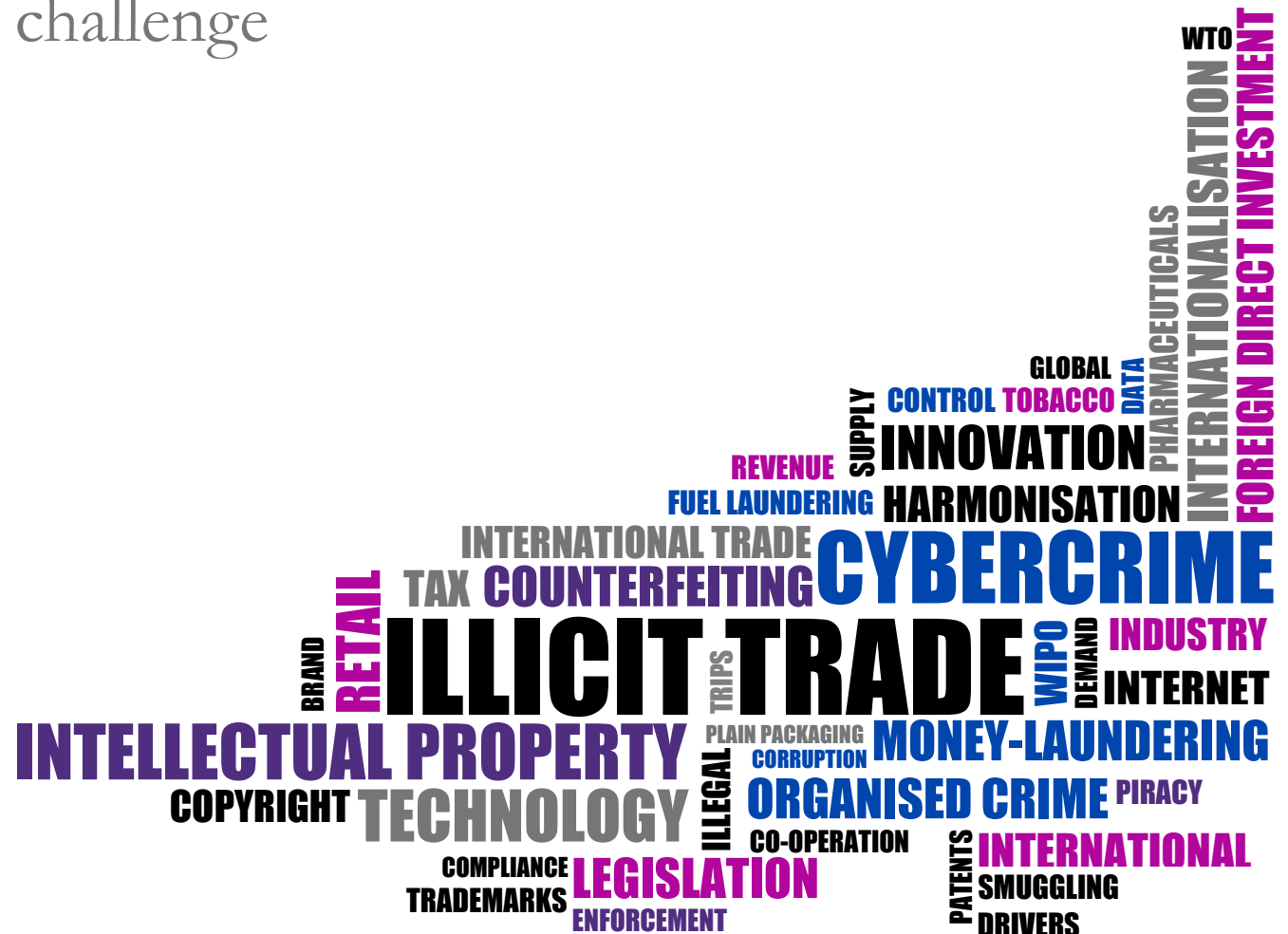
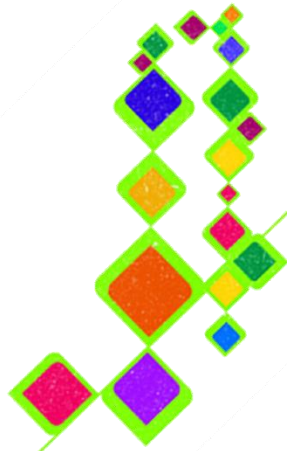




Illicit trade

an Irish and global challenge





Contents

	Page
Contents	1
Introduction	2
Executive summary	3
Key statistics	6
1 Intellectual property crime	7
2 Cybercrime	17
3 Money laundering	31
4 Retail update	45
5 Conclusion	61
About us	65
Notices	68
Bibliography	69

Introduction

In 2013, Grant Thornton and Retail Ireland presented a report on illicit trade in Ireland. In the report, entitled “Illicit trade in Ireland - uncovering the cost to the Irish economy”, we focused on a number of areas in the retail sector. The objective of the 2013 report was to highlight the cost of illicit trade to the Irish economy and provide a detailed assessment of the problems faced by the selected sectors, namely: fuel, tobacco, digital piracy and pharmaceuticals. Although the report focused on specific sectors, a recurring theme of the report was the international nature of illicit trade. This report builds on research previously carried out by Grant Thornton and extends the discussion to the broader and more international dimensions of illicit trade with a focus on the core challenges for Ireland.

Fuelled by the same forces that encouraged international trade (increased access to markets, people, ideas and capital), illicit trade continues to grow both in scale and scope undermining the competitiveness of the global economy. By its very nature, illicit trade is difficult to quantify which presents problems for economic policy making and research. But beyond this, the unregulated trade imposes enormous revenue losses for governments which directly affect its debt levels and ability to fund socially beneficial programmes such as healthcare or education. In parallel, it creates a supply of products that require to be highly regulated or are often illegal in the first place, thus impinging on our society.

Global business optimism and growth indicators continue to improve and internationalisation is again in policy makers minds. In the last number of years, the Irish approach to international trade has been extremely business friendly which is reflected in its 28th position in the World Economic Forum global competitiveness index and 1st in Forbes “best countries to do business”.

Despite these positive indicators, both Ireland and the international community need to be mindful of the increased risks posed by illicit activity and protect themselves from being exploited by criminal elements of society. As a small open nation with a limited domestic market, free trade and internationalisation is of vital importance to the continued growth of the Irish economy. Added to this is Ireland’s dependence on Foreign Direct Investment (“FDI”) in terms of employment, capital investment, and other positive externalities such as technology and education spillovers, increased competition and benefits for suppliers.

There are a number of emerging trends in the area of illicit trade and intellectual property (“IP”) crime that need to be considered, such as:

- 1 changing means of access and consumption;
- 2 new technologies;
- 3 increased user involvement;
- 4 shifting business models; and
- 5 an increasing global market.

In the context of these trends and evolving nature of illicit trade together with the increased competition for FDI, Ireland, we need to remain vigilant to maintain its attractive position for foreign investors. In our 2014 report we begin by exploring illicit trade in the context of intellectual property crime, the emerging trends and the importance of intellectual property protection from an international perspective. We then focus on the rising issue of cybercrime, which has broken down previous barriers. Next, we look at money laundering and how the emergence of new developing economies has had an impact on the financial markets. Finally, we provide a recap of the key issues from 2013 and assess key developments that have occurred in these areas.

We hope this report will help policy-makers and businesses to better understand the international issue of illicit trade and support informed decision-making.



Brendan Foster
Partner
Business Consulting and Advisory
Grant Thornton

Executive summary

The growing threat of illicit trade and intellectual property crime is a real issue for the international community. This report focuses on the challenges currently facing both the Irish and international community across a number of different areas. Ultimately this report puts forth a number of key recommendations to help address these challenges. The specific focus has been on the areas of intellectual property crime, cybercrime, money laundering and retail.

Intellectual property

It is widely accepted that the recognition of intellectual property plays a vital role in promoting innovation, providing economic stimulus and attracting international FDI. Despite the importance of IP, the international IP protection framework is falling behind and there continues to be widespread abuse of IP rights. Having a strong IP framework that protects right owners has significant positive benefits for countries through increased innovation and attracting foreign direct investment. With IP abuse not being restricted to any particular sector it has far reaching impacts on an economy, especially those economies with industries dependent on IP such as Ireland.

Ireland has the largest contribution to GDP of IP intensive industries in Europe

A fundamental issue with the international nature of IP protection is that rights granted in one nation are not necessarily recognised in another. For less developed countries there is less of an incentive to have a strong IP framework, which protects these rights, than for more developed countries. The main reason for this

Internationalisation has facilitated the global growth of illicit trade

is that these less developed countries seek to gain access to valuable foreign intellectual property to stimulate the country's development. This, however, in turn leads to the theft of valuable IP and the supply of products infringing IP.

Whilst progress has been made at an international level to improve cross border IP protection, statistics show increasing numbers of items being seized by customs officials as a result of IP infringement. Increased harmonisation of IP laws and

international agreements with real power to enforce law are needed to stop further growth of IP crime. Beyond this there needs to be increased collaboration with developing countries in the development of IP protection.

Cybercrime

Cybercrime is heavily impacting on the economies, both in Ireland and internationally. We have estimated it could be costing the Irish economy as much as €630 million annually. Its international nature makes it difficult to prevent particularly in a small open economy like Ireland. It is, however, critically important for Ireland to lead in the international fight against cybercrime. Ireland's fast growing technology sector is a key driver in our economy. Our government needs to legislate appropriately, businesses need to detect and prevent cyber-attacks and our work force needs to be aware of and have the skills to fight cybercrime and secure online systems. This combined approach can help Ireland to protect its businesses and consumers in the online world and protect technology and intellectual property driven foreign investment. More specifically:

Cybercrime is costing the Irish economy €630 million annually

- Ireland needs help with ensuring international harmonisation of cybercrime laws. In particular, Ireland should implement the 2005 EU Framework Decision on attacks against information systems including mandatory data breach disclosure;
- Ireland should urgently develop and publish a national cyber security strategy. This is a plan designed to improve the security and resilience of Irish national infrastructures and services. It should establish a range of national cyber security objectives and priorities to be achieved in specific timeframes;

- Irish businesses should be focusing their planned cyber security investments on the ability to detect and react to data security breaches. In the current environment, it is not a question of will an Irish business be subjected to an online attack but a question of when? The ability of the business to detect and react to the attack will be the key factor in limiting the impact of the cybercrime; and
- ensuring appropriate education of the impact of cybercrime on Ireland is key.

Money laundering

A critical element of decreasing illicit trade is to not only limit the opportunities for criminals to profit from illicit activities but to also ensure that proceeds from illicit trade cannot be used by those criminals. In this report we have estimated that over €5.4 billion was laundered in Ireland in 2012 alone.

The aim of preventing criminal proceeds from entering the legitimate financial systems can only be achieved through the implementation of strong anti-money laundering (“AML”) legislation. Strong legislation and compliance has a significant impact for the overall economic environment.

Over the past number of years Ireland has made significant progress in terms of bringing its anti-money laundering regime in line with the EU regulations through the introduction of the Criminal Justice Act (CJA) 2010 and CJA 2013. Despite this progress, our analysis of the performance of both the Irish current and historic AML regimes suggests that, whilst constantly improving, there are still areas that require further attention. Specifically, these areas include

- legislation: with the Fourth EU AML Directive underway, Irish regulators should be prepared to promptly update the existing regulations;
- reporting by the compliance and enforcement bodies: a more thorough compilation of data is required to reflect the true and fair scope of the money laundering issue in Ireland;

AML has only recently become a priority and remains underdeveloped

- reporting by the designated persons: the issues of under-reporting and reporting of activities not related to money laundering need to be addressed primarily through education and feedback;
- education: whilst some guidance has been provided to designated persons in Ireland a more dialog-like approach is recommended to ensure full understanding of the regulatory requirements;
- creation of a culture of compliance: providing training to companies around the problem of money laundering to facilitate a thorough understanding of responsibility and reporting obligations; and
- collaboration: a more co-ordinated approach is required to ensure that the issue continues to be addressed appropriately across agencies and industries.

Raising awareness and training will be key to improving our AML systems

Retail

Illicit trade in retail products shows no signs of abating. In 2013, we estimated that this could be costing the Irish economy as much as €1.48 billion. In 2014, we estimate that the losses to the Irish economy are in the region of €1.53 billion as highlighted in the Table below.

Table 1 - Cost of illicit trade¹

	Right holders/retailers Lost revenues, €'m		Government Loss to the Exchequer, €'m		Total loss to the economy, €'m	
	Low	High	Low	High	Low	High
Fuel laundering	€112	€205	€142	€261	€254	€466
Tobacco	€54	€122	€240	€575	€294	€697
Digital piracy	n/a	€260	n/a	€57	n/a	€317
Pharmaceuticals	n/a	n/a	€25	€53	€25	€53
	€166	€587	€407	€946	€573	€1,533

In terms of the incentive for the supply and demand of illicit products in the retail sector, price remains the main driver to partake in illicit trade and no material changes have been made to address this issue since last year.

Whilst there have been some efforts to improve legislation and enforcement across the sectors reviewed, the fundamental problem of unaligned, unbalanced and sector specific strategies continues to exist. It is likely that without stronger penalties and enforcement, in addition to a joined up approach to address the issue across various sectors, illicit trade will continue to grow.

The need for a new strategy

Since our previous report, little has been done to address the increasing challenges faced to address the growing issues of intellectual property crime. There are a number of global trends that are having an impact on the Irish economy beyond purely retail.

The issue of illicit trade has a real impact on international trade and attracting inward investment. Ireland needs to be proactive in its efforts at both domestic and international level in order to ensure that we meet the dynamic needs of consumers.

IP is vital to attracting and keeping FDI

To tackle illicit trade, a comprehensive legislative framework and enforcement measures are required regarding IP infringements, production, distribution and purchase of illicit products is in place. Through the introduction of a consistent and evidenced based approach to the problem across all industries, we believe that it is possible to more effectively target the drivers behind illicit trades, learn from the

International harmonisation of regulations is required to facilitate the global efforts to tackle illicit activities

lessons from other industries and enable Ireland to become more proactive in the fight against illicit trade. In last year's report, we put forth an eight step strategy to tackle illicit trade and we believe that this strategy merits discussion at the highest level. This 8 step strategy is illustrated by the diagram across.

At a domestic level, it is recommended that a committee be established, comprising of both sector and state interests, which would have direct responsibility for illicit trade in Ireland across the spectrum of industries suffering from illicit trade. The

objective of the committee would be to facilitate information sharing and to ensure that there is a more proactive and aligned approach taken to tackling all areas of illicit trade.

Ireland, through the EU, needs to influence the global international IP system. Ensuring that there is more consistent and effective enforcement of IP laws in developing economies will be a critical element of this.

Any measures that are introduced need to be flexible to meet both the changing pattern of consumer's behaviour and the needs of businesses, whilst at the same time consider the balance between industrial and development priorities of the developing countries with weak IP laws.



Key statistics

The scale of illicit trade operations globally is enormous. It results in significant financial losses to the international and domestic communities and businesses. It supports organised crime and affects the overall wellbeing of the global population.

This page presents the key statistical highlights of the report and aims to show a bigger picture to help the reader to appreciate the scale and the impact of illicit trade.

Cost of IP crime
Up to 7%
Of Global GDP

Up to
5% of
Global GDP
laundered

Costs of Cybercrime
€241bn
to the global economy

Average cost of a databreach for a business is
€3m in
the US

IP intensive industries create
90% of
EU exports

An estimated
€5.4bn
laundered
in Ireland 2012

Costs of Cybercrime
€630m
to the Irish economy

Loss to the economy due to fuel laundering
up to €466m
in Ireland

€390m
Cost of illicit tobacco
to the Irish economy

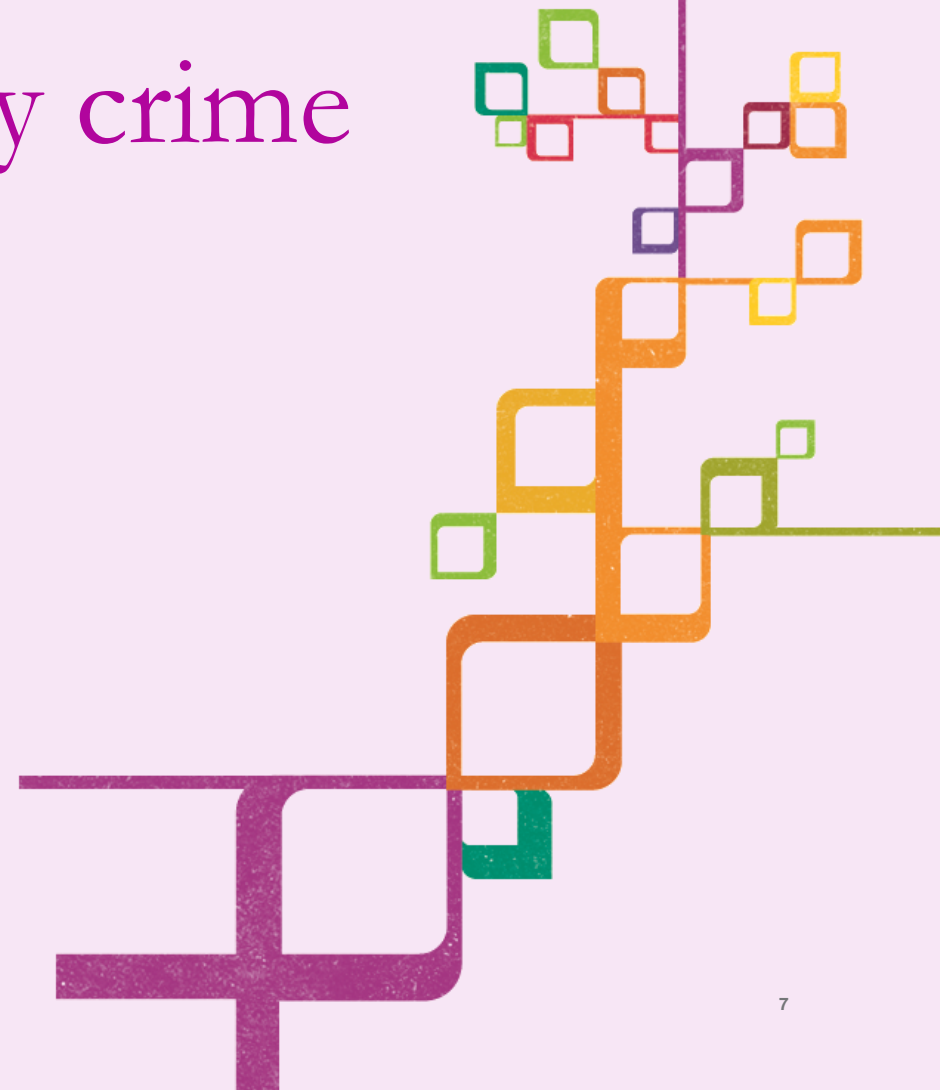
64% of
consumers believe
stricter fines and
harsher laws
will help to diminish
illicit trade

7 out of 10
consumers believe
illicit trade supports
organised crime

23% of
consumers in Ireland
knowingly
purchase illicit tobacco

23% of
employment
in Ireland is in
IP intensive
industries

1 Intellectual property crime



Intellectual property crime

Intellectual Property (“IP”) is a valuable asset and is increasingly the subject of abuse and infringement. As we move towards a more global and knowledge based economy the importance of IP and its protection is fundamental.

In our 2013 report we focused on the importance of IP in the context of illicit trade in Ireland and highlighted its significance for the domestic economy. Our estimates suggested that the total cost of intellectual crime in tobacco, pharmaceutical and digital areas could be costing the Irish economy up to €1 billion² annually. These costs threaten to undermine the significant benefits of IP to the Irish economy.

IP is an integral part of international trade. The protection of IP has become an important element in the decision-making process for international companies in deciding where to invest. Increasing globalisation and the borderless nature of the internet has created opportunities for business but it has also created challenges. For this reason we have expanded our analysis to take into account the role of IP for international business and Ireland in the global context.

Types of IP

- **copyright:** an automatic right covering a wide range of works including literary, artistic, dramatic and musical works, sound recordings, films and broadcasts.
- **trademarks:** a monopoly right that protects symbols (logos and brand names) which distinguish goods and services.
- **patents:** an exclusive right that allows the patent holder to limit use of specific inventions by others. Available for up to 20 years on payment of renewal fees. Longer term protection also possible, e.g. for pharmaceuticals.
- **design rights:** can be a monopoly or non-monopoly right. Protect the overall visual appearance of a product.

Despite the importance of IP, the international IP framework is falling behind and there continues to be widespread abuse of the IP rights. International estimates have put the cost to the global economy to be in the region of 5% to 7% of global trade.

In the context of escalating illicit trade, both domestic and international, we evaluate the importance of IP to the economy, identify the ways in which it is abused and assess the efforts to combat the problem. Finally, will provide some recommendations as to what could be done to improve the IP framework by policy makers in Ireland to ensure that we have a state of the art IP framework that continues to attract investment from foreign investors and promotes innovation.

Importance of IP in international business

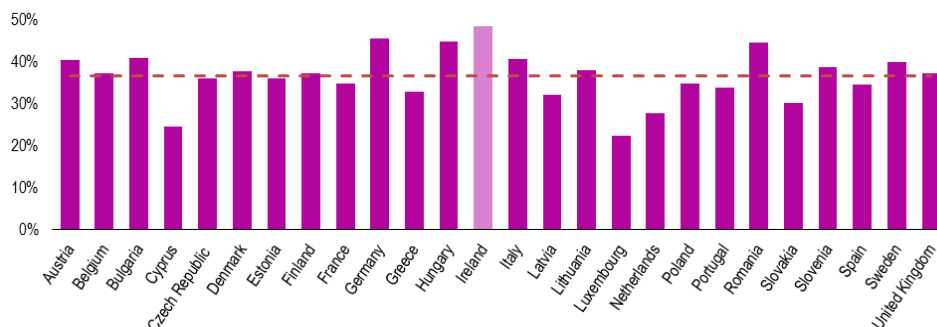
Increasingly IP is a feature in both developed and developing economies across the world and its importance cannot be underestimated. The evidence suggests that having a strong IP framework enables countries to attract greater inflows of international capital investment. This investment in turn encourages international distribution and marketing networks that are critical to building larger markets and improved economies of scale that drive internationalisation.

