partnerships at the global level to address financial crimes.

The BBA Financial Crime Policy Group acts as our key oversight committee for delivery of the strategy, though regular reports will be provided to the BBA Board over the coming years. Consideration of cyber crime is an intrinsic element of our strategic approach in this area given that criminals employ cyber techniques for a range of financial crimes, particularly fraud and money laundering. The BBA has also recently established a new dedicated Cyber Advisory Panel, bringing together senior bank representatives to coordinate industry strategy and policy on strategic cyber security and cyber risk management issues.

**Our partnership with Financial Fraud Action UK**

The BBA works closely with FFA UK to support our members’ efforts to address cyber enabled frauds. Key areas of collaboration include:

• **Campaigns to raise customer awareness of fraud** and promote bank best practice

• **Promoting the sharing of knowledge and expertise** within the banking sector on emerging fraud threats

• **Developing common approaches on fraud policy issues**, including joint representations to UK and international bodies where appropriate

The FFA UK and the BBA will continue to work together to promote effective fraud prevention and raise customer awareness of emerging risks. Whilst the BBA and FFA UK have some common retail bank members the BBA also is keen to further ensure that investment bank, smaller bank and private bank members are brought into industry level initiatives where appropriate.

**Areas for future consideration**

The BBA welcomes the proactive approach of HM Government to engagement with the private sector on cyber crime matters. In particular, the BBA is pleased to be participating in the recently formed Cyber Crime Reduction Partnership that brings together industries, HM Government and academia to develop collaborative efforts to address cyber crimes.

Beyond this, we would suggest that the following could be considered to strengthen our collective capabilities to address cyber offending:

**Intensified public awareness campaigns**

Whilst recent banking industry led campaigns have successfully raised public awareness of cyber crime risks, there is a need for an intensified multi-sector approach to ensure that members of the public better understand the threats they face. Further targeted campaigns are needed to ensure that prevention messages are reaching key audiences, such as younger online users and the vulnerable.

**Reforms to the legal and policy framework**

BBA members are of the view that government should consider possible improvements to the legal and policy framework for financial crime. Specifically there may be merit in considering updates to the Proceeds of Crime Act, to ensure it is up-to-date with modern financial crime offending techniques. Policy or legislative change may also support a more effective balance between data protection obligations and the requirement for firms to share information to address financial crimes.
Enhanced investigation and enforcement capabilities

The establishment of the National Crime Agency is a real opportunity to develop the highest quality capabilities for investigation and enforcement against cyber offenders. BBA members are keen to support the strengthening of enforcement capabilities by putting in place the strongest possible information exchange mechanisms and through the exploration of potential “two-way” sharing of staff between the National Cyber Crime Unit in the NCA and BBA member banks.

A coordinated global partnership

Given the global nature of cyber offending and the widespread harm it causes, the BBA is of the view that a coordinated international multi-sector approach is required. The UN Experts Group on Cyber Crime may provide a useful mechanism for international policy development but we believe that beyond this can be done globally at a practical level. This could include sharing of knowledge between different sectors to enhance understanding of emerging cyber offending techniques, improvements to international standards for addressing cyber crimes and the promotion of greater public awareness of cyber crime risks.

I hope this provides useful supporting information to the Committee and I look forward to discussing these issues further on 16th April.

Anthony Browne
Chief Executive
British Bankers’ Association
April 2013
Further to your letter of 25 March 2013, I have provided further information from Facebook relating to your inquiry:

1 Facebook user numbers in the EU: Facebook does not provide public data on the number of active Facebook users in the European Union as a whole. However here are the monthly active user numbers for the largest five markets in the EU made public at the time of our most recent quarterly results:

   UK 33 million
   France 26 million
   Germany 25 million
   Italy 23 million
   Spain 18 million

2. HTC phone and pre-installed Facebook features: In retrospect, Mr Ruane’s question was probably prompted by press speculation about a product launch, which was pure speculation on the day of the hearing itself. On 4 April 2013, Facebook announced the launch of Facebook Home. This will come preinstalled on HTC phones in the US. It can be turned off at any point by the user and can also be uninstalled at any time. When Facebook Home is active, we will log information about the user’s activity on Facebook's suite of products. In addition to the standard information we log with all our apps, we will also log notifications and app information when they interact with Facebook Home. We do not log or track the user when they use apps independent of Facebook on the phone.