Data released by the European Patent Office which compares the relative share of Gross Domestic Products (GDP) for IP intensive industries highlights the importance of IP for European countries (See Figure 1.1). The striking observation from this data is the fact that it is Ireland that has the highest contribution from IP intensive industries in percentage terms in the EU, with almost 50% of total Irish GDP and over 23% of the total employment³ coming from these companies. This fact highlights the importance of IP protection for Irish business and its investors.



Intellectual property crime

Figure 1.1 – GDP share of IP intensive industries⁴



The importance of IP

- encourages innovation
- drives economic growth and competitiveness
- differentiates Irish products in the international marketplace
- creates and supports jobs
- incentivises education
- rewards entrepreneurs
- helps incentivise the search for solutions to global challenges
- encourages Foreign Direct Investment

Although it is established that a strong IP framework is essential for developed countries, for developing economies IP laws can actually have a negative impact on economic development specifically in the area of technical change. Weak rules on IP can favour information transfer through the low cost imitation of foreign products and technologies as domestic invention and innovation is insufficiently developed and does not require protection. This enables countries to advance its own technological development through infringing on foreign IP and promoting illicit trade. As they move up the development scale, a strong IP framework increasingly becomes more important as they begin to attract increased FDI flows and foster their own innovation. It is therefore important that the international community works with these emerging countries to ensure a balance is struck between industrial development priorities and better national regimes for the enforcement of IP.

For Ireland, as developed economy with a high dependence on IP intensive industries (see Figure 1.1) a strong national framework for the protection of IP is of vital importance to its continued success, notably in the context of increased competition for FDI. IP protection is a prerequisite for Ireland's continued innovation and economic growth. Ireland therefore needs to be proactive in its efforts to improve IP protection domestically and, through the EU, promote more global harmonisation and enforcement.

International abuse of IP

“IP crime has long been a problem in the world of physical goods, but with the growing use of the internet, online IP crime is now an increasing threat to our creative industries.”

UK, Minister for IP, Lord Younger

With IP being inextricably linked with a variety of business sectors, there are numerous ways it can be infringed - from the simple private use of protected content (i.e. digital piracy), the actual production of products using protected elements (i.e. counterfeiting) and sale in unauthorised regions (i.e. smuggling). The issue of international abuse of IP is further complicated by the international nature of IP, differences between laws in different jurisdictions and the erosion of traditional borders.

Although there are various factors that contribute and facilitate IP crime, financial incentives remain the major driver of IP rights abuse for consumers and suppliers (most notably in developing countries that lack strong IP regulations and enforcement).

An inherent characteristic of any illegal activity is that it is not properly recorded. As a result it is not possible to provide an accurate estimation of illicit trade. Various estimates suggest that the total economic value of counterfeit and pirated products can be anywhere between 5% to 7% of the world trade. Table 1.1 provides a summary of some estimates of the scale of IP abuse.

Intellectual property crime

Table 1.1 - Estimates of the scale of illicit trade

European Commission	Between 5% and 7% of world trade, representing €200 billion to €300 billion in lost revenue and the loss of 200,000 jobs worldwide
World Customs Organisation	Around 5% of world trade
OECD	More than 5% of world trade
The International Anti-Counterfeiting Coalition (IACC)	5% to 7% of world trade
International Chamber of Commerce	\$650 billion (2010), growing to \$1.77 billion by 2015 ⁵ .

Regardless of the estimate used, it is clear that at an international level the scale of this crime is huge. As a result of the enormous size of IP abuse in the world, significant losses are seen by private sector businesses, governments and customers in addition to the intangible non-financial damage. The international protection of IP, therefore, is an important factor in ensuring business development, innovation and ultimately growth.

Trends in the area of IP

There are a number of trends that are having an influence on the international abuse of IP. Globalisation, changing means of access and new technologies are just a few of the trends affecting the IP landscape. To understand the abuse and potential opportunities in IP it is necessary to assess the forces that are shaping the environment where IP is created and distributed. In the Table 1.2 opposite we identify the key trends and factors affecting IP and assess the implications of each.

Table 1.2 - Key trends^{6 7}

	Description	Implications
Changing means of access and consumption	Technological developments such as internet, wireless access, mobile devices, cloud computing and social networks allow for instantaneous access to and quick distribution of information stored anywhere in the world.	IP regulatory frameworks lag behind and are not reflecting the new consumption models.
New technologies	Development of new technologies stimulates creation of new content, distribution of it and access to it in new more efficient ways.	Easy to make copies of content and transfer it.
Increased user involvement	Increase in the amounts of shared content and dissimulation of borders between users and creators.	Facilitates creation of new complex contents, yet results in difficulties with respect to ownership and rights to this content.
Shifting business models	There has been a shift to electronic distribution and resulting from it decrease in the marginal costs to produce and distribute an additional copy of digital content. Move from sale of physical copies to sale of a licence and a right to access content.	Ease of access and variety of choice. Traditional distribution channels such as rental shops are going out of business; licencing agreements result in lack of flexibility for users in terms of use of the contents.
An increasingly global market for content	Internet enables content to move freely across various countries therefore creates a global market for the creative content and provides access to larger audiences.	Lack of cross border IP protection mechanisms to reflect the global nature of the modern IP.
Increased fragmentation of copyright ownership	Increased user involvement and large amount of content available online results in this content being used to create new products.	Regulations need to ensure that the rights of the owners of the original content are protected.
Growing importance of brands	The value of brands has increasingly grown and is often companies most valued asset.	The production of counterfeit products is a major issue with a high number of infringing products being traded.
Patent backlogs	Patent offices across the world have seen large increase in applications over the past number of years. As a result, they have built up significant backlogs.	The large backlog delays innovation and can adversely affect economic growth.

What we have seen from our analysis of IP trends is that the legislative frameworks need to continually evolve in order to keep pace with how content is

Intellectual property crime

created, distributed and consumed. To do this, it is important that business and governments have in place flexible structures and mechanisms both at a national and international level.

International structures and mechanisms

The fundamental issue with international IP protection is that IP rights granted in one nation are not legally recognised and enforceable in another. Without appropriate mechanisms at an international level to ensure cross-border compliance and enforcement, IP abuse will continue unabated. Cross border compliance and enforcement is a real challenge to effective IP protection and continues to be a barrier to international trade. In this section we therefore identify and assess the contribution of the existing organisations, legislation and enforcement measures to international co-operation to protect IP.

International organisations

IP crime is a clearly identified international issue and there are several institutions and treaties that govern IP at a global level in an effort to facilitate its protection. Although there are a number of international institutions, the two most important are the World Intellectual Property Organisation (WIPO) and the World Trade Organisation (WTO).

WIPO is a United Nations' agency that is devoted to stimulation of innovation and creativity through the use of IP. WIPO and its members aim to improve understanding and the respect for IP. It closely co-operates with Interpol, the World Customs Organisation, the International Chamber of Commerce/Business Action to Stop Counterfeiting and Piracy (ICC/BASCAP Initiative) and the International Trademark Association (INTA) to develop a coordinated solution to combat counterfeiting and piracy⁸.

WTO is an international organisation dealing with the rules of trade between nations. Its primary function is to administer the international Trade Related Aspects of IP Rights (TRIPs) which sets minimum standards for national IP protection frameworks and negotiate WTO agreements between nations.

International mechanisms

Trade Related Aspects of Intellectual Property (TRIPs)

TRIPs is the most comprehensive international agreement on IP rights to date. This agreement provides an international framework of principles, rules and disciplines dealing with international trade in counterfeit and pirated goods.

A vital part of TRIPs has been the establishment of binding and transparent rules that form the basis for a dispute resolution system. The availability of such a mechanism helps give confidence to countries and companies that export and continue to expand internationally.

Although TRIPs was a significant milestone in setting higher standards of protection for IP rights and dispute resolution on a global scale, the TRIPs standards of protection remain considerably less stringent than those prevailing in most developed countries, such as Ireland.

Added to the complexity of obtaining global IP agreements are the conflicting interests of developed and developing countries. These conflicting interests and differences in standards have resulted in difficulties in the negotiation and the establishment of more comprehensive international agreements. It is therefore likely that significant worldwide change on IP is unlikely and many countries, including EU countries, have sought alternative agreement outside the WTO.

Intellectual property crime

Anti-Counterfeiting Trade Agreement (ACTA)

One such international agreement is the ACTA. The ACTA aims to establish international standards of enforcement of IP rights. As at March 2014, the ACTA has been signed by 32 countries and the EU. Despite its signature, the agreement was not ratified by the European Parliament in July 2012 as "The intended benefits of this international agreement are far outweighed by the potential threats to civil liberties". As it has yet to be ratified in the EU, it cannot be considered in the context of this report.

EU free trade agreements

The EU has been proactively pursuing its own trade agreements. Given the link between IP protection and international trade it is unsurprising that these agreements generally include IP provisions with the aim of harmonising regulatory

frameworks and protection of each parties IP rights. Most recently, the EU has been negotiating with the USA on the Transatlantic Trade and Investment Partnership (TTIP). Although both the EU and the USA have efficient rules on IP protection, the agreement specific IP issues and different approaches to make trade easier without weakening the IPR framework of the respective regions.

“Ireland and Northern Ireland in particular, as export driven economies with strong traditional ties to the US economy, stand to gain from a TTIP. We stand to gain in three broad trade and investment areas: increased market access, a reduction in regulatory barriers and non-tariff barriers to trade, and by effectively setting the new global regulatory standards, for instance on IP rights (IPR), environment, labour and other globally relevant challenges and opportunities.”

An Taoiseach, Enda Kenny T.D.

Table 1.3 – International IP protection frameworks

Right	International	European	United States	National
Patents	TRIPs sets a minimum 20 year potential lifetime for patents applicable to all WTO members. There is no 'global' patent. Patent Co-operation Treaty (at WIPO) provides a single international search and preliminary examination. Patent must still be granted for individual states or regions by respective offices.	European Patent Convention aligns protection of patents across EU countries, although some differences remain. In addition national systems for processing also differ.	Differences in grant by offices and enforcement in courts between Europe and US, e.g. on biotech, software and business models. US system is currently "first to invent". However US are likely to change to the "first to file" system as the rest of the world currently have in place.	National law in Ireland is aligned with European Patent Convention, though some differences remain. National systems for processing also differ.
Copyright	The Berne Convention is an international copyright treaty providing minimum legal protection for authors of copyright works. It has 166 contracting parties (July 2013).	The EU is a contracting party of the Berne Convention.	US permits use of copyright material without consent by the rights holder, provided it is considered "fair use". In the EU there is a list of specific exceptions.	Ireland is a member of the Berne Convention via the EU. There are differences in what is protected by copyright between countries.
Trademarks	The Madrid Protocol is a system for the international registration of trademarks. The Madrid protocol has 91 contracting parties, 56 of which are also contract parties to the Madrid agreement. Trademark Law Treaty harmonises national application procedures of trademarks. It has a total of 53 contracting parties (July 2013).	At EU level, trademarks are granted by OHIM (the EU trade mark and designs office). This grants a mark valid in all 27 Member States. The Madrid Protocol is an international registration system for trade marks (administered by WIPO).	The US has a requirement for use before registration. Specifications are therefore more explicit and often longer than UK counterparts. 'Passing off' is known as 'palming off' in the US. There are differences in the legal definitions.	Trademarks can be granted in each country through the national IP office. No restriction on the length of a trade mark right, provided a mark is used. In Ireland, similar to the UK, trademarks can also be protected through common law aka 'passing off'.
Design rights	The Hague Agreement provides a mechanism for registering a design in several countries by means of a single application (administered at WIPO).	EU-level Registered Community Designs (RCD) are granted by OHIM, which protects for 25 years. There are also Community Unregistered Design Rights lasting 3 years.	In the US, a design patent is a patent granted on the ornamental design of a functional item. Design patents are a type of industrial design right.	Ireland is a member of the Hague agreement via the EU. The Patent Office registers design rights.

Source: The UK's International Strategy for IP, IP Office

Intellectual property crime

Enforcement

Enforcement remains a real challenge to IP protection and is a significant barrier to international trade. Although IP enforcement is improving as a result of the international mechanism outlined in Table 1.3, there remains fragmentation in many IP frameworks which is a barrier to continued internationalisation.

The lack of harmonisation notably with developing countries represents a test for IP protection internationally. According to the European Commission almost 90,000 IP infringing cases were registered by Customs in 2012. The high number of detentions is related to the high number of small parcels, which are likely to be a result of internet sales. As far as the almost 40 million detained articles are concerned, the value of the equivalent genuine products is estimated to be just below €1 billion. This shows a continuation of the trend of the high number of shipments suspected of violating IP rights⁹.

These statistics demonstrate how the infringement of IP continues to be a significant issue despite global efforts. Although customs officials are effectively doing their jobs, many developing countries continue to deliberately disregard IP protection regulations and supply contraband to the EU markets. Without real reform in these regions, IP infringements are likely to continue to grow. Despite the fact that a large portion of shipments that violate IP originate from these developing countries, it is important to ensure that these countries are not excluded from the global market and are given an opportunity to access and join the IP protection mechanisms.

Ireland

In the context of the national innovation agenda, the EU and international obligations, the Irish government has been proactive in its efforts to ensure that the IP laws are kept relevant and up-to-date.

“Ireland’s reputation as a country with strong IP rights plays a critical role in that process and its ability to attract a continuing flow of US investment.”

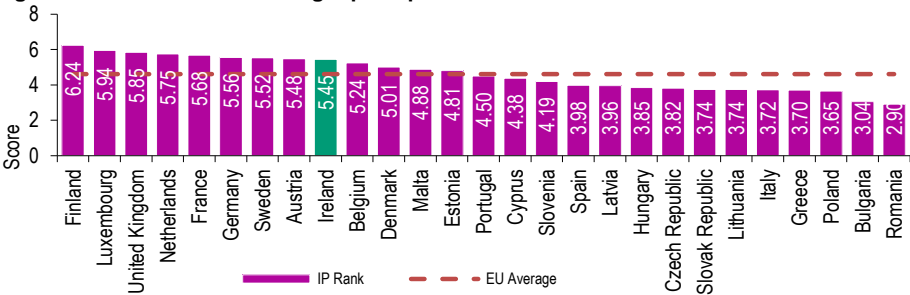
Grant D. Aldonas, former US Undersecretary of Commerce

Substantial efforts have been made over the last couple decades to introduce measures to protect IP in Ireland to ensure that there is an appropriate legislative framework in place that protects IP right holders. Although there are a number of laws and regulations governing IP, the primary legislation includes the following:

- Trade Marks Acts 1996;
- Madrid Protocol 2001;
- Patents Act 1992; and
- Copyright and Related Rights Act, 2000.

Although much of the IP legal framework is governed at EU level, each member state has a degree of freedom as to how directives are transposed into law. In this regard, Irish legislation is seen to be strong. This fact is demonstrated by the findings of the World Economic Forum which ranks Ireland as ninth in Europe based on the ratings of IP owners.

Figure 1.2 – IP framework strength perception¹⁰



Intellectual property crime

Copyright Review Committee

One of the most recent developments in the area of IP since our 2013 report is that the Copyright Review Committee has returned with its findings from its independent assessment of the current Irish copyright legislation. The key recommendations of the report relate to the establishment of a Copyright Council of Ireland and specialist IP tracks in the district and circuit courts, and to the introduction of tightly-drawn exceptions for innovation and fair use.

The introduction of the Copyright Council is a major step forward for the Irish IP Framework, as it introduces a digital copyright exchange and will support the efforts to educate and advise companies on copyright issues both at national and international level.

Plain packaging

One of the most significant topics in IP law in recent years has surrounded the issue of standardised (or plain) packaging, specifically in the area of tobacco. The objective of standardised packaging is to remove the “fashion element” from the culture of smoking with the ultimate aim of reducing demand.

Initially introduced in Australia, the Irish government gave its approval in May 2013 to begin the process of introducing standardised packaging into Ireland. Ireland will therefore be only the second country to introduce such a measure. In the context of research in the area of IP and illicit trade it is important that this issue is considered. We have therefore explored some of the potential consequences for the Irish economy and the international perception of such a move.

In an area that is already rife with illegal activity, the introduction of standardised packaging introduces a number of legislative and economic risks that could exacerbate an already significant issue. The sale of illegal cigarettes is costing the Irish economy as much as €575 million¹¹ per year. Our analysis suggests that introduction of plain packaging could escalate some major risks, including:

1. Increase illicit trade
 - a easier for illicit producers to reproduce;
 - b decrease production costs;
 - c decreased differentiation between illicit and legitimate products; and
 - d undermine the current efforts of the digital code.
2. Damage international reputation of Irish legislative framework
 - a high proportion of IP intensive industries in Ireland; and
 - b reputational damage from foreign investors surrounding the commitment to the protection of IP.
3. Precedent
 - a there may be concern from other industries that such measures may be introduced into other areas such as food or drink. For example, a World Health organisation report published in February 2014, while not explicitly calling for the introduction of plain packaging, suggested that similar legislative approaches to those deployed against tobacco need to be evaluated in other areas, notably consumption of alcohol and sugar-sweetened beverages.¹²

“These measures, if adopted, would send an immediate signal to foreign countries and investors about the standard of IP protection in Ireland”.-
Presentation by IBEC to the Oireachtas Committee on Health and Children¹³

Beyond these issues it remains to be seen whether or not the introduction of such a measure is in fact legal or will have any impact on reducing the prevalence of smoking in Ireland.

Ultimately, Government efforts to reduce consumption of tobacco should be commended. However, the introduction of standardised packaging introduces significant risks and a precedent that could have the unintended consequence for both the Exchequer receipts and international investment in Ireland. The lack of data to support either argument suggests that the Government should conduct a

Intellectual property crime

detailed independent research on the issue and await more detailed evidence on the merits of standardised packaging.

Conclusions

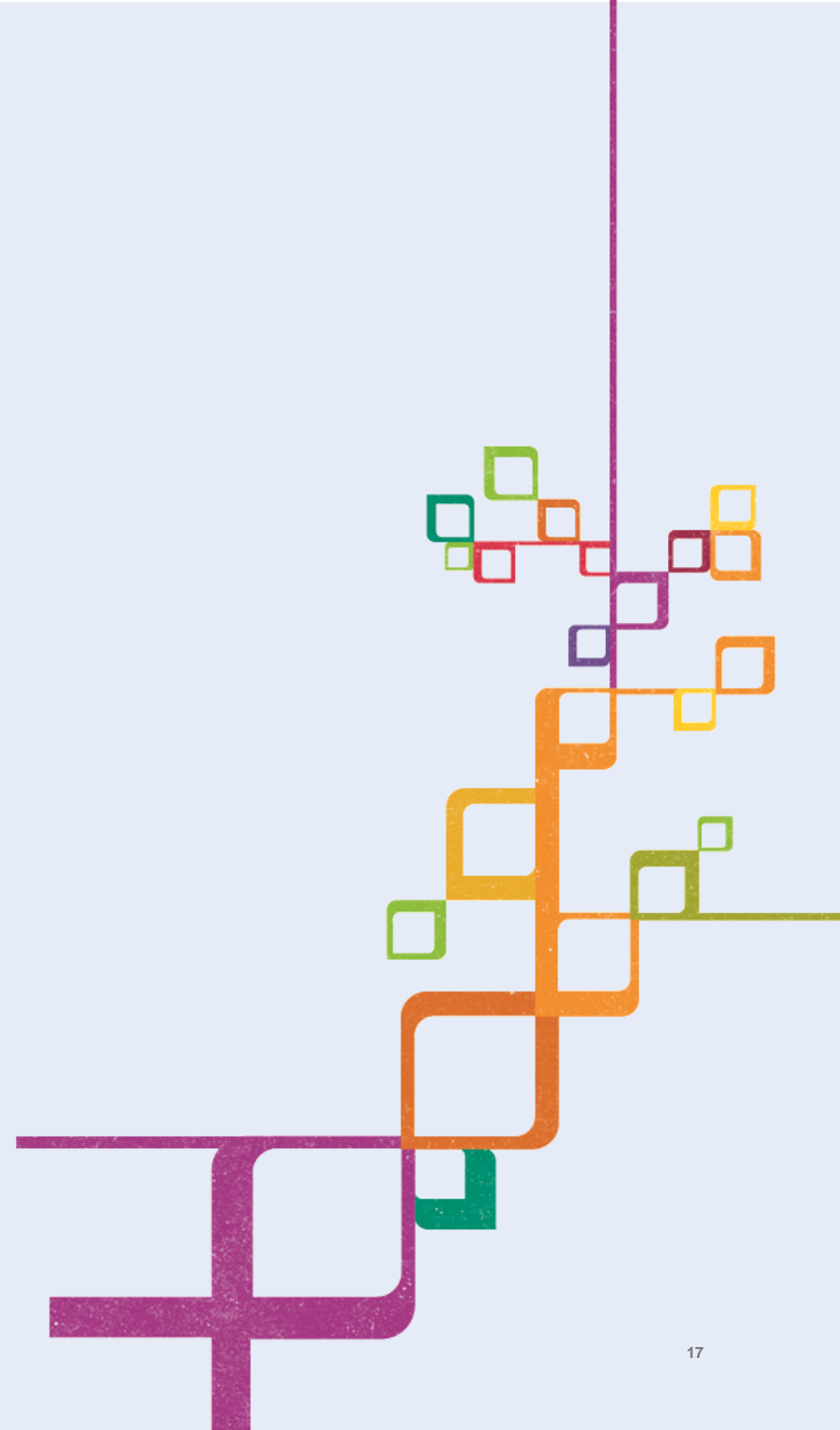
With its importance to growth and innovation, IP protection has always been an important pillar to economic policy in developed countries. Recent data has shown that Ireland currently has the largest contribution to GDP of IP intensive industries in Europe. The emergence of new technology and new industries as a result of both domestic innovation and foreign investment has only served to increase the importance of having a strong IP framework.

The protection of IP cannot occur simply at a national level alone, therefore international structures and mechanism are an important element to IP protection. Whilst the structures that are currently in place have introduced vital minimum standard of protection, the existing framework is not sufficient or flexible enough to address the emerging trends of technology, access and consumption.

Progress on IP protection can be problematic due to the conflicting interests and differing perspectives of the various stakeholders. The cross border nature of business and protection of IP, has led to difficulties in international enforcement. Beyond this it is fair to say that the benefits to IP protection are not shared equally. Although developing countries will benefit from the strong IP protection, for these countries there can also be strong incentives to keep IP legislation weak to allow for greater information transfers.

Aligned international strategies are required both for the EU and Ireland to improve national and international co-operation. At a national level, awareness of IP crime needs to be raised to ensure that there is an increased understanding of how it can affect businesses and the wider economy. This in turn will assist in moving IP crime up the national agendas to ensure that increased operational activity is pursued. For a broader international level, more needs to be done to continue to harmonise IP laws with our trading partners. Proposed agreements like TTIP are a positive step. The greatest challenge however remains weak IP regimes of the less developed countries. Globally, efforts need to be made to assist these developing countries in developing their economies and building stronger national IP regimes.

2 Cybercrime



“The lesson from both of these attacks is clear: individuals, businesses and Government must be constantly vigilant and ensure that our systems evolve to meet the ever-growing threat.”
Tánaiste and Minister for Foreign Affairs & Trade, Mr. Eamon Gilmore T.D.¹⁴

Data is increasingly playing an important part in the global economic landscape. As we seek to provide more efficient services or gain more meaningful insights into consumer behaviour, we are collecting and storing more and more information. This information has become a valuable commodity to many and as such the collection and use of this data is a growing area for the international community in terms of legislation and enforcement.

As this new economy continues to grow, so too does the associated shadow economy. Throughout this report we have identified the increasingly global nature of illicit trade, but it is especially relevant in the area of cybercrime. Recent high profile examples of personal data theft in Ireland and internationally has pushed the issue of data theft and cybercrime to the forefront of global debate.

Many governments have in fact identified cyber security as one of the top threats to their country alongside natural disasters, international terrorism and military invasion.

The development of ICT has broken down borders and technology continues to develop rapidly. However, the legislative and enforcement frameworks continue to lag behind making it difficult to prevent and track data breaches.

The rise of cybercrime is not disputed. However the wide varieties of estimates, which range from a few billion euros to hundreds of billions, reflect the inherent difficulties in measuring the true economic impact.

For Ireland with its focus on foreign direct investment, in particular in the areas of financial services and information technology, this will be a key battle ground

against the growth of illicit trade to ensure that firms feel confident in the regulatory environment and government response that protects its strong reputation.

In order to plan the appropriate level of resources for both governments and firms to fight cybercrime, we need to create a broader understanding of the importance of data and examine the key characteristics and drivers of the global and Irish markets for illegal data.

Types and characteristics of cybercrime

Definition of cybercrime

In assessing the current state of cybercrime, we need to consider what exactly constitutes a cybercrime. The standard definition calls it “criminal activities carried out by means of computers or the internet”. However, it is difficult to distinguish between computer-based and computer-aided crimes. In this technologically driven age virtually any crime may have been aided or facilitated by technology, whether using a website to hire a hitman¹⁵ or using the internet to research a crime¹⁶. We will not attempt to give a complete description of all cybercrimes, instead we focus on pervasive, large scale and automated types of data breaches where data (personal or otherwise) has been the subject to unauthorised access, collection, use or disclosure for monetary gain.

The cybercrime of interest can be categorised into a number of areas of focus:

- **identity theft** – cyber criminals obtain personal data from individuals (i.e. address, date of birth or bank account details) and exploit this online by opening fraudulent accounts (for example, bank accounts and mortgage applications). In many cases, the victims are not even aware of a problem until the impact becomes severe.
- **online/internet scams** – cyber criminals obtain financial or other valuable information by fraudulent means, usually by tricking individuals through interrelated online scams which include:

- **online purchase fraud:** such as making people pay for goods they do not intend to despatch;
- **pharming:** redirecting website traffic from a legitimate website to a fraudulent website. This can also be used to infect an individual's computer with malware and compromise online accounts e.g. online banking.
- **phishing:** this is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy party in an electronic communication. For example, sending fake money-transfer requests from foreign countries to thousands of e-mail accounts;
- **spear phishing:** highly-personalised fake e-mails targeted at a single individual. This is often used to target high net worth individuals or as the first step in a wider attack to compromise data in an organisation;
- **vishing (voice phishing):** is similar to phishing type of scam using voice messages that purport to be from a trustworthy party to defraud customers.
- **cyber theft from business:** cybercriminals steal data or revenue directly from businesses. This usually involves unauthorised access and targeting of company online systems, websites, databases, accounts and monetary reserves. Recently, the reputational impact of a successful cyber theft has become critically important for Irish businesses¹⁷.
- **cyber extortion:** this involves an attack or threat of attack against a business, coupled with a demand for money to avert or stop the attack. This includes holding a company to ransom often through deliberate denial of service. For example, by using malware to overwhelm a company's website with internet traffic or by manipulating website links, which could lead to substantial brand damage (for example, by redirecting links for a retailer website to a pornography website). In recent years, cyber criminals have targeted many Irish organisations using so call "ransomware" that is used to encrypt the victim organisation's data. The cybercriminal then demands money for the decryption key¹⁸.
- **industrial espionage:** this takes many forms, such as a competitors gaining authorised access to confidential data to gain competitive advantage or individuals gaining insider knowledge for financial gain. This could include finding out a competitor's bid price or becoming aware at an early stage of a possible merger or acquisition.
- **online intellectual property theft:** cybercriminals, often sponsored by competitor organisations or, increasingly, countries' governments, steal designs, technical specifications, trade secrets, process information or detailed methodologies, which can quickly erode competitive advantages. The impact of this cybercrime can be particularly strong in a small export driven economy like Ireland.

These are the cybercrimes that are dramatically increasing in occurrence and are having the greatest economic impact both in Ireland and internationally. It is important to note that the financial impact of such cybercrime comes in two forms:

- **transfer of funds:** for example, through the transfer of money from online bank accounts or the use of compromised credit cards.
- **the intrinsic value of the data stolen:** for example personal financial data or credit card details can be traded on underground sites on the internet¹⁹. In fact, a valid stolen credit card can be worth as much as \$100 online depending on the amount of information available with the card²⁰.

Key drivers to cybercrime

By applying the traditional economic forces of supply and demand to the economic landscape of data we can begin to understand the true drivers behind the growing incidences of cybercrime.

Supply

On the supply side, it is the institutions (and some cases the customers of the institutions) in both the public and private sectors that are the producers of the commodity (i.e. data), whereas the cybercriminals act as agents who procure and sell these products at the going market price. It is these agents supply of this illicit product which creates the actual market itself. Below we have given a profile of breach agents collated by Verizon.

International profile of cyber-attack agents

- 92% perpetrated by outsiders
- 14% committed by insiders
- 1% implicated business partners
- 7% involved multiple parties
- 19% attributed to state affiliated actors

Source: 2013 Data Breach Investigations Report, Verizon, 2013

Clearly the vast majority of breaches of cyber security are committed by agents external to the organisation targeted. Historically it has been felt that attacks committed by insiders had a greater financial impact on institutions. However, recently the sheer intensity of attacks coupled with the volume of data stolen would indicate, anecdotally at least, that the impact of attacks external to institutions is now much greater. This volume of data is no surprise: over the past decade organisations (and consumers) have dramatically increased the volume and quality of data that they produce. Whether it is a bank's information on its customers or an individual's data stored on a social networking site, the volume of valuable data that is potentially accessible through online channels has rocketed. Clearly the potential market is large and growing, as increasing amount of information is available online.

This has placed an increasing strain on the ability of organisations to protect both their and their customer's data from authorised access attempts. In fact, dramatically increasing spend on online security controls has not always protected organisations from falling victim to a data breach. Organisations who do not invest in online security will eventually fall victim to a breach, which will result in the company investing in security to protect their business anyway in addition to the direct costs of a data breach. It is therefore important that an appropriate balance is found.

There are a number of other factors that dramatically ease the acquisition and supply of illicit data that assist perpetrators of cybercrime. Primary amongst these is the fact that the risk of discovery remains low due to the ability to conceal their identity. This coupled with the lack of harmonised legislation across borders results in jurisdictional issues for law enforcement. In addition, the increasing sophistication of attackers coupled with a commoditisation of exploitation techniques has lowered the barrier to entry for cybercriminals. Fundamentally, for potential cybercriminals it is increasingly easy (and cheap) to instigate an attack, with the chances of being detected remaining low and even if they are detected the penalties are likely to be limited.

Demand

The continued increase in the size and scale of data breaches demonstrates the growing demand for this illicit information. The research indicates that for malicious cybercrime, unsurprisingly, it is financial motives that are the main driver in the commercial sphere. However, for cybercrime in the public sector there are additional motivations such as access to intellectual property, military intelligence and insider information etc., which fuels the demand.

From our research we have seen the demand being consumed by five key categories of consumers, each with different motivations and incentives. The Table below gives a profile of each of these consumers.

Table 2.1 - Cybercrime consumers²¹

Consumer	% of total	Description
Organised crime	55%	With more than half external breaches internationally being carried out by organised criminal gangs, this reflects the high prevalence of activities such as scamming, payment fraud, identity theft etc.
State affiliated	21%	State affiliated breaches are not necessarily motivated by financial incentives. They seek other types of information such as military, insider information, intellectual property or source codes.
Unknown	13%	Unidentified / untraceable breaches.
Unaffiliated	8%	Individuals not linked to other categories. Majority would be individual hackers or current employees.
Activist	2%	Activists form another important part of the threat actors within the cybercrime landscape. Such activists are more concerned with ideological motivations and as such are leaking this information to the public.
Former employee	1%	Former employee of organisation.

The international nature of the demand means that the potential impact on a small open economy like Ireland is not limited by the size of the Irish market demand.

Trends in cybercrime

The area of cybercrime trends has and continues to change at an incredibly rapid pace. The increasing use and dependence on technology continues to be one of the major influences on both the domestic and international economic landscape. With each new year, new cybercrime trends emerge, further complicating an already challenging environment for businesses and legislators. This speed of change requires agility in their response that both business and government struggle to deliver.

Below we have outlined some of the key cybercrime trends affecting the global economy:

- **“big data” technologies are increasing the effectiveness of attacks.** The “big data” trend is driving organisations to gather increasing volumes of data from their operations and customers. The importance of speed to market means that

many organisations with “big data” initiatives are not making the investments to ensure that this new data is secured appropriately. Increasing an organisation’s ability to gain insight from its data very often leads to an increased risk of unauthorised access.

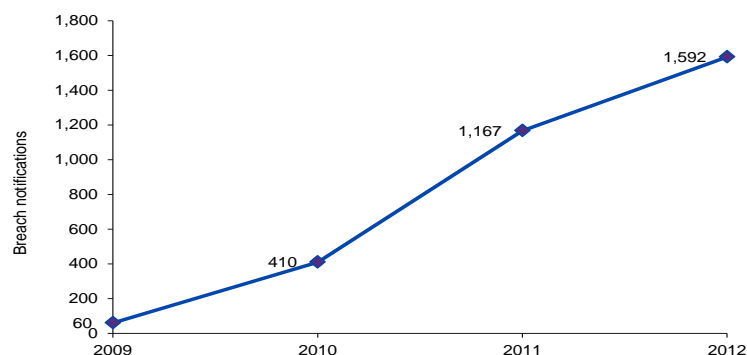
- **organised criminals continue to be the main players.** Over the past decade organised crime has been the main driver of cybercrime. This initially manifested itself in large automated attacks on the customers of financial institutions and online merchants. Recently, however, criminals have shifted their targets away from individuals to companies. They are focusing not only on stealing data from the institution’s customers but stealing customer information directly from the institutions themselves. Because of this the frequency, size and cost of cyber-attacks are on the increase.
- **financial motives continue to be at the heart of the increase in cybercrime.** Cybercrime has been and continues to be a commercial endeavour driven by supply and demand. This is consistent with the fact that the most costly attacks for organisations tend to be those that are malicious or are criminal attacks. In addition, there is evidence to suggest that the US and UK companies who have a strong security position (posture, incident response and senior executive attention) have the greatest reduction in data breach costs.
- **non-reporting of cybercrime by business and individuals** continues to be an issue globally. Organisations are often concerned by the reputational impact of cybercrime. They do not want their customers to know that the security of their data has been compromised. This has resulted in a lack of information to accurately assess the financial costs of cybercrime and lead the increasing use of data breach disclosure legislation in many jurisdictions.
- **mobile cybercrime.** The dramatic increase in the proliferation of mobile devices like tablets and smart phones has opened new avenues of attack. The opportunities for cybercrime attacks on consumers using these devices are only beginning to be realised and it is likely that this is an area for future growth.

Irish trends

The increasing importance and commoditisation of information has resulted in the creation of an international market for such information. In terms of market trends, it is fair to say there is no sign that cybercrime is going away. There has been in fact a marked increase in the number of data breaches in terms of the frequency, size and cost both domestically and internationally.

From an Irish perspective we have seen a continued rise in the number of security breaches. During 2012, the Office of Data Protection Commissioner, dealt with 1,592 personal data security breach notifications²², which is the fourth straight increase since the introduction of the Code of Practice in 2010. This is illustrated by Figure 2.1 below.

Figure 2.1 – Breach notifications (2009 – 2012)²³



According to the annual report of the Data Protection Commissioner, although the “complexity of certain data security breaches increases it is the more mundane situation of correspondence being issued to an incorrect address that continues to account for the largest percentage of data security breaches”.

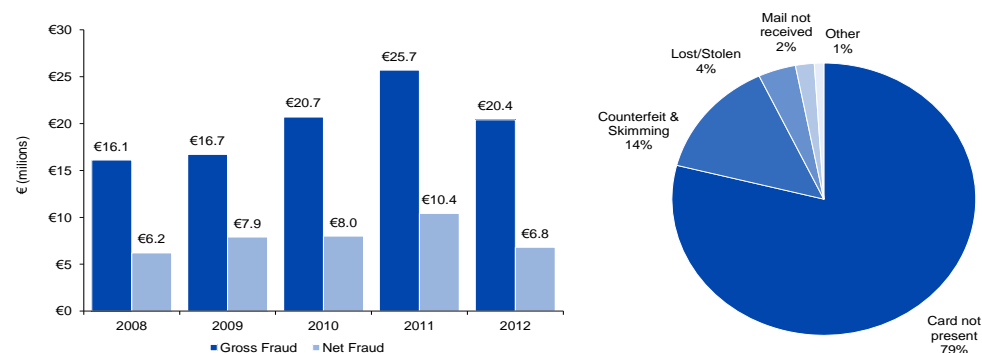
It is important to note that although the majority of breaches reported are described as mundane related to operation failures. However, a general tendency of Irish organisations to not report data breaches if at all possible coupled with a

lack of sophistication and maturity in Irish organisation’s security capabilities would lead one to conclude that the level of data breaches in Ireland is substantially under reported.

Online payment card fraud

Online payment card fraud continues to be one of the most common and best understood types of cybercrime in Ireland. Data from the Irish Payment Service Organisation (IPSO) indicates that card fraud is estimated at €20.4 million, with 79% of this taking place with card not being present at the time of payment (i.e. online)²⁴.

Figure 2.2 - Online payment card fraud in Ireland²⁵



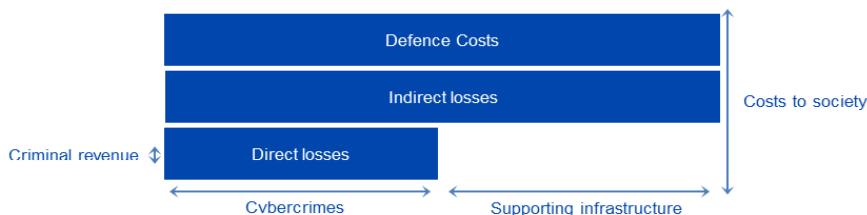
Costs of cybercrime

There are real costs to the economy of cybercrime. However, they can be difficult to quantify. The newness of the issue of cybercrime has resulted in widely varied estimates of the costs of international cybercrime ranging from €27 billion to €400 billion. Internationally, the average cost of a data breach to a company is €2 million per breach. For our nearest neighbour, the UK, the cost of data security breaches ranged from €200,000 to €6 million last year. In Ireland we have seen similar wide ranges.

Given such wide ranges in security breaches, we explore what makes up the costs of cybercrime both from a financial and non-financial perspective.

In considering these costs we have used a framework developed by an international team of scientists led by the University of Cambridge. This framework together with data gathered by the Poneman Institute has allowed us to identify the costs, associated losses and estimate what we believe to be a reasonable range of the cost of the issue for the Irish economy. We first identify the costs for individual businesses operating in Ireland²⁶ and then broader costs for the Irish economy as a whole.

Figure 2.3 - Costs of cybercrime²⁷



Direct losses

The first element to this framework is direct losses. These losses relate to equivalent losses, damage or other suffering by the victim as a consequence of cybercrime. Primarily amongst these losses are notification costs and intellectual property costs, but they also include financial losses associated with money withdrawn from victim accounts etc.

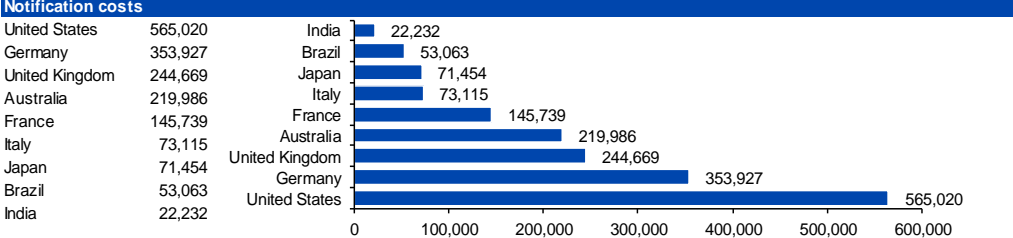
Notification costs

For businesses there is a growing body of regulations that must be complied with regarding the collection and use of information about individuals. Many of these laws focus on the types of personal information that are subject to data breaches and the requirements of the organisation to notify individuals affected by a breach. Ireland itself has adopted a voluntary breach notification code (“Guidance

and Personal Data Security Breach Code of Practice”). However, it is not legally binding.

There are real costs associated with responding to a breach, which typically include IT activities, determination of the regulatory requirements, engagement of outside experts, and finally postal and follow up communication costs. Much of this is further complicated by the different requirements in different jurisdictions. The average cost to an institution can be as high as \$565k in the USA and \$244k in the UK²⁸. If we take the average for the European countries reviewed, the cost to an Irish company would be in the region of €194k.

Figure 2.4 - Notification costs per organisation, '\$'



Intellectual property costs

It is likely that the greatest cost to a company is the loss of its intellectual property. Whilst this may not have a direct financial impact on its current profit and loss account, it can have a significant impact in the long term. The loss of intellectual property may not show up in a competing product for years. With companies investing heavily in research and development to build this intellectual property, a breach of its cyber security and the resulting loss of trade secrets could significantly impact on the company.

Loyaltybuild – Largest Irish data breach.

Loyaltybuild is an Ennis-based company that provides services to companies running holiday break promotions. It was hit by a major data security breach in late 2013. The breach involved the compromise of the personal details of about 1.5 million people across Europe. This included about 90,000 Irish customers of companies such as Axa, Clerys, ESB, Supervalu, and Pigsback.

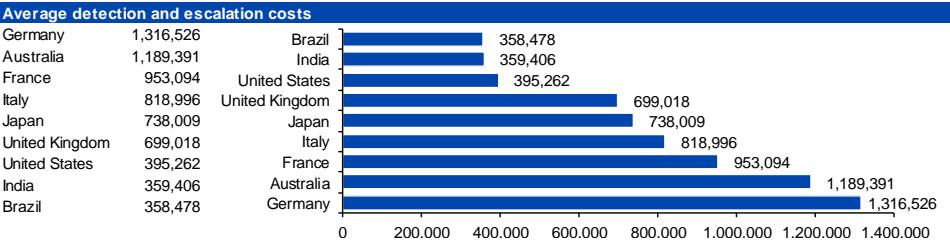
Initially, the company and clients including Supervalu and Axa had reassured customers that their personal data had not been compromised. But it was later acknowledged that this was not the case. Some of the personal information had been stored in unencrypted form and in some cases, credit card information was involved. Loyaltybuild ceased taking bookings on its websites and in its call centres in November when the Irish Data Protection Commissioner began investigating the breach and the business did not recommence until March. During this time the company also had independent expert undertake an investigation into the cyber-attack. In addition, they invested €500,000 in new security systems.

Defence costs

Defence costs are the monetary equivalent of prevention, detection and escalation costs which represent one of the most significant costs associated with cybercrime. As companies are increasingly concerned with ensuring the protection of its data they are spending more on data breach discovery and detection. Detection costs typically include forensic and investigative activities, assessment and audit services, crisis management and communications to executive management.

Germany has the highest defence costs per organisation at \$1.3 million, with the Europe average also being significant (\$946k) ²⁹.

Figure 2.5 - Average detection and escalation costs per organisation, ‘\$



Response cost and cost of securing network

The response to a data breach is critical to ensuring that this does not happen again, but more importantly reassuring stakeholders that such a breach cannot happen again. In this regard the reputation of a company is critical. The costs of such a breach can be as high as \$1.4 million³⁰.