3. People reporting crime on Facebook: While Facebook makes it easy for people who use our service to report potential abuse or violations of our terms of service, we do not have any specific data which relates to the Committee’s question about reports of crime. Instead our Help Centre advises users to contact local law enforcement if they wish to report a crime. An example of that advice is shown in the screenshot below, from the Help Centre, relating to human traffic
How do I help someone who may be a victim of human trafficking or has posted suspicious content related to human trafficking?

If you encountered content or photos that indicate someone is in immediate physical danger related to human trafficking, please contact 911 or local law enforcement for help.

Facebook is working with the National Human Trafficking Resource Center, operated by Polaris Project, to provide resources and assist victims of human trafficking. To learn more about the signs of human trafficking, visit http://www.traffickingresourcecenter.org or contact the National Human Trafficking Resource Center at 1–888–3737–888 to learn about local resources and discuss options.

If you're a victim of human trafficking or would like resources to share with a potential victim, please review the following resources:

**United States**
National Human Trafficking Resource Center
http://www.traffickingresourcecenter.org
📞 1–888–3737–888
✉️ nhtrc@polarisproject.org

**Canada**
Contact Canadian Crime Stoppers
📞 1–800–222–8477 (TIPS)

**Latin America**
Bilateral Safety Corridor Coalition (BSCC)
http://www.bscccoalition.org
📞 619–666–2757
✉️ info@bsccinfo.org

**United Kingdom**
Blue Blindfold UK
📞 0800–555–111

4. Data collected when people use other sites: All the questions raised under this point are addressed in considerable detail in two reports of the Office of the Irish Data Protection Commissioner (I-DPC) in December 2011 and September 2012, which can be accessed at the links below, including detailed, independent technical appendices. Both reports and their technical appendices were published in full.

http://www.dataprotection.ie/docs/Facebook_Ireland_Audit_Report_December_2011/1187.htm
http://www.dataprotection.ie/docs/Appendices_to_Facebook_Ireland_Audit_Report_Dec_2011/1188.htm
In summary:

- Facebook’s Data Use Policy states that we delete or anonymize data collected through social plugins on other sites within 90 days. This has been verified by the I-DPC.
- The I-DPC reviewed Facebook’s data security operations and concluded that: *It is important to state at the outset that as could be expected FB-I places an enormous and ongoing focus on the protection and security of user data. Our audit has confirmed this focus.* (December 2011 report, para 3.9.4)
- And further: *The majority of the controls described by FB-I appeared to this Office to be effective. It can be reasonably concluded that if large-scale, frequent data breaches were taking place on Facebook’s corporate networks, that this would be widely reported, particularly considering Facebook’s global profile. Since this is not the case, the information security controls in Facebook appear to be preventing these types of incidents.* (ibid, para 3.9.6)
- Facebook does not share information collected via social plugins with third parties over and above the information shared by an individual making use of those websites. This extract from our Help Centre makes this clear and explains the reasons we collect this information:

**What information does Facebook get when I visit a site with the Like button or another social plugin?**

If you’re logged in to Facebook and visit a website with the Like button or another social plugin, your browser sends us information about your visit. It’s important to note that Facebook is not retrieving this information. Rather, since the Like button is a little piece of Facebook embedded on another website, the browser is sending information about the request to load Facebook content on that page.

We record some of this information for a limited amount of time to help show you a personalized experience on that site and to improve our products. For example, when you go to a website with a Like button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you’re visiting, the date and time and other browser-related information.

If you’re logged out or don’t have a Facebook account and visit a website with the Like button or another social plugin, your browser sends us a more limited set of information. For example, because you’re not logged into Facebook, you’ll have fewer cookies than someone who is logged in. Like other sites on the internet, we receive information about the web page you're visiting, the date and time and other browser-related information. We record this information for a limited amount of time to help us improve our products. For example, we sometimes find bugs in the systems we’ve built to gather aggregate data on how people are interacting with sites that use the Like button or other social plugins. It’s helpful to be able to reference this anonymized information when investigating these bugs so we can find their sources and fix them quickly.