Figure 2.6 - Average ex post response costs per organisation, ‘\$

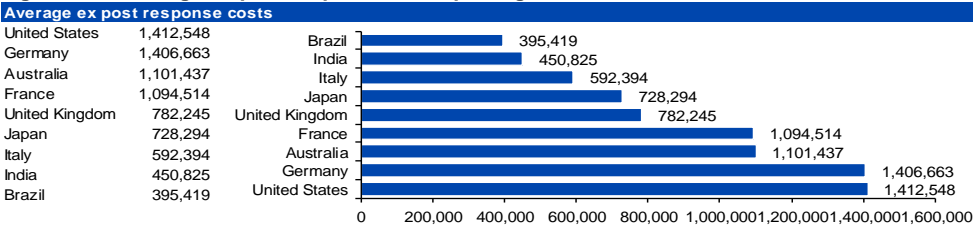
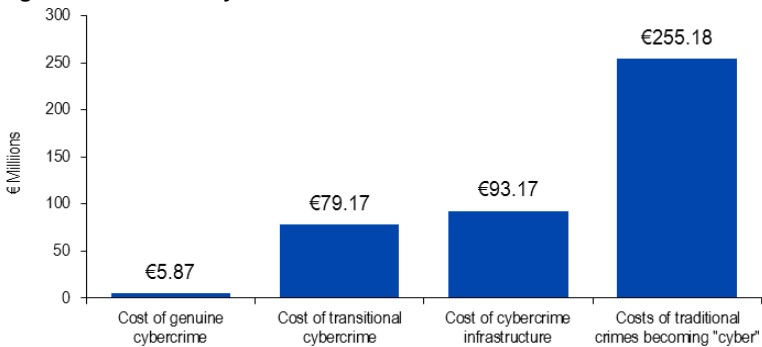


Figure 2.7 - Costs of cybercrime



Factors influencing the cost to businesses of a data breach

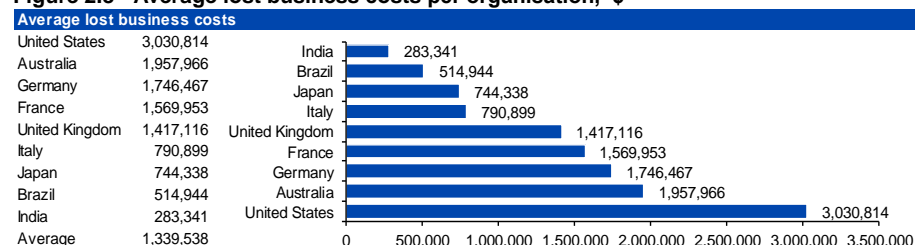
- 1 The company has an incident management plan.
- 2 The company had a strong security posture at the time of the incident.
- 3 Chief Information Security Officer appointed.
- 4 Data was lost due to a third party vendor.
- 5 Company notified breach victim quickly.
- 6 The data breach involved lost or stolen device.
- 7 Consultants were engaged to help remediate the data breach.

Indirect losses

For companies that suffer a data breach there are less direct and intangible lost business costs associated with such an incident. These include abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

A company's reputation can be difficult to quantify, however its importance cannot be underestimated. It is only when it is damaged one truly sees its value. The loss of confidence in the brand and associated goodwill can have devastating impact on the share price of a company. The Poneman Institute have estimated that average lost business costs could be as high as €3.03 million³¹.

Figure 2.8 - Average lost business costs per organisation, '\$'



Cost of cybercrime to Ireland

In addition to the costs to individual businesses there is the larger cost to the economy of Ireland itself. To estimate this figure we have built upon the framework of University of Cambridge in the paper "*Measuring the Cost of Cybercrime*" and applied it to the Irish economy. This framework estimates the global costs of the individual elements of cybercrime and scales these estimates to the country using its share of global GDP. Following this rationale, we have estimated the cost of cybercrime to the Irish economy to be circa €630 million. The analysis, shown in the Table 2.2, highlights that it is the cost of traditional crimes moving online that is the greatest threat to the Irish economy. This cost includes welfare fraud, tax fraud and tax filing fraud.

For the new types of computer crime, it is the defence and indirect costs that are in fact the most significant element and not the direct costs as one may assume. This could indicate that we should in fact be spending less on the anticipation of such and more in response to cybercrime.

Table 2.2– the Cost of cybercrime (Ireland, UK, US and Global)

Costs of genuine cybercrime	Irish Est.	UK Est.	US Est.	Global
Share of world GDP	0.23%	2.77%	18.82%	100%
Cost of genuine cybercrime	€'m	€'m	€'m	€'m
Online banking fraud				
- phishing	€2.55	€30.75	€208.90	€1,110 ³²
- malware (consumers)	€0.12	€1.44	€9.79	€52
- malware (businesses)	€0.51	€6.15	€41.78	€222
- bank tech countermeasures	€1.70	€20.50	€139.27	€740
Fake antivirus	€0.17	€1.99	€13.55	€72
Copyright-infringing software	€144.00 ³³	€1,299.57	€8,829.59	€46,916 ³⁴
Copyright-infringing Music	€20.00 ³⁵	€92.24	€626.71	€3,330 ³⁶
Patent infringing pharmaceuticals ³⁷	€31.82	€33	€296.92	€1,578
Stranded traveller scam	€0.02	€0.19	€1.32	€7
Fake escrow scam	€0.34	€4.10	€27.85	€148
Advance fraud	€1.70	€20.50	€139.27	€740
	€202.93	€1,510.32	€10,334.94	€54,915
Cost of transitional cybercrime				
Online payment card fraud	€6.80	€86.09	€584.93	€3,108
Offline payment card fraud				
- domestic	€3.57	€43.05	€292.46	€1,554
- international	€5.00	€60.28	€409.52	€2,176
- bank/merchant defence costs	€4.08	€49.20	€334.24	€1,776
Indirect costs of payment fraud				
- loss of confidence (consumers)	€17.02	€204.98	€1,392.68	€7,400
- loss of confidence (merchants)	€34.04	€409.96	€2,785.36	€14,800
PABX fraud	€8.44	€101.66	€690.69	€3,670
	€78.96	€955.21	€6,489.89	€34,484
Cost of cybercrime infrastructure				
Expenditure on antivirus	€5.79	€69.69	€473.51	€2,516
Cost to industry of patching	€1.70	€20.50	€139.27	€740
ISP clean-up expenditures	€0.07	€0.83	€5.65	€30
Cost to users of clean-up	€68.08	€819.92	€5,570.72	€29,600
Defence costs of firms generally	€17.02	€204.98	€1,392.68	€7,400
Expenditure on law enforcement	€0.68	€8.20	€55.71	€296
	€93.34	€1,124.12	€7,637.53	€40,582
Costs of traditional crimes becoming "cyber"				
Welfare fraud	€34.04	€409.96	€2,785.36	€14,800
Tax fraud	€212.75	€2,562.25	€17,408.50	€92,500
Tax filing fraud	€8.85	€106.59	€724.19	€3,848
	€255.64	€3,078.80	€20,918.05	€111,148
	€630.88	€6,668.45	€45,380.42	€241,129

Note: unless otherwise referenced, the source of information is Anderson et al, 2012 "Measuring the Cost of Cybercrime", WEIS 2012

Social costs

Although this paper focuses on the more financial elements of cybercrime, there are real social costs to an economy and to the welfare of its citizens. Although these costs are inherently difficult to quantify they are important and need to be acknowledged. From our research of the issue we have identified eight key social costs. These are:

- 1 slow the pace of innovation;
- 2 victimisation costs;
- 3 crime prevention;
- 4 changes in human behaviour;
- 5 cost of criminal justice for prosecution;
- 6 cost of over insurance;
- 7 job losses; and
- 8 access to illicit materials such as:
 - pornography; and
 - avocation of terrorism.

The importance of cyber security

A safe and secure online environment enhances trust, confidence and contributes to a stable and productive economy both domestically and internationally. This is particularly important for an open, technology focused country like Ireland. The emerging trend of cybercrime and the associated costs to business, consumers and government clearly demonstrate the need to have a clear strategy to deal with the many complex, multifaceted and evolving issues.

A strong cyber security strategy is becoming a prerequisite for both the private and public sectors. However despite this most organisations and governments are extremely inefficient at fighting cybercrime.

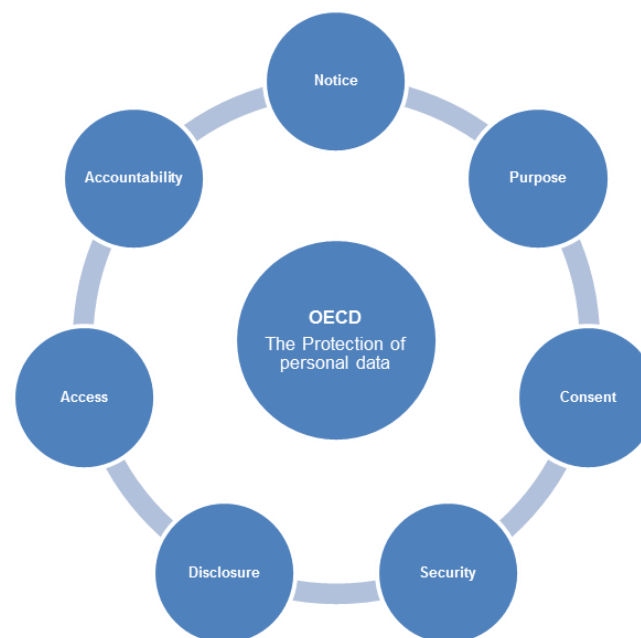
The private sector continues to build capabilities in data security and operate the day to day management of cybercrime, but the public sector needs to support

these efforts by ensuring that strong regulatory and enforcement frameworks are in place.

Principles for cyber security

Ultimately the same principles of security that exist in the physical world must be present in the digital and as such should protect the fundamental rights of expression, personal data and privacy. To assist with the development of national legislation on the issue of cybercrime, the OECD has developed seven principles governing the protection of personal data including a strong focus on security. These are illustrated by Figure 2.9.

Figure 2.9 - Principles of cyber security



To achieve appropriate level of protection of data it is vital that strategies are developed that build upon these principles whilst ensuring that they:

- leverage public-private partnerships and build upon existing initiatives and resource commitments;
- reflect the borderless, interconnected and global nature of today's cyber environment;
- adapt rapidly to emerging threats, technologies, and business models.
- are built on a risk based approach;
- focus on awareness; and
- focus on current cybercrime threats.

Key trends affecting cyber security in Ireland

Grant Thornton's experience shows that, security controls on IP in Irish organisations are generally poor, and remedies in law are rather restricted. Key issues include:

- 1 absence of document management means that organisations often do not know what IP is in their possession;
- 2 loose technical and process controls make it straightforward to steal information, and difficult to investigate such thefts;
- 3 lack of awareness of IP theft in the Irish business community leaves many organisations exposed to IP loss, and means that much IP theft is never detected;
- 4 cultural factors make it easier for employees to rationalise IP theft than financial fraud (e.g. "I'm only copying my own work, I'm not destroying it");
- 5 training on IT security and cybercrime prevention in Irish organisations is rare to non-existent;
- 6 weak laws and police underfunding have historically made it difficult to get IP theft prosecuted, although I think this is changing; and
- 7 civil remedies, while available, are typically expensive.

The legislative challenge

Legislating for cybercrime remains a challenge for law makers across the world. The current approach, which has evolved from the traditional or real world criminal and intellectual property law, is not sufficient to tackle the complexity and dynamic nature of the digital world.

It is the delay between the recognition of potential abuses of new technologies and the necessary amendments to national and international law that remains the most significant challenge in this regard. A further challenge is the multi-jurisdictional nature of cybercrime, which makes it difficult for organisations to comply with the many different and sometimes contradictory laws across its various locations. The burden of compliance can be high. In this section we outline the main laws and policies surrounding data protection in Europe, Ireland and the broader international community.

International co-operation

Cybercrime laws across the international community remain largely inconsistent or incompatible which has resulted in slow progress on international harmonisation, which is extremely important in the fight against cybercrime.

To assist the companies and governments operating in the changing digital landscape, efforts have been made to promote co-operation, both nationally and internationally between agencies. This is done through the various international initiatives to facilitate this co-operation, which includes:

- UN General Resolution on cyber security;
- G8; and
- OECD.

Fundamentally the investigation and prosecution of cybercrime presents a number of challenges for both sides of the law - regulators and enforcement agencies. Whilst there are a number of various forums and international best

practice guides, fundamentally the legislation in place is not adequate to meet the changing demands of the cyber security landscape. The legislation that does exist varies significantly. As a starting point, adjustments to national laws must begin with the recognition of the abuse of new technologies, which could be assisted by mandatory international data breach notifications.

Europe

European law is built upon the principles of the OECD recommendation from Figure 2.9. The EU issued a Data Protection Directive (95/46/EC) in 1995 which covers the processing and security of personal identifiable information. The notable absence within this directive was a general breach notification requirement.

The introduction of such a requirement has been the subject of much debate, which has resulted in the publication of its proposal for a regulation on the protection of individuals with regard to the processing of personal data and the movement of such data. It is intended that the regulation would replace the Data Protection Directive and that would remove the need for EU harmonisation of minimum standards.

The main cybercrime laws and regulations in the European Union

- European Communities (Electronic Communications Networks and Services)
- Data Protection Directive (95/46/EC)
- Proposed Directive (~2015)

Frameworks and forums to aid harmonisation

- 2005 Council Framework Decision on attacks against information systems
- Cybercrime Network Conference
- European Cybercrime Centre (Jan 2013)
- Budapest Convention
- 2005 EU Framework
- EU Cyber Security Strategy
- Cybercrime Network Conference
- European Cybercrime Centre (Jan 2013)
- Budapest Cyber Convention

Ireland

With no general breach notification in the EU, Ireland itself has adopted a voluntary breach notification Guidance and Personal Data Security Breach Code of Practice (“the Code”). However, the Code is not legally binding. In addition to the Code there are also the regulations, which apply to certain entities in the telecommunications sector.

Under the Code, the data controller of a business must immediately consider whether to notify the affected data subjects in situations where personal data has been put at a risk of unauthorised disclosure, loss destruction or alternation.

The main data protection laws and regulations in Ireland

- Personal Data Security Beach Code of Practice (the “Code”);
- European Communities (Electronic Communications Networks and Services);
- (Privacy and Electronic Communications) Regulations 2011 (the “Regulations”);
- Data Protection Acts 1988 and 2003; and
- Proposed Criminal Justice Bill;

In Ireland, whilst we have legislation and guidelines in line with other countries, legislative gaps still remain. In particular, the 2005 EU Framework Decision on attacks against information systems has not been transposed into Irish law. This would give effect to the Cybercrime Convention, as referred to already. Until implementation of the Cybercrime Convention and transposition of the Council Framework Decision on attacks on information systems into domestic Irish law, national law enforcement agencies across the Cybercrime Convention signatories, including Ireland, can only combat the more complex and generally international computer crime within the boundaries of limited domestic laws.

Conclusions

To say that cybercrime is an epidemic is not accurate. This would imply that organisations could avoid being compromised through good IT security hygiene or responsible investment. This is increasingly not true. For the vast majority

including those in Ireland the question is no longer if they will be a victim of cybercrime but when?

The scope of compromises is rapidly increasing, and the amount of data stolen on a daily basis is truly alarming. Some companies have lost all intellectual property related to the design of high-tech technologies and others have had millions of euros stolen from their accounts in a matter of days. The public will not always read the details of these cases because disclosure is not mandatory, but it is clearly a serious problem.

Key findings

- while it is difficult to quantify, we estimate cybercrime is costing the Irish economy circa €400 million per annum. This is in line with international estimates;
- the research indicates we may be spending too much on prevention of cybercrime and not enough on reacting to it when it happens;
- “big data” technologies are increasing the effectiveness of cybercrime attacks.
- organised criminals continue to be the drivers of cybercrime;
- financial motives continue to be at the heart of the increase in cybercrime; and
- non-reporting of cybercrime by business and individuals continues to be an issue both in Ireland and globally.

Key recommendations

Cybercrime is heavily impacting on the economy, both in Ireland and internationally. Its international nature makes it difficult to prevent particularly in a small open economy like Ireland. It is, however, critically important for Ireland to lead in the international fight against cybercrime. Ireland’s fast growing technology sector is a key driver in our economy. Our government needs to legislate appropriately, businesses need to detect and prevent cyber-attacks and our work force needs to be aware of and have the skills to fight cybercrime and secure online systems. Only with this combination can Ireland protect its

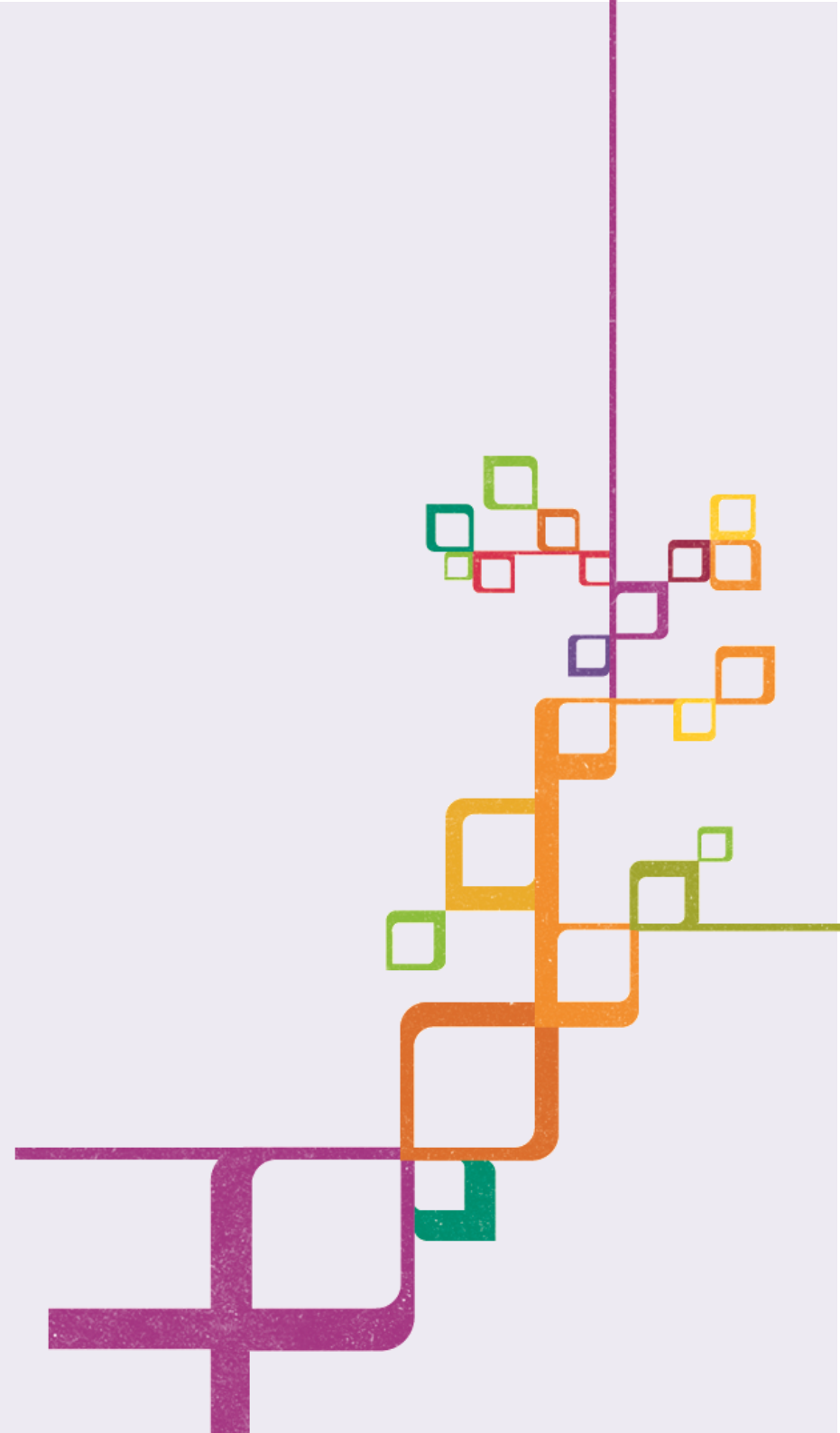
businesses and consumers in the online world and protect technology and intellectual property driven foreign investment. More specifically:

- Ireland needs help ensure international harmonisation of cybercrime laws. In particular, Ireland should implement the 2005 EU Framework Decision on attacks against information systems including mandatory data breach disclosure;
- Ireland should urgently develop and publish a national cyber security strategy. This is a plan designed to improve the security and resilience of Irish national infrastructures and services. It should establish a range of national cyber security objectives and priorities to be achieved in specific timeframes;
- Irish businesses should be focusing their planned cyber security investments on the ability to detect and react to data security breaches. In the current environment, it is not a question of if an Irish business will be subjected to an online attack but a question of when? The ability of the business to detect and react to the attack will be the key factor in limiting the impact of the cybercrime; and
- ensuring appropriate education of the impact of cybercrime on Ireland is key.

This includes ensuring:

- consumers understand the basics of protecting themselves online;
- business leaders understand the impact of cybercrime on their businesses. There have been a number of government initiatives in the UK that could be mirrored (e.g. the FTSE 350 Cyber Governance Health Check); and
- in addition, whilst there are a number of courses in our third level institutions that address cybercrime and security issues, these subjects need to be expanded in the undergraduate syllabus and ensure that all technology graduates are aware of cybercrime, its impact and security techniques to prevent it.

3 Money laundering



Money laundering

“Increasing globalisation of the financial and business sectors and the increased sophistication of money laundering methods pose a particular challenge to the criminal justice system. The internationalisation of a significant element of criminal activity adds to that challenge”
The Minister for Justice, Equality and Defence, Mr. Alan Shatter T.D.”³⁸

For criminal profits to be used, they need to appear as legitimate funds. This is achieved through the process called money laundering. Money laundering is an integral part of organised crime. It aims to disguise the true nature of criminal money and spreads across the world through distribution and marketing channels, legitimate businesses and individuals. Estimates suggest that over \$1.6 trillion is laundered every year worldwide.

The development of the international financial system, new financial instruments, the promotion of free movements of goods and services and the emergence of the new developing countries have increased exposure of the global economy to the risks of money laundering.

To protect the global financial system and the economies of individual countries it is vital to ensure that comprehensive anti-money laundering (“AML”) systems are developed at both national and international levels. Appropriate AML measures help countries to ensure that their financial systems, businesses and reputation are protected from the adverse impacts of money laundering. It is therefore important that AML is one of the central elements to promote legitimate free trade, maximise the benefits for each country whilst making it more difficult for organised criminals to carry out their illegal activities.

For Ireland, protection against money laundering is especially relevant given the nature of its open economy and a growing financial hub. The financial services sector continues to attract international companies by offering a wide range of products to customers from all over the world resulting in funds moving across borders in vast quantities. Some experts suggest that the value added by the financial sector to the Irish economy may be as high as 10% of the Irish GDP³⁹.

Money laundering is a major threat to both the reputation of Ireland and the brand of those multinational companies that operate their businesses in Ireland. Therefore, it is vital to make sure that Ireland is seen to be at the forefront of the battle against criminal activities and laundering of its proceeds to secure future growth and ensure that Ireland is a safe place to live and do business.

To minimise the negative impacts of organised crime groups’ activities it is necessary to not only reduce the opportunities for criminals to profit from illicit activities but also to ensure that proceeds from illicit trade cannot be used.

In this section we will discuss the issue of money laundering, its nature, drivers and both the financial and non-financial impacts on a country’s economy. We will review the impacts it has on the global and the Irish economy and demonstrate the importance of comprehensive AML legislation and its enforcement.

The process of money laundering

Money laundering is a complicated process that involves a large number of people who play their own part in it. In order to protect the global financial system from being penetrated by illegal money it is important to understand who and what is involved in money laundering.

To introduce criminal money into the legitimate financial systems without exposing its true nature there are a series of steps that are generally taken to distance the money from its criminal origin. These steps are:

1. placement;
2. layering; and
3. integration.

Placement is the first stage when illegal cash first enters the financial system through either lodging it to bank accounts or purchasing assets. The risk of

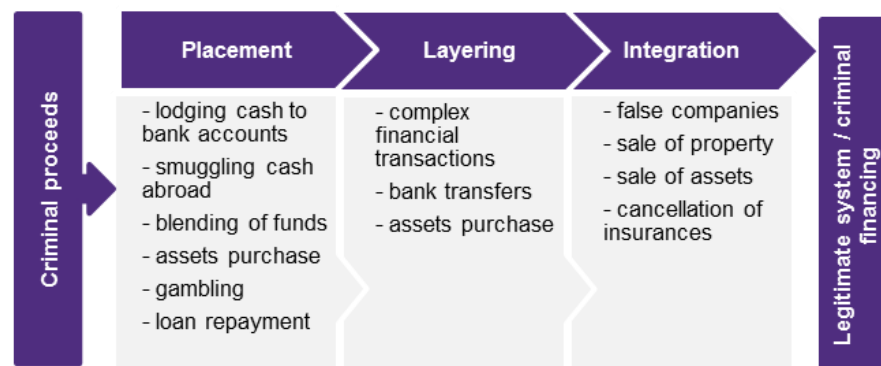
Money laundering

exposure for criminals is high at this stage as crime proceeds are still close to its source and can be traced back to its origin.

The second stage, **layering**, is concerned with disguising and concealing the true nature of the criminal funds. It often involves complex transactions, the use of multiple bank deposits, intermediaries and the transfer of funds from one institution to another across multiple jurisdictions.

Integration is the third and the final stage of the process. By this stage, the criminal funds have been completely detached from its original source and the audit trail is difficult to follow. Funds are then pulled back together into one account to allow criminals to use and control them as if they were earned legitimately.

Figure 3.1 - The money laundering process



For criminal funds to smoothly move through the three stages of money laundering a number of individuals are involved. This includes people who have access to and control over financial instruments.

Anyone who knowingly or unknowingly assists in money laundering or knows about it and doesn't take an action helps criminals to make sure that their criminal

activities pay dividends. A clear message should be sent by the enforcement and regulatory authorities about the importance of adhering to AML requirements in order to help avoid being used for money laundering.

Key developments in the money laundering environment

As our financial system and the legislation governing it are constantly evolving so too does the money laundering process. Over the past few years there have been a number of changes that have shaped the process of money laundering to its current form. The three key areas where changes have occurred include: on-going internationalisation, the growth of international trade, a significant advancement of technology related to big data and money transfer and the widening of the scope of regulations guiding AML. Table 1.3 provides some more detail on the recent developments.

Table 3.1 - Recent trends

Developments	Description
Internationalisation	The on-going process of internationalisation has significantly stimulated the growth of the global economy. At the same time, weak AML regulations in some countries can leave them exposed to international money laundering.
Technological development	The increase in the use of on-line channels to carry out various transactions provides money launderers with an opportunity to access these new channels to turn illicit money into legitimate funds.
Development of new payment mechanisms	Technological progress has enabled the development of new payment mechanisms, such as Bitcoin. Whilst these can provide significant benefits, they are also highly exposed to the risk of money laundering due to the lack of legislative governance and unawareness of its weaknesses that expose it to various risks.
Emergence of cyber laundering	The internet offers money launderers the possibility of cheap and tax-free money transfers which are especially relevant at the layering stage. In addition, use of yet unregulated virtual currencies and online casinos provide another useful tool for money launderers.
International financial system development	Free transfer of funds across various jurisdictions, easy access to international bank accounts and the development of new complicated financial instruments could make it more difficult to trace the source of funds.
Large scale of international trade and data transfer	The scale of international trade and the transfer of associated funds and data make it easier for money launderers to hide and disguise their operations.

Money laundering

Developments	Description
Variations in regulations	Legislation governing financial instruments, trade and other channels used by money launderers is not aligned across different countries. And whilst many countries have realised the importance of AML measures, money launderers continue to take advantage of the existing weaknesses in some countries to bring funds into the legitimate supply chain.
AML regulations	The issue of money laundering has been recognised by many countries and significant effort has been made by the international community in recent years. The scope of AML regulation continues to expand to widen the definition of designated persons and recognise new channels and instruments used by money launderers.
Bank secrecy	Bank secrecy rules in some countries are being revised to allow for more efficient investigation of fraud.
International trade agreements	There are on-going negotiations between the US and EU on the Transatlantic Trade and Investment Partnership. As the agreement aims at removing barriers to trade and investment between the two regions, it is vital that the money laundering risks are carefully identified and appropriate measures are taken to eliminate them.
Single Euro Payments Area (SEPA)	Recent roll out of SEPA both simplify fund transfers and payment within the EU and provide for easier traceability of the funds origins.

Most of the recent developments discussed aim to improve the efficiency of the existing trade and other mechanisms. However, at the same time they may provide an opportunity for money launderers to use them for the purpose of disguising illicit proceeds. The recently grown internet currency Bitcoin is an example of how exposed new instruments are to the risk of criminal involvement.

At an international level, significant effort has been made to ensure that the risk of money laundering is minimised. We can expect further harmonisation of regulations, continuing expansion of the scope of AML legislation and increasing flexibility of the new regulations to reflect technological and other developments.

Supply and demand of money laundering

To develop an effective approach to combating money laundering it is necessary to analyse the motivation of individuals engaged in this criminal activity and the factors that provide for successful operation of the money laundering process.

As with any other product or service money laundering falls under the rules of the economic forces of supply and demand. Therefore, we further assess the supply and demand sides of the money laundering process as well as the key factors enabling the money laundering process.

Demand

Ultimately, it is criminals and terrorists who create demand for money laundering because in its original cash form proceeds from criminal activities are worthless. There are a large number of organised crime groups and terrorist organisations spread across the world with estimated global turnover exceeding \$870 billion⁴⁰. In Ireland alone, there are over 25 organised criminal groups⁴¹ who operate predominately in the urban centres. It has been acknowledged by the justice system that many of these groups have significant international links. These organised crime groups (“OCG”) fuel the demand within Ireland for money laundering. In last year’s report we estimated that illicit trade in fuel and tobacco alone could be costing the Irish economy up to €1.1 billion with much of these going into criminal pockets. The proceeds of these criminal activities consequently entered the money laundering process and penetrated the legitimate financial system.

Supply

Money laundering is unusual due to the fact that often the supply and demand can originate from the same individuals, in this case OCGs. Internationally the supply of the money laundering service is organised and controlled by the organised criminals through legitimate distribution channels. Money launderers involve people who have access to these distribution channels to either knowingly or unknowingly assist in the money laundering process. Ultimately, the main incentive for criminals to launder money is the benefit of funds becoming available to further use in their illicit activities or to support their life-style whilst other people involved in the process are driven by the financial gain or fear.

Money laundering

Distribution channels

In order to disguise the origins of the proceeds of illicit activities money launderers can use one or multiple legitimate distribution channels. These channels include financial institutions, legitimate businesses and even international trade. Whilst each channel attracts money launderers for different reasons, the key factors criminals take into account are the ease of access, the risk of discovery and the access to the international network.

The Table below provides a short description of the various channels and reasons why they are used by the criminals.

Table 3.2 - Money laundering distribution channels

Channel	Characteristics	Reasons for use
Cash	<ul style="list-style-type: none"> includes cash and other paper documents that have monetary value bulk (i.e. cargos) or couriers (i.e. luggage) smuggling prefer larger denomination notes 	<ul style="list-style-type: none"> familiar instruments avoids financial system easily accessible ease of travel maintains value
Banking system	<ul style="list-style-type: none"> high volume money transfers daily extensive international networks quick and secure channel to transfer money can open multiple accounts 	<ul style="list-style-type: none"> can transfer rights to the account can use fake IDs to open multiple accounts access to money internationally through branches or ATMs speed and security of transfers
Alternative money transfer systems	<ul style="list-style-type: none"> money transfer businesses are subject to lower regulations only ID is required to receive funds widespread international retail payment systems 	<ul style="list-style-type: none"> avoidance of regulated banking system access to areas with underdeveloped banking systems retail payment system – non face-to-face transactions
Third party legitimate businesses	<ul style="list-style-type: none"> illegal cash is introduced into a legitimate business and is mixed with legitimate cash (if any) to be lodged into bank accounts mainly cash intensive businesses (i.e. casinos, retails, beauty salons, bars) 	<ul style="list-style-type: none"> lower risk of detection when legitimate business is involved economies of scale through lodging large amounts legitimate business cash can be used for terrorist financing
International trade	<ul style="list-style-type: none"> high volume of legitimate goods and services use of trade transaction to legitimise 	<ul style="list-style-type: none"> appears as legitimate trade higher volume and longer term channels

Channel	Characteristics	Reasons for use
	criminal funds (misrepresenting prices or quality & quantity of goods or creation of trade debt to settle with dirty money)	<ul style="list-style-type: none"> easy to hide due to large volume of legitimate trade
Assets (financial products, moveable goods, estates)	<ul style="list-style-type: none"> many appreciate in value over time can be transferred across borders 	<ul style="list-style-type: none"> safe storage and high liquidity (financial assets) large shareholdings allow to establish control over business many moveable goods and estates appreciate over time promote luxurious life-style

Infiltration of the legitimate economy by the illicit proceeds has various negative impacts on the global and local economies and societies. One of the key issues remains the fact that the regions with weak AML allow illegal cash to enter the legitimate supply chain.

Effects of money laundering

Money laundering has tight links with organised crime and terrorist financing which makes it one of the most significant problems of modern society.

Its indirect impacts can be seen in all areas of the modern world. Some of those relate to the actual monetary loss such as the loss of government revenue whilst other impacts such as ineffective resource allocation can damage the wider economy.

Economic impact

Ultimately, any money that is going through the money laundering process is revenue lost to the legitimate businesses and governments. As financial performance of organised crime groups is not subject to any recording and reporting regulations it is difficult to accurately assess its size. Thus, the amount of proceeds from criminal activities that are subsequently laundered can only be estimated.

Money laundering

Estimates of the size of money laundering:

- the United Nations Office for Drugs and Crime (UNODC) estimates that illegal activities account for 3.6% of global GDP, with 2.7% (or \$1.6 trillion) being laundered.
- this falls within the widely quoted estimate by the International Monetary Fund ("IMF"), who stated in 1998 that the aggregate size of money laundering in the world could be somewhere between 2% and 5% of the world's gross domestic product.⁴²
- the European Commission calculates the damage caused by corruption in the EU alone at some €120 billion a year, equivalent to 1.1% of EU GDP⁴³ and Member States lose over 2% of their GDP annually to tax crimes.
- another estimate suggests that in 2006 organised crime turnover in 20 OECD countries only, exceeded \$610 billion⁴⁴

Table 3.3 provides some estimates of the size of money laundering in Ireland based on the UNODC and IMF figures.

Table 3.3 - Size of money laundering in Ireland

		Ireland ('m)	Global ('m)
GDP 2012		\$210,771	\$72,440,449
UNODC (2.7%)	2.70%	€4,207	\$1,955,892
IMF - Low end (2%)	2.00%	€3,116	\$1,448,809
IMF - High end (5%)	5.00%	€7,791	\$3,622,022
Exchange rate \$/€	0.7393		
Midpoint		€5,454	\$2,535,416

Our estimates show that the size of money laundering in Ireland is likely to range from €3.1 billion to €7.8 billion. It is clear that money laundering has a significant financial impact on both the global and local economies. However, the financial cost of money laundering to the society is much larger. It also includes the following costs:

- loss of government revenue – criminals do not declare profits they make and do not pay any taxes on it. This diminishes Exchequer receipts and increases the tax burden on other people and businesses;
- cost of enforcement – as money laundering stimulates organised crime additional resources are spent on regulations and enforcement; and

- compliance costs for businesses – the use of legitimate businesses by money launderers creates the necessity for businesses to allocate resources to the AML function.

Money laundering's negative influence is not limited just to the monetary loss, it has much wider implications for the economy as a whole.

As criminal money enters the legitimate supply chain it inevitably leads to imbalances in the economy. A healthy market economy operates based on a principle that individuals act rationally and are looking for the most efficient way of investing their funds. When the economy is infiltrated by money launderers this principle no longer applies, as money launderers' investment decisions often do not have any economic rationale behind them. Below we identify the potential macroeconomic issues created by money laundering.

Table 3.4 - Effects of money laundering

Impact	Description
Damage to the integrity of financial markets	By placing criminal money into financial institutions criminals damage the integrity of a financial institution through exposing it to the reputational risk, risk of liquidity issues and risk of law suits and penalties. This results in loss of profits, loss of high quality clients, and termination of relationships with other financial institutions, assets seizures, criminal investigations and decline in the value of the company. As a result international and domestic consumer confidence in the country financial institutions can be damaged.
Damage to competitiveness of the legitimate private sector	The involvement of criminal funds in the private sector results in criminal businesses that have access to cheap illegal funds, having a competitive advantage over legitimate business through undercutting current market prices.
Control of private sectors by criminals	Criminals often choose to invest laundered funds into existing legitimate businesses. This allows criminals to control entire sectors of an economy. When criminals are no longer interested in those industries they abandon them causing the collapse of those sectors and ultimately damaging the overall economy.
Distortion of foreign trade balance	High level of luxurious items purchased using laundered money together with a high level of illicit product exports may cause abnormalities in the country's foreign trade balance.

Money laundering

Impact	Description
Impact on policy and decision making	The existence of undocumented illicit sector and financial flaws in the economy lead to statistical data not being able to accurately reflect the situation in the country. This would lead to poorly informed decision making by governments.
Privatization efforts	Laundered money used to purchase formerly state-owned companies can ultimately eliminate any benefits of privatisation.

The above impacts would ultimately lead to a slowdown of the economic growth in the country, can attract attention of the international community and consequently have an adverse impact on the investment rating of the country.

Other economic impacts

Whilst money laundering can substantially weaken the country's economy through penetration of its legitimate sectors it can also facilitate criminal activity, adversely impact businesses and damage the country's overall wellbeing.

Fines and penalties

Organisations that are found to be involved in money laundering are subject to "substantial fines and penalties". Beyond this, the legislation provides for the people entrusted with governance in those organisations to be held personally responsible for the failure to ensure that appropriate AML systems are in place.

Increased crime and corruption

Money laundering stimulates organised crime growth and increases criminal activity especially in the country where money laundering is carried out. Lax legislation in some regions of the world attracts money launderers making those countries havens for money launderers. This in turn attracts organised crime and hinders further development of the economies of these countries.

Damage to the reputation of the country and its companies

All the negative impacts mentioned above ultimately damage the reputation of a country that is associated with money laundering activities. This consequently has

a negative impact on the image of the country and its attractiveness to foreign investors. In the modern global economy reputational damage can result in a country being excluded from international trade and investment networks.

Although difficult to quantify, reputation also has a real value for companies. For organisations, any association with money laundering can have a direct impact on its reputation and subsequently its share price.

It is extremely important for Ireland as an economy for which foreign direct investment plays a critical role that its reputation remains intact. It is vital to ensure that Ireland is seen as a safe place to do business and its financial system and businesses are well protected from the negative impact of money laundering.

Importance of anti-money laundering

Over the past number of years the issue of money laundering has come to the attention of the global agenda and significant progress has been made on both international and national levels.

In the previous sections we have analysed the devastating impacts money laundering has on the economy and society of countries worldwide. The damage money laundering can cause to economies and businesses makes it clear that international communities must ensure that the issue is addressed and all efforts are made to limit the exposure of the global and local financial systems to the risk of money laundering.

International effort to combat money laundering

As money laundering is a recognised international issue there are a number of international organisations in place to oversee and facilitate the AML regulations, policies, procedures and enforcement across various countries. In this section we review the progress made to date by the international community and Ireland specifically and identify areas for future improvement.

Money laundering

International collaboration

International organisations aim to establish common AML structures, rules and regulations and provide independent advice to its member countries on AML matters. Various recommendations and guidelines have been issued by regulators across the world. However, there are some common areas of focus that are emphasised in all of them. Figure 3.2 illustrates some of them.

Figure 3.2 Key elements of AML system



Key elements of AML system

- **Risk assessment procedures** – assessment of risk prior to establishing relationship and throughout to manage risks;
- **Suspicious Transaction Reporting (STR)** – reporting of suspicions activities to ensure enforcement and prosecution of money launderers;
- **Customer due diligence** – appropriate customer identification and verification;
- **Training** – sufficient training to those involved and exposed to the risk;
- **Record keeping** – keeping records of CDD, reports and other documents to allow for review and improvement;
- **Governance** – control over the process to reduce risk; and
- **Policies and procedures** – clearly documented process of AML to ensure common understanding.

By focusing on the above areas both at the international and national levels countries facilitate the development of a unified strategy to combat money laundering.

The efforts made by the international organisations provide for on-going harmonization of local AML regulations to accommodate for the global market. The main international body that oversees the development of these regulations is The Financial Action Task Force on Money Laundering.

The Financial Action Task Force on Money Laundering

The Financial Action Task Force on Money Laundering (FATF) is the main international body whose objectives are “to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system”.⁴⁵

FATF issued a number of recommendations in 1990 that were subsequently revised in 1996, 2001, 2003 and in 2012 to ensure that they reflect the most recent developments. These form a base of the EU AML legislation.

The Table below provides a summary of the key international bodies and their responsibilities with regard to the AML.

Table 3.5 - Other international organisations active in the AML area

Name	Responsibilities
International Monetary Fund (IMF)	The IMF helps to shape the international AML/CFT policies, carries out AML/CFT assessments and is involved in the design of AML/CFT-related program measures, a large number of technical assistance, and research projects.
The World Bank	<ul style="list-style-type: none">• assesses the strength and effectiveness of countries efforts in the area of AML and counter terrorist financing (CTF);• carries out regular assessments that are diagnostic tools, identifying flaws or gaps and making recommendations to improve the country's framework⁴⁶

Money laundering

Name	Responsibilities
United Nations Office on Drugs and Crime (UNODC)	The objective of the UNODC Global Program is to strengthen the ability of member states to implement measures against money-laundering and the financing of terrorism and to assist them in detecting, seizing and confiscating illicit proceeds ⁴⁷ .
Interpol	Works to combat money laundering through the global exchange of data, supporting operations in the field, and bringing together experts from the variety of sectors concerned ⁴⁸ .
Other international organisations	<ul style="list-style-type: none">• Asia/Pacific Group on Money Laundering;• Caribbean Financial Action Task Force;• Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism;• Eurasian Group ;• European Central Bank;• European Bank for Reconstruction and Development.

European Union

Over the past number of years the EU has made a great effort to harmonise its regulations and ensure they are of a high standard. There is a high level of collaboration between Member States which is reflected in the developments of the common standards to be adopted by the EU countries. The key element of the current EU AML regulations is the Third Money Laundering Directive (2005/60/EC) (the Directive).

The Third Money Laundering Directive (2005/60/EC)

The Directive applies to banks, the financial sector as well as lawyers, notaries, accountants, real estate agents, casinos and company service providers. Its scope also encompasses all dealers in goods, when payments are made in cash in excess of €15, 000⁴⁹.

The Directive requires those who fall within its scope to apply either standard or simplified or enhanced customer due diligence procedures depending on the risk of customer.

Since the directive was first introduced in 2005, FATF has issued revised recommendations which will need to be reflected in the EU regulations. The development on the Fourth EU Anti-Money Laundering Directive is under way.

The Fourth Money Laundering Directive

The proposed Fourth Money Laundering Directive aims to reduce ambiguities in the existing regulations and further expand the scope of AML systems. It is expected that the directive will be introduced in late 2015.

The key changes that are expected to be reflected in the Fourth EU Anti-Money Laundering Directive relate to further expansion of the scope of the definition of designated person, new regulations regarding the countries' AML regimes, additional provisions regarding treatment of politically exposed persons and clarification of data protection mechanisms.

Other instruments governing the AML regulations in the EU are:

- Directive 2006/70 (Politically Exposed Persons);
- Regulation 1781/2006 (Traceability of transfers of funds);
- Regulation 1889/2005 (Controls of cash); and
- EU Council Decision 2000/642 (Cooperation between financial intelligence units of the Member States).

Ireland

In recent years Ireland has advanced significantly in terms of AML regulations and enforcement driven by the EU harmonisation efforts. Despite this, there are still areas that require attention to further strengthen and improve the Irish AML systems.

Below we provide an assessment of Ireland's current legislative, compliance and enforcement position. In addition we review recent improvements made and discuss what could be done to further strengthen the Irish AML system.