As our [Data Use Policy](#) indicates, we use cookies to show you ads on and off Facebook. Regardless of whether or not you’re logged in, we don’t use the information we receive when you visit a site with the Like button or another social plugin to create a profile of your browsing behavior on third-party sites to show you ads. However, we may use anonymous or aggregate data to improve ads generally and information we receive to study, develop or test new and
existing products or services. We delete or anonymize the information we receive within 90 days, and we don't sell it to advertisers or share it without your permission.

5. Do Not Track (DNT): Facebook believes in the importance of user control of data about them and therefore we are supportive of the efforts of stakeholders, including at the World Wide Web Consortium and the Digital Advertising Alliance, to develop a standard for DNT that will enable people to control their information as they browse the web. We are actively involved in those industry-wide discussions, which cover many difficult technical questions that will need to be resolved before any DNT standard can be adopted.

6. Review processes for Facebook apps: Facebook provides extensive information to users in respect of applications, including the data being shared with each application upon its installation. Applications can only be installed once the user has given permission for such sharing. The policies which developers have to comply with are clear and we take a number of steps to enforce them. Our actions in this respect were audited by the I-DPC and this excerpt from the audit report summarises the I-DPC’s assessment:

"The role of Platform Operations is to enforce Facebook’s Platform Policy, interacting with developers of third party apps and developers using the social graph, i.e., social plugins, to ensure adherence to Platform Policy. An examination was conducted of the work queues of the Platform Operations Team. It was noted that Facebook has now introduced a number of automated tools, developed in Dublin, to proactively and automatically identify and disable applications engaged in inappropriate activity such as spamming friends or friends of friends, excessive wall posting, etc. The Team also responds to specific user complaints regarding the behaviour of applications and enforces a graduated response against the application and the application provider depending on the nature of the contravention of the Platform policy. We examined one complaint from a user in relation to unauthorised use of Intellectual Property by another developer which was received on 9 November and action was taken to delete the application within 2 hours. The account of the developer was disabled and all other applications which they had developed were also subjected to review. We also examined a phishing complaint received from a user who reported an application trying to retrieve their email and password. The application was immediately disabled and further action taken. It was also pointed out that in line with Facebook’s real name culture that all applications (even those developed by the large games developers) must be developed by and attributable to an identifiable user on Facebook." (December 2011 report, para 3.6.5)

7. Reports of hijacked accounts or scams: Anyone believing that their account has been hijacked or hacked is advised on our Help Centre to go to: www.facebook.com/hacked where they can manually lock down their account with immediate effect, reset their password and take other steps to secure their account. Any user reporting that their friend’s account may have been hacked is provided with the same advice – ie their friend should take these steps. We also take a number of preventative steps to guard against the possibility of an account being hacked:

- **Recognised devices:** Facebook allows people to register devices that they use Facebook on regularly.
- **Remote log-out:** If someone forgets to log out of Facebook, they can remotely log off any live session they have running by accessing this tool in their security settings
- **Secure browsing:** Facebook encourages all users to turn on secure browsing for added protection (add ‘s’ to the end of http in their browser address)
8. **Hacks against Facebook:** Security is a top priority for us, and we devote significant resources to protecting people's accounts and information. We maintain a strong relationship with security experts around the world and work closely with them in the rare instances in which they find vulnerabilities on Facebook. We’ve created a simple form for these people to contact us that we link to both from our Help Centre and from the “Whitehats” tab on the Facebook Security Page [https://www.facebook.com/whitehat](https://www.facebook.com/whitehat). We also recently rewrote our responsible disclosure policy to make it even easier for researchers to let us know when they find a vulnerability, so we can fix it quickly and before it is exploited.

I hope that this further information is useful to the Committee.

Simon Milner  
Policy Director, UK  
Facebook  
April 2013