Money laundering

Legislation

AML legislation in Ireland was initially introduced in 1994. Although since then there have been a number of regulations and amendments, there has been no single framework that would guard AML systems in Ireland.

Money Laundering Primary Legislation prior to CJA 2010:

- Criminal Justice Act 1994 (Sections 31, 32, 57)
- Disclosure of Certain Information for Taxation and Other Purposes Act 1996 (Section 2)
- Criminal Justice (Miscellaneous Provisions) Act 1997 (Sections 14, 15)
- Criminal Justice Act 1999 (Sections 25–28)
- Criminal Justice (Theft and Fraud Offences) Act 2001 (Sections 21–23)
- Central Bank and Financial Services Authority of Ireland Act 2003 (Section 33AK)
- Criminal Justice (Terrorist Offences) Act 2005 (Sections 32 and 36)

In 2010, the Criminal Justice (Anti-Money Laundering and counter Terrorist Financing) Act 2010 (“CJA”) transposed the Third Anti-Money Laundering Directive into the Irish law. The Act creates a comprehensive framework that requires designated persons to apply a risk based approach to their relationship with clients. The CJA 2013 has since been introduced which broadened the CJA 2010.

“The Criminal Justice (Money Laundering and Terrorist Financing) Act, 2010 represents a radical overhaul of the anti-money laundering system in establishing a new framework of anti-money laundering regulation for credit and financial institutions and other "designated persons"

The Minister for Justice, Equality and Defence, Mr. Alan Shatter T.D.

Prior to the introduction of the CJA 2010 the Irish AML system was underdeveloped. An assessment carried out by FATF in 2006 placed Ireland in a follow-up process as a result of a partially compliant rating for certain core recommendations in relation to AML. Since the introduction of the CJA 2010, FATF has recognised that Ireland had made substantial progress in addressing the

deficiencies identified in the 2006 assessment and has removed Ireland from the regular follow-up process in June 2013⁵⁰.

Whilst CJA 2010 creates a comprehensive AML regulatory environment in Ireland, it has taken 5 years to develop this Act and transpose the Third AML Directive into Irish Law. In the context of the Fourth AML Directive being developed, Ireland needs to be prepared to amend and expand its regulations to effectively reflect any developments proposed by the Fourth Directive in a timely manner.

Collaboration between stakeholders

The responsibility for the AML framework in Ireland is divided between the professional supervisory bodies, that are responsible for control and compliance and An Garda Síochána and the Revenue Commissioners who are responsible for enforcement and investigations. An Garda Síochána and the Revenue Commissioners receive STRs from both the supervisory bodies and from the individual companies. Therefore to ensure effective and efficient operation of the AML controls a high level of communication and co-operation is required.

Compliance and control

The CJA 2010 has identified supervisory authorities for different sectors. For example, the Central Bank of Ireland is responsible for compliance and control of the credit and financial entities. The supervisory authorities assess the compliance by the companies and impose sanctions on those who fail to comply.

“Enforcement is a key component of the regulatory framework and we will continue to work with our supervisory colleagues to implement a system of assertive risk based supervision backed up by the credible threat of enforcement”

Derville Rowland, Director of Enforcement of the Central Bank of Ireland⁵¹

Money laundering

The overall level of compliance has shown improvement, which is likely to be a result of increased activity and focus of the relevant supervisory bodies. The Table below shows the number of inspections carried out by the selected bodies in 2012 and 2011.

Table 3.6 - Inspections by the selected supervisory authorities in 2011 and 2010⁵²

Name	Total number of AML/CTF inspections in 2012	Total number of AML/CTF inspections in 2011
The Central Bank of Ireland	28	19
The Law Society of Ireland	426 (73% compliant)	370 (70% compliant)
Chartered Accountants Regulatory Board	24 on-site visits	n/a
The Minister for Justice and Equality – Anti-Money laundering compliance unit	368	370

One of the primary functions of the supervisory bodies is education and communication of regulation to companies. They achieve it through issuance of guidelines, ad hoc advice, news updates and seminars. In addition, as a direct result from an increased number of compliance inspections, there has been an increase in the level of education and support to the designated persons from these competent authorities. For example, in October 2012 the Central Bank of Ireland has issued a letter to over 7,000 Irish credit and financial institutions highlighting the importance of AML/CTF and outlining the key control failures it had identified in the course of its inspections.

However, it is important to make sure that all supervising authorities are active in their areas and their educational initiatives are not limited to selected companies. They need to reach the wider target audience and to be organised in a two-way dialogue manner to help organisations in developing a culture of AML compliance.

Enforcement and investigations

An Garda Síochána and the Revenue Commissioners are the enforcement authorities in Ireland who investigate money laundering and terrorist financing.

Over the past number of years, the number of STR to both An Garda Síochána and the Revenue Commissioners has increased. A relative increase in the number of STRs can relate to an increase in the level of suspicious activity or, which is more likely given the efforts of compliance and enforcement agencies, to an increased awareness about the reporting obligations by the designated persons.

Table 3.7 - Inspections by the selected supervisory authorities from 2009 and 2012⁵³

	2009	2010	2011	2012
An Garda Síochána	10,400	13,416	11,168	12,488
Revenue Commissioners	-	-	11,070	12,175

Despite the increase in the number of STRs, there has been a low level of prosecutions in relation to money laundering. Only four people were charged with money laundering offences between 2011 and 2012. There are a number of reasons that can explain the low level of prosecutions.

One reason for the low level of prosecutions may relate to the fact that “it is the practice that an individual is charged with a predicate offence⁵⁴ only as this is the substantive crime whereas the money laundering is regarded as the ancillary⁵⁵ offence”⁵⁶. Therefore, whilst the criminal is ultimately prosecuted for the primary crime, he is not charged for the money laundering offence under the CJA 2010.

The second reason could relate to the fact, that 80% of the STRs filed relate to the tax offences⁵⁷ and despite the fact that tax evasion falls within the CJA 2010 definition of money laundering⁵⁸, these offences are prosecuted solely under the tax regulations. The main rationale behind this is likely to relate to the cost of investigation and prosecution. Due to the complicated nature of money laundering transactions, it is more expensive to carry out a money laundering

Money laundering

investigation compared to the cost of a tax evasion investigation and enforcement process. Despite the fact that significant amounts of money are recovered by the Criminal Assets Bureau from the other offences that are associated with money laundering and terrorist financing, the fact that tax evasion is prosecuted solely under the tax regulations means that enforcement of the CJA 2010 remains weak.

This low level of prosecutions under the CJA 2010 suggests that AML has not been a priority in Ireland.

Reporting

Despite the noticeable improvements in the areas of enforcement and recording, compared to 2010, when Ireland was one of the two EU countries (the second was France) that were unable to provide data for the Eurostat study on money laundering in Europe, transparency of the enforcement system still requires improvement. Specifically, this would be in the area of compilation of statistical data⁵⁹ to provide a fair reflection on the issue of money laundering and the progress made in AML.

In Ireland, a key element of the AML framework is the system of reporting suspicious transactions by companies and individuals. For the system to operate efficiently, reporting must be instant and should take a unified form. However, it is likely that there remains a significant number of unreported suspicious transactions by the designated persons. Our experience shows that the key reasons for this are the cultural barriers, a lack of understanding, an insufficient level of training and an inability to distinguish money laundering from other finance related offences by the reporting entities. The best way to approach this problem is through comprehensive training and through feedback.

In relation to feedback, currently the Garda Financial Intelligence Unit and the Revenue Commissioners are making efforts through the hosting of annual events with major stakeholders to facilitate a feedback process and discuss other related

issues. Whilst this is a good approach, more could be done to increase transparency and acknowledge the efforts made by individual stakeholders.

Training

To create an environment that restricts the ability of organised crime groups to launder money it is necessary not only to introduce the laws and regulations but also to ensure that appropriate educational efforts are made to create awareness and facilitate the culture of compliance. The importance of training and education has been recognised in the CJA 2010 and one of key is for companies to ensure that appropriate training is received by all staff.

From our experience, it is evident that, although very competent in terms of regulatory requirements, the service providers offering AML training often lack “on the ground” expertise in the area of AML. This training, whilst achieving an objective of communicating the regulatory requirements, does not create the urgency, facilitate understanding or develop a culture of compliance. More practical and tailored training could significantly improve the quality of STRs and address the issue of under-reporting.

The issue of developing a culture of compliance and reporting is especially relevant for Ireland which has traditionally had a poor record on reporting. As a distinct feature of the Irish culture, it will be important that proactive efforts to raise the awareness of the issue of money laundering are required to change the mind-set.

“Throughout history, the tag of “informer” had been “one of the dirtiest words in the Irish vocabulary, so we have to change that culture”

Brendan Howlin, T.D. Minister for Public Expenditure and Reform⁶⁰

Cultural change is often the most difficult change to manage. In order for it to be successful, a collaborative effort is required from regulators, enforcement agencies, companies and individuals. This should include training given by people

Money laundering

who can inspire and lead by an example, feedback from enforcement agencies, internal policies and procedures within companies and overall appreciation and acceptance of the urge and necessity to report money laundering and terrorist financing transactions.

“The cultural shift has to happen with practice, with education, with training, with a code of conduct that is respected by employers, so that at the end of the day the resort to the legislation is rare”
Brendan Howlin, T.D. Minister for Public Expenditure and Reform⁶¹

With creation of a culture of compliance being a strategic priority and continuous improvements in enforcement and control Ireland will continue improving its AML systems, ensure security of its legitimate financial systems and remain an attractive destination for investors.

Conclusion

Money laundering is a widespread crime that has close links to organised crime and can also provide funds for terrorist financing. The importance of AML to the society, the economy and the reputation of Ireland has been highlighted throughout this section.

Ireland has made marked progress in terms of its AML framework in recent years. Despite this, there are a number of areas that require further attention. To ensure that continuous progress is achieved and to facilitate an on-going improvement of the Irish AML system we have suggested some recommendations in the following areas:

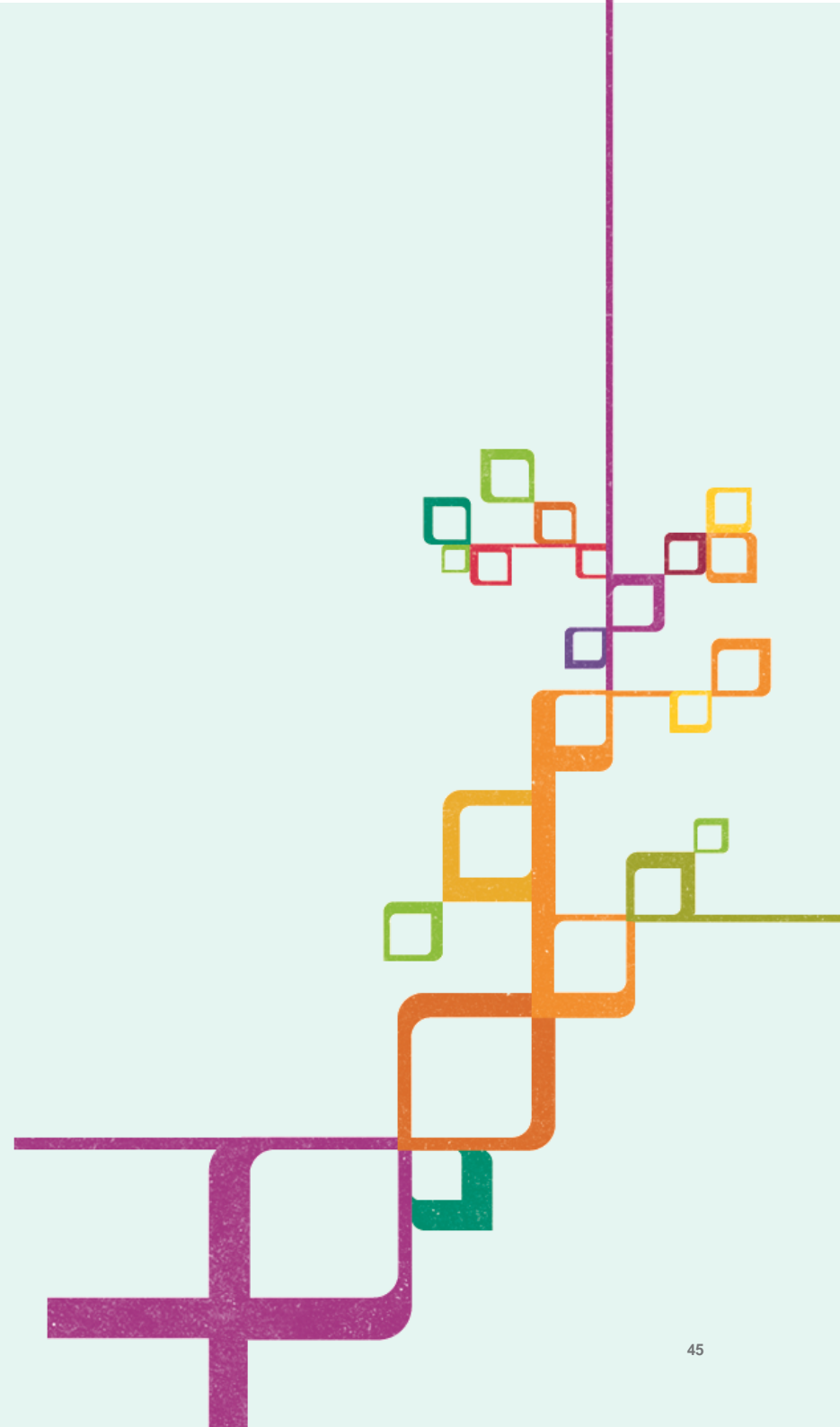
- **legislation:** the CJA 2010 was a huge advancement for the Irish AML systems. However, it took five years from the introduction of the Third AML directive for it to be developed. With the Fourth AML directive underway, Irish regulators should be prepared to promptly update the existing regulations;

- **reporting by the compliance and enforcement bodies:** a more thorough compilation of data is required to reflect the true and fair scope of the money laundering issue in Ireland;
- **reporting by the designated persons:** the issues of under-reporting and reporting of activities not related to money laundering need to be addressed primarily through education and feedback;
- **education and training:** whilst some guidance has been provided to designated persons in Ireland a more dialog-like approach is recommended to ensure full understanding of the regulatory requirements, including standards of suspicious transactions reporting;
- **creation of a culture of compliance:** reporting and whistleblowing have traditionally been underdeveloped in Ireland due to cultural specifics. For those providing training to designated persons it is important to create urgency around the problem of money laundering to facilitate a thorough understanding of responsibility and reporting obligations; and
- **collaboration:** similar to last year’s findings, when looking at the level of cooperation between various agencies both internationally and in the domestic economy, a common theme emerges. Whilst significant effort has been made to tackle different areas of illicit trade and money laundering by both regulators and enforcement agents, a more co-ordinated approach is required to ensure that the issue continues to be addressed appropriately.

“Our current self-assessment is that we have a distance to travel in this area if we are to reach international standards or best practice. It is likely that the current IMF review will concur with this view. It is therefore important that we continue to focus on this area.”

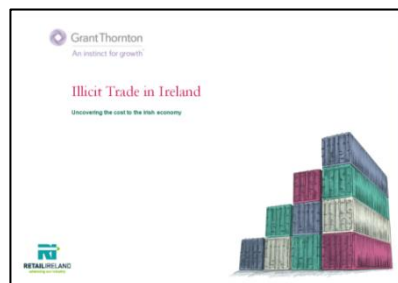
Cyril Roux, the new Deputy Governor and Head of Regulation at the Central Bank of Ireland

4 Retail update



Introduction

In 2013 Grant Thornton, together with Retail Ireland, presented a report on illicit trade in Ireland. The report, entitled “Illicit trade in Ireland - Uncovering the cost to the Irish economy”, focused on a number of core areas in the retail sector that are most affected by illicit trade, namely: fuel, tobacco, digital piracy and pharmaceuticals. The objective of the report was to highlight the issue of illicit trade and provide a detailed assessment of the problem.



Last year as a result of our assessment we have identified a number of recurring themes across the sectors reviewed, such as, for example, the lack of understanding of the issue, ineffective regulations, and weak international and cross sector collaboration. Based on these common themes we developed a set of recommendations to address the issue of illicit trade in Ireland (see Figure across).

One of the key recommendations last year was the establishment of the cross sectorial Committee on Illicit trade.

This year, we aim to provide an update on the issue of illicit trade in the retail sector.



The purpose of this section is to provide an update on the recent developments in the areas from last year and review the progress made over the past year in combating the issue of illicit trade. Each area includes an overview of the **key developments** and a summary of the **consumer and retailers survey**, which was carried out as part of the report to gather their opinion on the issue of illicit trade.

Key developments

To assess the progress made across the retail industry we reviewed the 2013 developments in the sectors of fuel laundering, tobacco, digital piracy and pharmaceuticals. Our review included a brief summary of the last year findings, any changes in the areas of enforcement, legislation, cost to the economy, key drivers and key stakeholders' opinions. We conclude each section with a short summary of the key areas that require further attention.

Survey

To complement our work we have undertaken a survey of consumers and retailers in Ireland. We believe this approach has enabled us to gain a balanced viewpoint of the issues and how these issues are affecting both consumers and corporates alike. Details of the survey results are presented at the end of each sector.

To undertake this element of the review, we engaged with Amárach who have significant experience of undertaking similar surveys.

Illicit trade in Ireland: consumer survey

- A sample of 1,000 to match the gender, age, social class and region of the Irish population was selected.
- The survey was completed online.

Illicit trade in Ireland: survey of retailers

- A sample of 200 shops, equal number from each region, was selected.
- A 5 minute fact-to-face interview with owners or head managers of retail stores.

What is illicit trade in fuel

- there are four main types of illegal fuel related activities: smuggling, mixing, stretching and fuel laundering;
- we focused on the diesel sector and more specifically fuel laundering as it offers the greatest financial incentive to criminals in Ireland; and
- fuel laundering is the illegal process which removes the marker dye red (UK) and green (ROI) contained in agri-diesel;

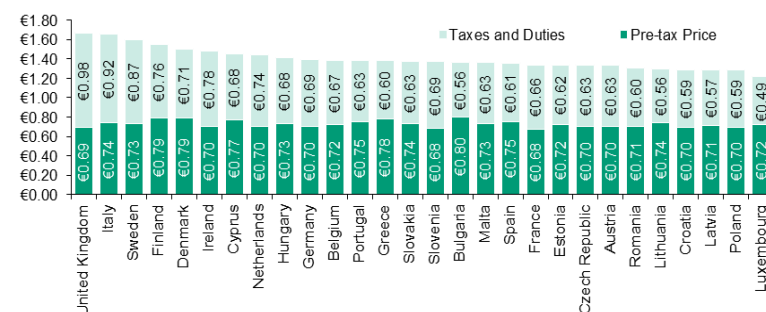
Key findings from 2013 report

- despite positive efforts from enforcement officials, it has become more difficult for officials to detect fraudulent fuel due to the increasing complexity of the supply chain.
- estimates of the financial costs associated range from €140 million to €260 million⁶²;
- the key driver for fuel laundering is the price differential between agri-diesel and road-diesel;
- there are also many non-financial costs: legitimate retailers of fuel are struggling to survive, consumers are being impacted through the damage that such fuel can cause to their engines and local communities are being affected through environmental damage and the subsequent clean-up costs;
- although there is a clear strategy by the Revenue Commissioners to tackle the issue, illicit trade continues to be driven by the price differential as the potential risk of prosecution is outweighed by the potential reward; and
- we identified specific recommendations to tackle fuel laundering:
 - the introduction of new marker technology
 - equalisation of prices
 - essential user fuel rebate
 - registration system
 - audit scheme
 - more punitive penalties.

Key developments in 2013

- Price

- as at 6th January 2014, Ireland had the sixth highest price in the EU at the pump per litre for diesel at €1.48, in comparison to €1.53 at the same time last year⁶³;
- agri-diesel remains significantly cheaper than regular diesel at €1.05 per litre, and there has been no major changes in the price since last year⁶⁴;
- there was no increase on excise duty for fuels in the Budget 2014;
- the Figure across breaks the price down into pre-tax price and taxes and duties segments which are combined to illustrate diesel pump prices across the EU; and
- it appears that price is a key driver of fuel laundering as the incentive still remains.



Key developments

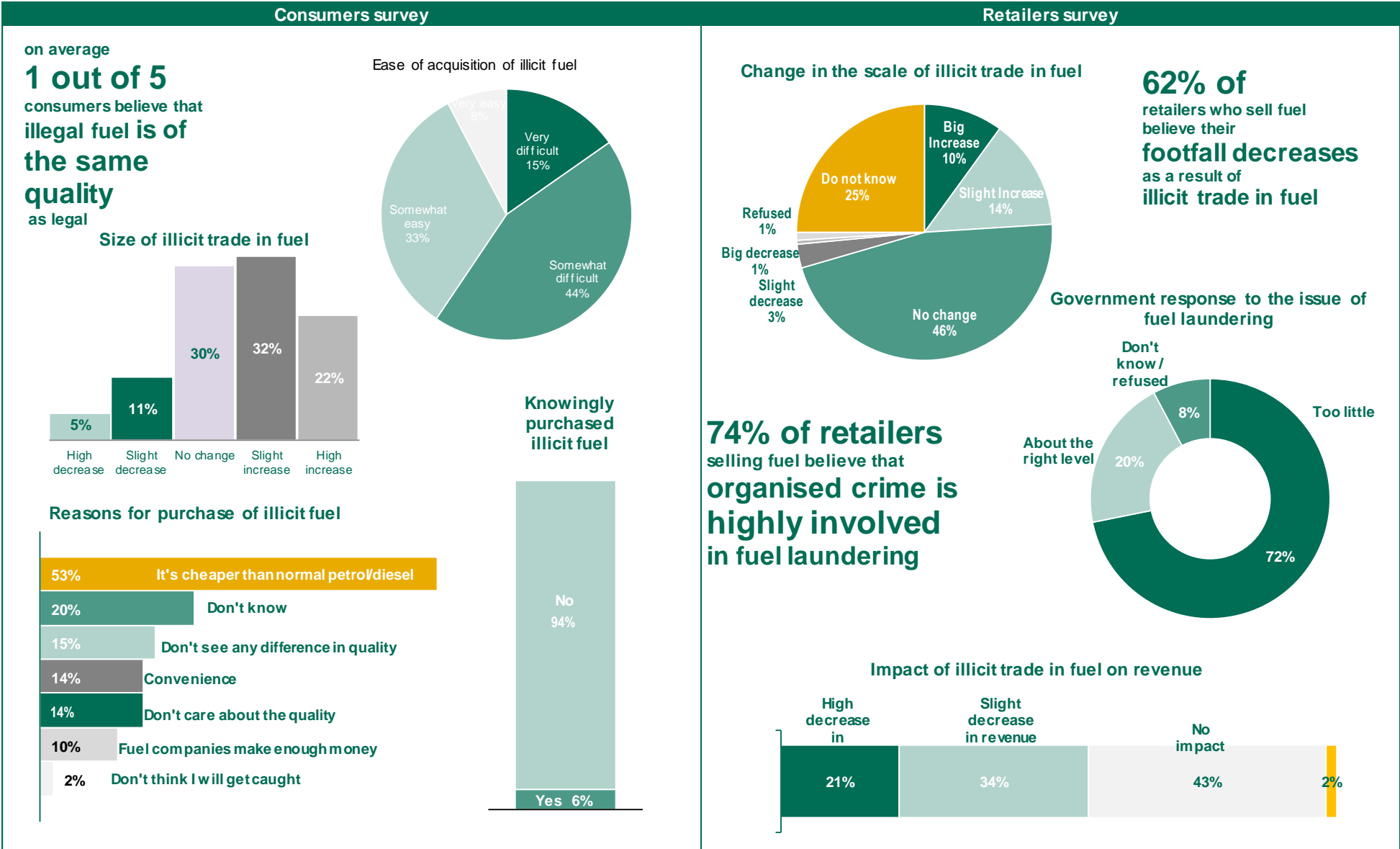
- Enforcement

- there was a higher number of illegal green diesel detections carried out in 2013 with 1,310 occurring, up from 1,158 in 2012. This could suggest either the increasing efforts made by enforcement officials or an increase in fuel laundering⁶⁵;
- 174 vehicles were seized in 2013, up from 114 in 2012 and 67 commercial seizures in 2013, down from 79⁶⁶;
- 533 warning letters were issued and 25 stations were shut down in 2013⁶⁷;
- there were 9 fuel laundry detections in 2013, of which three major discoveries of oil laundering plants occurred⁶⁸;
 - Dublin: in May, with the capacity to launder fuel with a potential loss to the Exchequer of €1.75m per annum;
 - Waterford: in November, with the capacity to launder fuel with a potential loss to the Exchequer of €5 million per annum; and

	2011	2012	2013
Detections	1,153	1,158	1,310
Vehicle seizures	162	114	174
Laundry detections	9	11	9
Commercial seizures	88	79	67

	<ul style="list-style-type: none"> iii Meath: in December, with a potential annual loss to the Exchequer of €1.5 million.
Key developments	
- Legislation	<ul style="list-style-type: none"> the Revenue Commissioners introduced an electronic tracking system to control the movement of product from July 2012 and implemented the system whereby all licensed fuel traders are required to make electronic returns in relation to their fuel transactions each month from early 2013; and to-date, there has been no change in terms of introducing a more effective fuel marker and this has been flagged by Deputy Michael Noonan as an on-going issue and this process is expected to be finalised shortly⁶⁹.
Updated costs to the economy	<ul style="list-style-type: none"> estimated costs of fuel laundering remain unchanged, despite the slight fluctuation of the cost of diesel, with up to €261 million loss to the Exchequer and up to €205 million loss to the retailers.
Industry opinion	<ul style="list-style-type: none"> 55% of the retail survey respondents believe that illicit trade in fuel has had a negative effect on their revenues; 72% believe that the Governments response to the issue of fuel laundering has been insufficient; the Irish Petroleum Industry Association ("IPIA") has acknowledged that there is no single 'silver bullet' that will rid Ireland of this problem. They have made further recommendations to tackle fuel laundering, including: <ul style="list-style-type: none"> a radical overhaul of the imposition of penalties; county councils permanently closing fuelling stations operating illegally; the introduction of an electronic card for off road users with their details which, when used, would automatically register at the discounted price. the introduction of a new marker for off road diesel; suspending licences for offending retailers; and
Consumer opinion	<ul style="list-style-type: none"> 54% of the consumer survey respondents think that there has been an increase in fuel laundering; 41% believe that it is easy to acquire laundered fuel; and the dominating reason for the purchase of illicit fuel was that it's cheaper than legal petrol/diesel.
Conclusion	<ul style="list-style-type: none"> in 2013 fuel laundering continued to have a significant impact on the local economy and the taxpayer despite increased efforts from the Revenue Commissioners to tackle the problem; the high price differential between road diesel and agri-diesel remains unchanged, which continues to create an incentive to launder fuel; despite continued efforts to assist retailers, no major changes have occurred. A more balanced approach should be adopted as there needs to be increasing penalties for those who abuse the system; and in the coming months the impact on fuel laundering of the introduction of more efficient fuel marker will be an interesting development

Survey results



What is illicit trade in tobacco

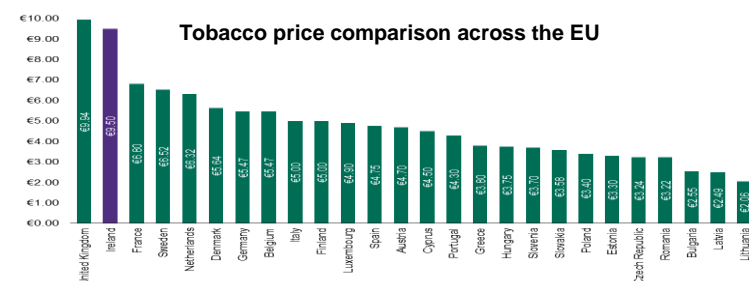
- illicit trade in tobacco deals with the production, importing, exporting, purchasing, sale or possession of tobacco failing to comply with legislation; and
- there are three main classifications of illicit tobacco: contraband, counterfeiting and illicit whites.

Key findings from 2013 report

- the smuggling and sale of illegal cigarettes remains a huge challenge for the independent retail sector, despite the efforts of both the Revenue Commissioners and An Garda Síochána in seeking to deal with this problem;
- as Ireland has the second highest price of tobacco products, the incentive to buy illicit tobacco is driven by price and affordability, whilst the incentive to supply illicit tobacco is driven by the margin of profit available for suppliers;
- different taxation policies in regions bring about opportunities of not paying domestic rates of excise duty to smugglers;
- Revenue estimates losses to the Exchequer to be around €250 million per year, whilst the Irish Tobacco Manufacturers Association estimates that the cost can be as high as €569 million;
- given the high levels of illicit trade and extensive losses to the Exchequer, it is apparent that the taxation policy of continuous increases in excise duties has not acted either as a deterrent or a successful revenue generating measure for the Government, but has only served to perpetuate the market demand for illicit products in Ireland.

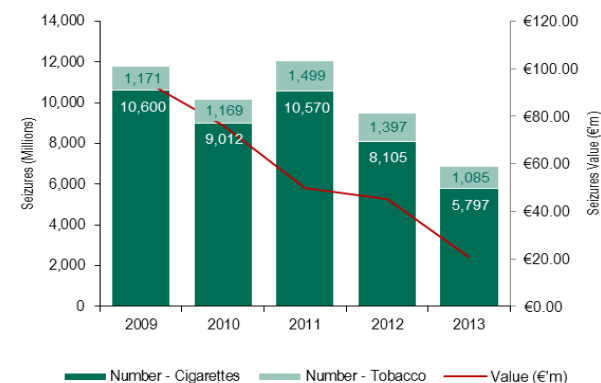
Key developments in 2013 - Price

- excise duty increased by 10c per packet of cigarettes in the Budget 2014;
- Irish Tobacco Manufacturers' Advisory Committee's most recent European price comparison of existing EU countries of tobacco ranks Ireland as the second most expensive country at €9.50 for premium RRP of 20 sticks;
- prices in non-EU countries at the Eastern borders remain significantly lower;
- price, as the key driver of illicit trade in tobacco has increased, so too has the incentive to supply illicit tobacco.



Key developments - Enforcement

- over the past year there has been a significant decline in the number of seizures, in both cigarettes and tobacco. The value of products seized decrease by almost 80% since 2009;
- in 2013, there were 5,797 seizures of illicit tobacco, with the total value of €40 million⁷⁰;
- similar to last year, convictions in 2013 showed conflicting trends from the sale and smuggling of illicit tobacco;
- the number of convictions for cigarette smuggling increased from 56 in 2012 to 66 in 2013, while the number of convictions for cigarette selling decreased from 76 in 2012 to 45 in 2013⁷¹; and
- at the same time the level of consumption has not decreased significantly, which suggests that an evolution in the way organised crime groups are operating and in particular supplying the Irish market. The business of traffickers is constantly evolving as they keep changing their tactics to evade detection.



Key developments - Legislation

- since the publication of the previous report, all tobacco products placed on the market on or after 1 February 2013 must comply with regulations introduced by Minister Reilly in 2011 to place in addition to text warnings, picture health warnings on cigarettes and other smoked tobacco products;
- legislative changes to introduce plain packaging were approved in May 2013 by the Irish government, although this has not yet been enacted into law. There are many contrasting views on this subject. The issue of plain packaging is covered in greater detail in section 1 of this report;
- further legislation change suggested in the Department of Health “*Tobacco Free Ireland*” report is the introduction of fixed penalty notices (on the spot fines) for offences and the publication of the information in relation to these fines⁷²; and
- in 2013, Dublin City Council announced the establishment of a special group comprising The Revenue Commissioners, An Garda Síochána and business owners to tackle the problem in Dublin city centre. The group facilitate the sharing of information and intelligence on the ground between enforcement officials and traders⁷³. Retailers Against Smuggling (“RAS”) hope that such a scheme can be rolled out in other councils throughout the country.

Updated costs to the economy

- the European Anti-Fraud Office, OLAF, estimates that illicit cigarettes result in losses of over €10 billion annually in the European Union⁷⁴;
- tobacco tax is a significant source of tax revenue in Ireland as €1.4 billion is collected in tobacco tax and VAT from tobacco consumption annually⁷⁵; and
- Revenue Commissioners have not yet released the data in relation to the excise receipts, however, by applying the price increase of 1% (or 10c) to the last year estimates, the total loss to the Exchequer can be as high as €575 million (this figure includes €185 million that relates to non-domestic legal cigarettes).

Industry opinion

- 77% of retailers believe that illicit trade in tobacco affects their revenues; with 6 out of 10 noticing the impact it has on the footfall;
- 64% of retailers surveyed believe that the introduction of plain packaging will result in an increase in illicit trade; and
- The National Federation of Retail Newsagents (“NFRN”) in their speech to the Oireachtas on 13 March 2013 stated that “Almost nobody under the age of 30 is coming into our shops to buy cigarettes, and yet the level of smoking in this age group is almost identical to what it was ten years ago. This is because young people are sourcing their tobacco on the black market, putting cash into the pockets of criminals and subversives”⁷⁶.

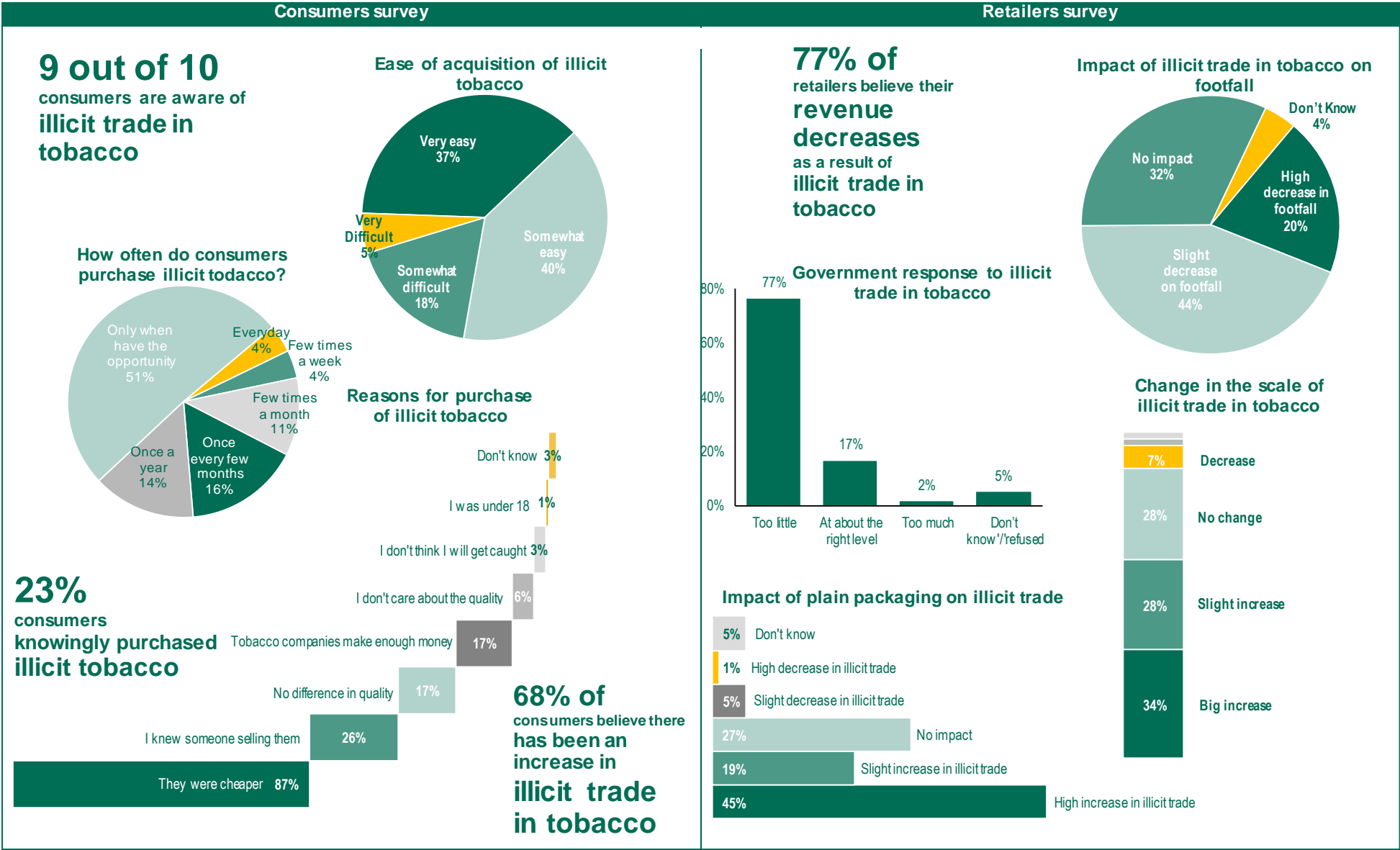
Consumer opinion

- 77% of customer survey respondents as part of this research believe it is relatively easy to purchase illicit tobacco in Ireland;
- 87% said that the reason for purchasing illicit tobacco was that they were cheaper than legal cigarettes. This result indicates that price is the key driver for the purchase of illicit tobacco; and
- over half of the respondents admitted that they believe illicit products are of poorer quality.

Conclusion

- the smuggling and sale of illegal tobacco products remains a huge challenge for the retail sector in 2014. Further joint forces are required in this year’s strategy on combatting the illicit tobacco trade;
- price increases continue to create an incentive for tobacco smugglers and increase illicit trade; and
- as Ireland will be only the second country to introduce plain packaging, the risk of an increase in illicit activity will need to be closely monitored by enforcement officials and the Revenue’s 2014 strategy on combat the illicit tobacco trade will be expected to cover this in detail.

Survey results



What is illicit trade in pharmaceutical products

- illicit trade in pharmaceuticals relates to the sale of falsified or counterfeit medicines; and
- a falsified medicine is any medical product with a false representation of its identity, its source, or its history. A falsified medicine may be counterfeited; or it may be authentic, but the packaging or labelling could be falsified or may be supplied without a valid prescription. Finally, the medicine could contain too much, too little, or no active substance.

Key findings from 2013 report

- the pharmaceutical industry plays an important role in the Irish economy. Last year Ireland was one of the largest net exporters of pharmaceuticals in the world, with the Irish share in global pharmaceutical exports being 7.7%⁷⁷;
- a significant share of FDI in Ireland relates to the pharmaceutical companies, with over 120 overseas companies having their plants in Ireland, including 9 out of the 10 largest pharmaceutical companies.
- the international growth in illicit trade has major consequences for existing and potential FDI in the Irish economy;
- the key drivers of demand are the price differential, convenience and a lack of awareness about the dangers of purchasing medication online;
- the supply, on the other hand, is driven by the high profit margins and ease to produce and conceal;
- the main distribution channel is the internet; in Ireland internet sale of prescription medicine is prohibited;
- the Irish market for illicit medicines is according to Pfizer⁷⁸ (2010) the sixth worst in Europe for illicit medicine trade and its illicit market is worth more than €86 million every year to the economy;
- seizure numbers remain relatively stable, here was no significant change in the amount of seizures of illicit medication in 2012 with €2.1 million worth of medicines detained⁷⁹;
- we have estimated that Irish exporters have potentially suffered losses in revenue in the region of €2.3 billion in 2011. These losses in turnover would represent a loss in corporation tax of between €36.2 million and €57.9 million, with a loss of 1,014 jobs; and
- to tackle the problem we recommended strengthening the supply chain, increasing cross border regulations with regard to online sale of medication, developing a consumer awareness campaign and introducing a digital verification system.

Estimate value of world illicit trade in pharmaceuticals

	WHO, 2005		EFPIA, 2011		Peter Pitts
Value of world pharmaceutical market	€550bn		€614.5bn		n/a
	Low end 5%	High end 8%	Low en 5	High end 8%	\$75bn
Value of illicit trade	€27.5bn	€ 4bn	€30.7bn	€49.1bn	€53.9bn

Key developments in 2013

- Pharmaceutical industry in Ireland

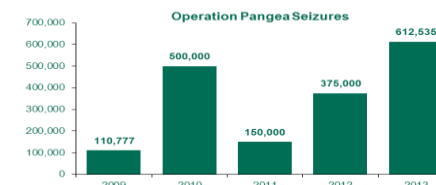
- total Irish export declined by 5% in 2013. The decline is mainly attributed to the reduction of almost €5 billion in the export of chemicals and related products. In 2013, these products accounted for 58% of the Irish export, with 25% being medicinal and pharmaceutical product. This represents a decrease of 2% and 2.5% respectively compared to 2012 Figures and 3% decrease compared to 2011⁸⁰;
- the decrease is likely to be related the expiry of patents on a number of key products manufactured in Ireland⁸¹; and
- despite the fact that the share of Irish exports has declined, it still accounted for 6% (down from 7.7% in 2011) of the global pharmaceutical exports in 2012⁸².

Key developments - Price

- despite the introduction of reference pricing under the Health (Pricing and Supply of Medical Goods) Act 2013 there have been no significant changes to the price of medications in Ireland; and
- the chief executive of the Consumers' Association of Ireland, Dermott Jewell, has said it is "outrageous that the price of medicine is still so astronomically high"⁸³.

Key Developments - Enforcement

- enforcement agencies continue their efforts to combat illicit trade. In the first six months of 2013 over €2 million illegal and counterfeit medicines were detained by the Irish Medicines Board (IMB), Revenue's Customs Service and An Garda Síochána;
- during a week-long INTERPOL co-ordinated operation Pangea by the IMB, Revenue's Customs Service and An Garda Síochána seized over €612,535 worth of illicit drugs⁸⁴; and
- a total of 3,911 enforcement investigations involving breaches of medicinal products legislation were initiated.⁸⁵



Key Developments - Legislation

- the Falsified Medicines Directive was transposed into the Irish law through amendment of the Medicinal Products Regulations (Control of Placing on the Market, Control of Manufacture and Control of Wholesale distribution); and
- the aim of these changes is to prevent the entry of illegal medicines into the legitimate supply chain.

Updated costs to the economy

- using the European Federation of Pharmaceutical Industries and Associations' updated estimates of the value of the global pharmaceutical market (i.e. €667 billion⁸⁶); and
- the share of Irish exports in the global pharmaceutical exports (i.e. 6%); and
- we estimated that illicit trade can cost the Irish pharmaceutical companies up to €3.2 billion, up to almost €50 million in corporation tax losses to the Exchequer and the loss of up to 1,500 jobs.

Industry opinion

- As one of the leading locations for the pharmaceutical industry in Europe the industry opinion of the counterfeiting is critical for Ireland.
- Pat O'Mahony of IMB, said: "As with previous years, the IMB is concerned with the consistent levels of counterfeit and illegal medicines being detained year on year and is warning consumers of the dangers of purchasing medicines from unauthorised sources"⁸⁷.
- Pharmaceutical companies are having to invest millions in security to protect its intellectual property; and
- "Counterfeit medicines pose a serious threat to patient health and safety. Patient who unknowingly purchase counterfeit medicines are denied the therapeutic benefit of the medicines their doctors have prescribed....At Pfizer there is no higher priority than ensuring that every patient who purchases a Pfizer medicine receive an authentic product" – John Clark, Vice President and Chief Security Officer, Pfizer Global Security⁸⁸

Consumer opinion

- Stephen McMahon, Irish Patients' Association, said that despite the huge risk associated with illegal medicines, countries and internet search engine firms are failing to form a unified strategy to tackling illicit trade; and
- the results of the survey, carried out as a part of this research, indicate that cost differential and convenience remain the two key drivers for consumers to purchase medication online.

Conclusion

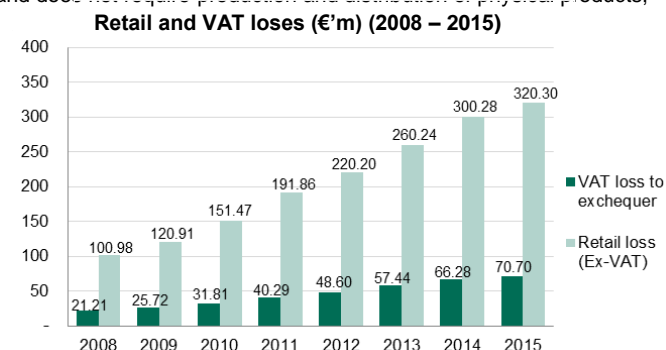
- a number of best-selling drugs' patents are expiring in the near future, resulting in a decrease in the manufacturers' revenues. And as Irish exports remain highly sensitive to the level of pharmaceutical exports, this could lead to an overall decrease of Irish exports;
- to minimise the impacts to economy, Ireland should ensure that it continues its efforts to combat illicit trade and strengthen the legislative framework regarding both manufacturing and distribution of medication and protection of IP of pharmaceutical companies;
- this will facilitate the creation of an environment that will stimulate research and development and ensure FDI continues to flow into Ireland;

What is digital piracy (plus types)?

- the scope of digital piracy includes a range of infringements on IP rights; and
- it includes audio-visual piracy, software piracy and the theft of other electronically transmittable IP.

Key findings from 2013 report

- digital piracy is a major issue both globally and in Ireland;
- unlike other illicit trades, digital piracy is not always motivated by the monetary ambition of criminals and does not require production and distribution of physical products;
- despite these differences the financial implications for both industry and government are significant;
- the demand is driven by the price and convenience;
- the commercial value of software piracy in Ireland is estimated to be around \$144m⁸⁹;
- it is estimated that by 2015 the cumulative job losses in the creative industries sector in Ireland could be as high as 7,376 and the retail sector losses can reach €320 million with an estimated loss to the Exchequer of €70.7 million in tax⁹⁰. Such losses are having a major impact on both creative and retail industries in Ireland. This fact is evidenced by the large numbers of recent high profile commercial casualties within the trade;
- despite the negative impact of digital piracy, it is believed to stimulate innovation as right owners continually improve their products to make it more difficult for the pirates to steal;
- the main legislation regulating IP in Ireland is the Copyright and Related Rights Act, 2000. The Irish High Court Judgement on EMI v UPS⁹¹ case ruled that "Irish copyright legislation currently does not provide appropriate remedies for copyright owners in respect of on-line infringement of their rights"⁹²; and
- in order to protect the digital content and the IP rights associated with it, the legislative framework needs to be strengthened and brought in line with the EU directives.



Key developments in 2013

- Digital industry in Ireland

- two media giants Xtra-vision and HMV went into receivership in 2013. One of the main reasons for the bankruptcy of the two firms, as mentioned by various experts, is the increase in online consumption and digital piracy;
- later in the year, Xtra-vision and HMV (Ireland) were acquired by Hilco Capital, who integrated HMV and Xtra-vision stores and reopened a number of stores around the country under a new business model; and
- development of the new business models is becoming more evident as legitimate businesses are learning to make profits on online streaming of their content (i.e. further development of services such as Spotify). This can be seen as a response to the consumers switch towards streaming of the contents rather than owning a copy of it.

Key Developments - Enforcement

- Sony Music Entertainment Ireland, Universal Music Ireland and Warner Music Ireland are taking a court action against one of the main internet providers in Ireland trying to force it to implement measures such as a graduated response system to the customers accused of piracy⁹³;
- the High Court ordered the Irish internet service providers to block access to bit torrent tracking sites Pirate Bay and Kick Ass Torrents. This created a precedent of blocking access to digital content. However, these measures appear to be ineffective as numerous mirror (or proxy) websites have been created to grant access to the illegal content;
- there are two viewpoints on the blockage of access and the introduction of a graduated response systems. The first opinion is that of the creative industries who insist on the implementation of the above measure to protect their IP rights; the second opinion, which is supported by a number of experts and the Digital Rights Ireland, who insist that the blockage and graduated response systems undermine the freedom of internet and privacy.

Key Developments - Legislation

- the Copyright Review Committee submitted a consultation paper for the Department of Jobs, Enterprise and Innovation. It recommends establishing specialist intellectual property tracks in the District and Circuit Courts and the introduction of innovation and fair use exceptions. It also drafts a Copyright and Related Rights (Innovation) (Amendment) Bill 2013;
- the aim of the proposed changes is to strengthen the position of the right owners whilst allowing for greater access to the contents and innovation to the content users; and
- the term of protection of musician's copyright was extended from 50 to 70 years⁹⁴.

Updated costs to the economy

- in terms of the cost of digital piracy to the Irish economy, there have been no significant changes to our estimates.
- we estimated that:
 - over 900 jobs could be lost in 2013;
 - retailers have suffered a loss of €260 million; and
 - the Exchequer lost €57 million in VAT receipts as a result of digital piracy⁹⁵.

Industry opinion

- the opposition of the audio visual industry to piracy is well-recognised. It is evidenced by the numerous court cases seeking injunctions against internet providers.
- in 2013, the industry has voiced its concern of the slow action of the internet provider and failure to implement a graduated response, similar to Eircom "three strikes policy" and categorised it as "deeply disturbing"⁹⁶;
- for the internet providers they have stated that "it is the government or the courts who are the appropriate body to make such determinations (to prevent piracy) and we await Judge McGovern's decision in this regard"; and
- in addition, in its annual report Sony Music Entertainment Ireland points out that illegal downloading, physical piracy, downward pressure on recorded music, and growing competition for discretionary spending has led to the decline in physical recorded sales⁹⁷.

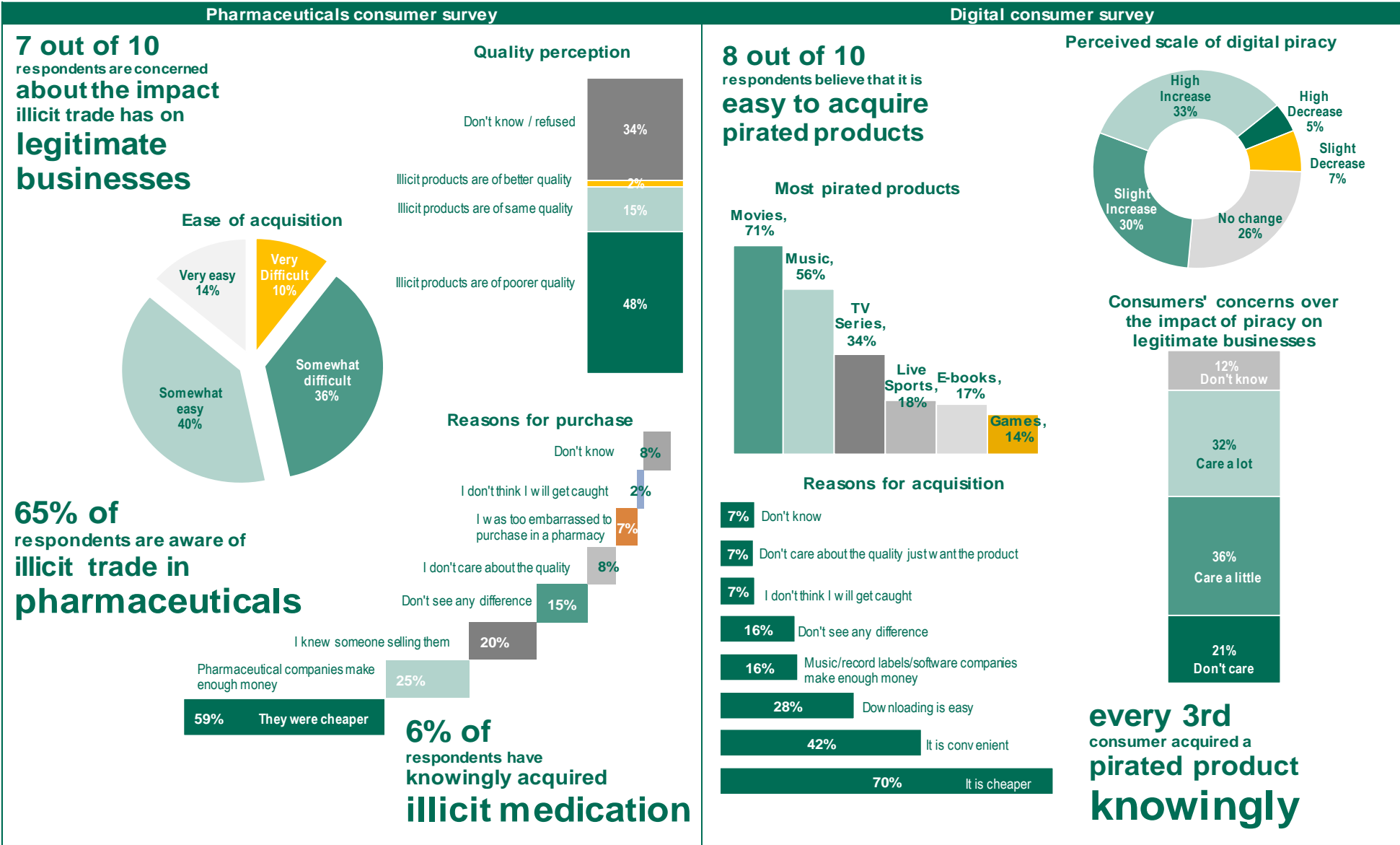
Consumer opinion

- consumers continue accessing the digital content online;
- over 35% of consumers who responded to our survey this year confirmed that they have knowingly illegally downloaded digital content; and
- with 70% of respondents selecting cost and 42% selecting convenience as the main reason for their downloads.

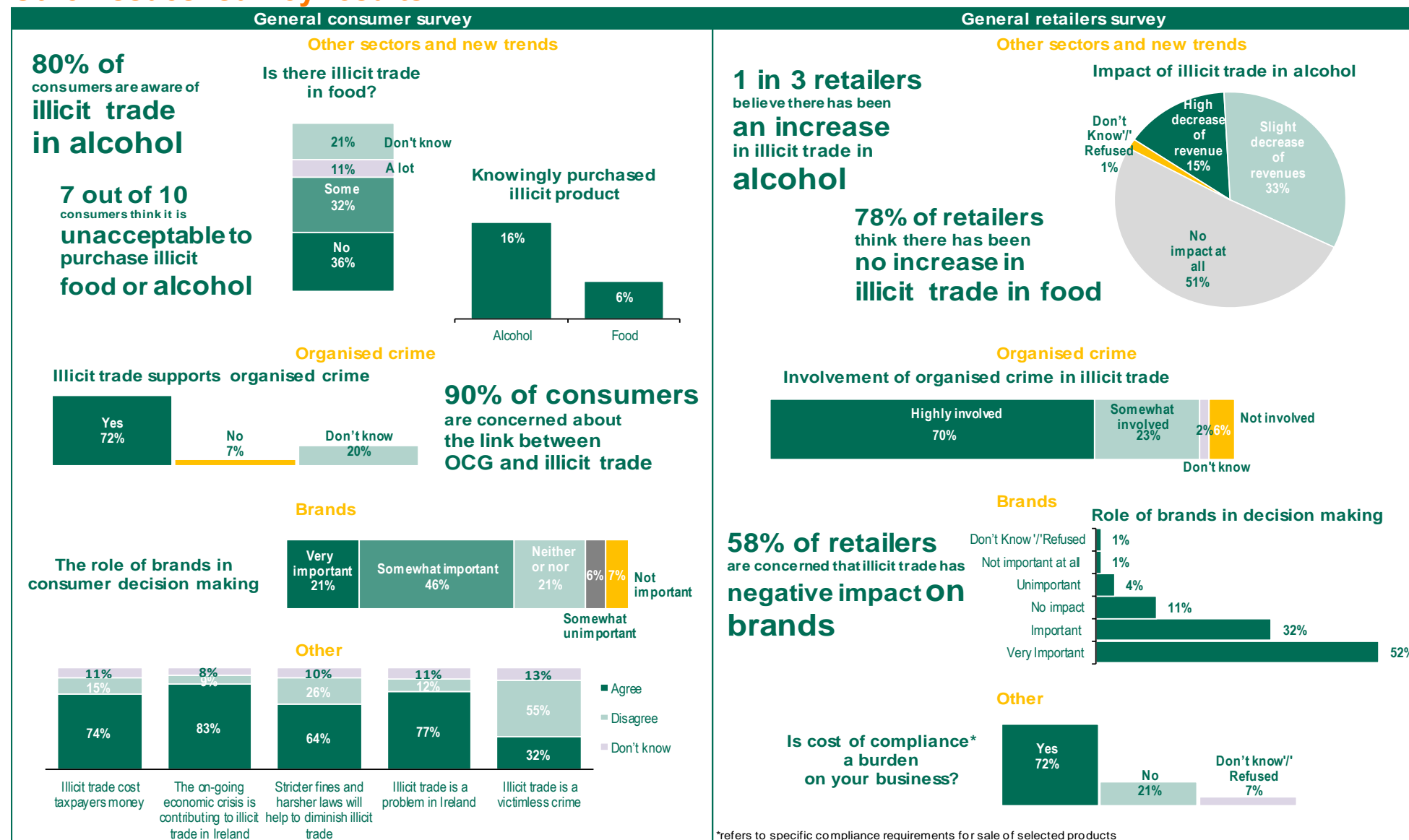
Conclusion

- digital piracy continues to undermine the creative industries growth and results in closures of legitimate businesses, significant losses to retailers, right owners and the Exchequer. In addition, a significant number of jobs are lost annually as a result of digital piracy;
- enforcement measures appear to be expensive and inefficient as pirates continue to find ways around the legislation and Court rulings. As a result, the trend emerges where businesses are starting to move towards new business models that allow exploitation of the opportunities offered by the new technologies; and
- despite the fact that various steps have been taken in 2013, including the publication of recommendations by the Copyright Review Committee, no regulatory change has been made. The issue is very complicated and the solution needs to take into account two extreme viewpoints. Various stakeholders, including the Government bodies, industry representatives, service providers and consumers should come together to develop a co-ordinated approach to the issue of digital crime. Different perspectives on the issue will facilitate the development of a flexible framework that will both protect the legitimate businesses and allow users to enjoy the products of creative industries whilst protecting their privacy and freedom of internet.

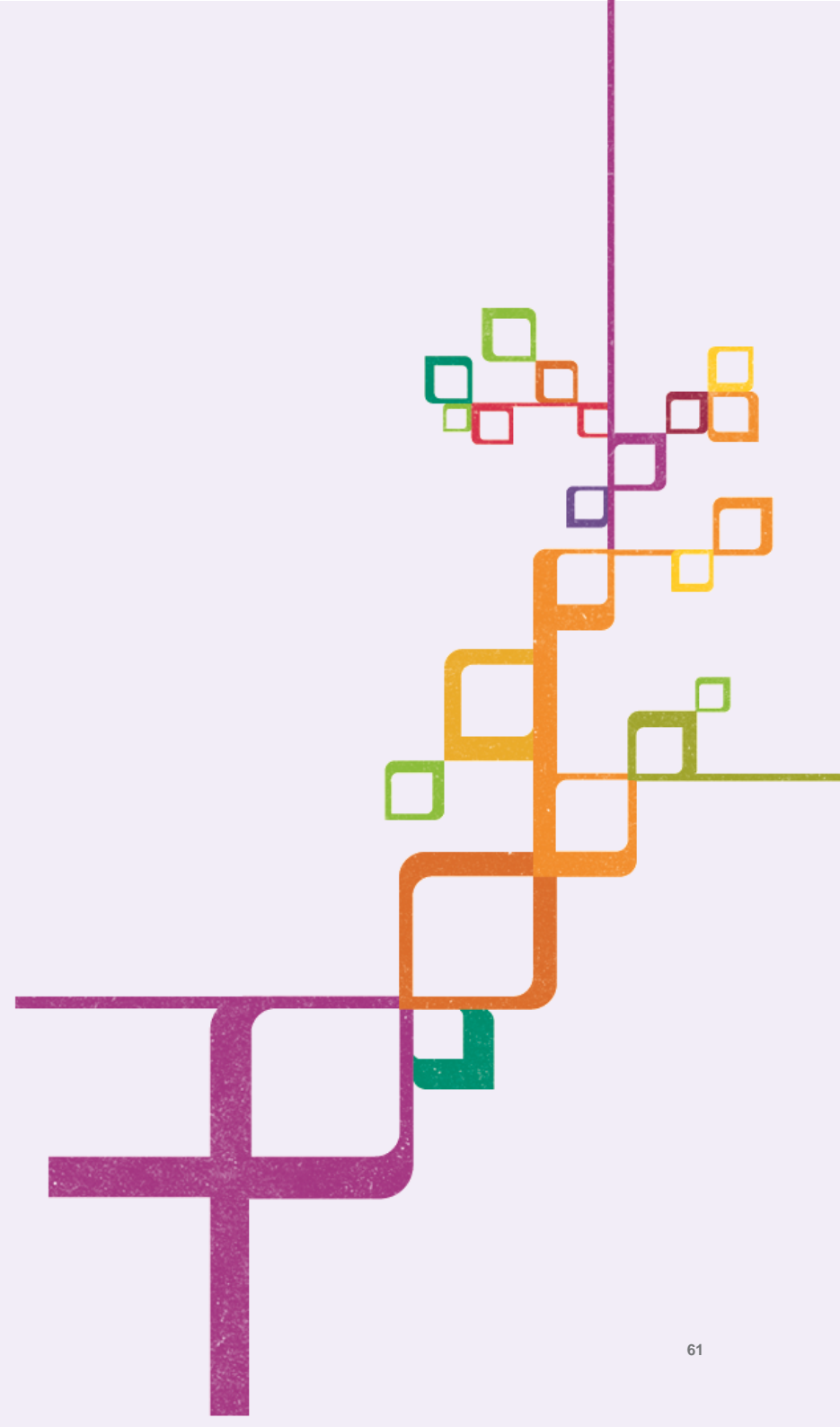
Survey results



Other issues: survey results



5 Conclusion



Conclusion

In this paper we have reviewed the issue of international illicit trade and its implications for the Irish economy. Measures have been taken to address this issue by both businesses and policymakers; however they have not been sufficient to meet the rapidly evolving nature of the global environment.

Widespread abuse of IP, increasing instances of cybercrime and money laundering continue to have an adverse effect on both the national and international economies. The international nature of illicit trade has only served to heighten the problem.

In this report, we have estimated that:

- cybercrime is costing the Irish economy €630 million annually;
- over €5 billion is laundered annually through the Irish financial system; and
- losses incurred as a result of illicit trade in retail could be as high as €1.5 billion.

Across every industry, there have been efforts to tackle the problem, despite this, it has not been sufficient to halt the escalation of illicit trade. A joined up approach is needed to include education, legislation and enforcement across a variety of sectors and government agencies (this approach is illustrated by the figure across). The implementation of such an approach is required at three distinct levels:

- national,
- international; and
- corporate.

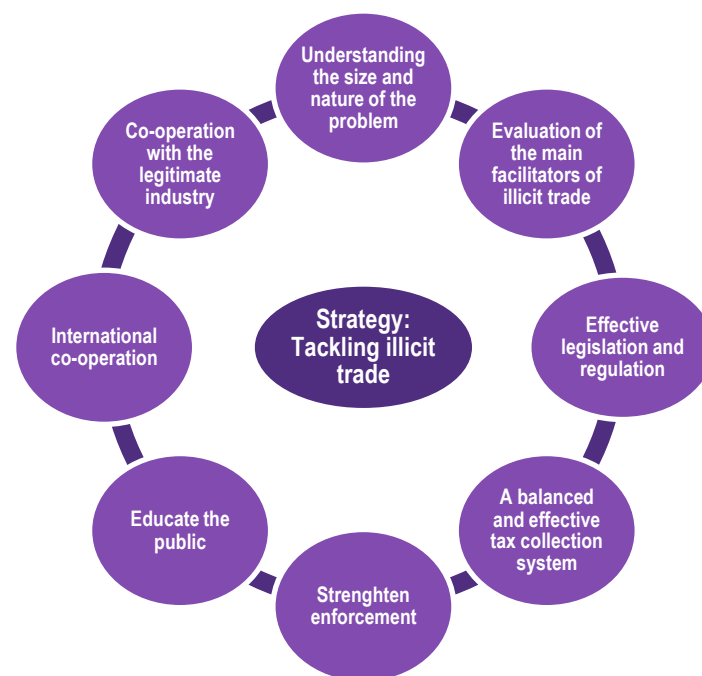
At a national level, the introduction of a strategic plan by the government is essential to combating the broad issue of illicit trade across a variety of sectors. This could be done through the introduction of a committee which would have direct responsibility for addressing the issue illicit trade in Ireland.

At an international level, more needs to be done to bring the developing countries towards international trade and to ensure that there are appropriate economic

incentives for them to comply with a more harmonised set of regulations (AML, cybercrime and IP).

Finally, there is a growing list of corporate victims being affected by illicit trade. To avoid this fate, organisations need to rethink their strategies to ensure that they are flexible and can keep pace with the emerging trends of technology, access and consumption.

In conclusion, illicit trade in Ireland continues to be a significant issue across a variety of sectors and unless more is done by policy makers it will continue to be a drain on our economy. For Ireland with its focus on FDI and innovation we need to be vigilant and proactive in our response to tackling illicit trade.



About us

About us

At Grant Thornton, we combine award-winning technical expertise with the intuition, insight and confidence gained from our extensive sectoral experience and a deep understanding of our clients. Through empowered client service teams, approachable partners and shorter decision-making chains, we provide a wider point of view. For clients, this means we can offer more meaningful and forward-looking advice. In Ireland, we are led by more than 36 partners and employ 500 of the profession's brightest minds, operating from five offices. We provide assurance, tax and specialist advisory services to over 10,000 privately-held businesses, public interest entities and individuals nationwide.

Our Advisory services team

Our Advisory Services team offers a range of services to support organisations in improving their performance by identifying opportunities to cut costs, assess risks, grow revenues, drive bottom line results, and achieve strategic objectives/goals. In doing this we:

- provide a comprehensive, objective and independent view of businesses and their operations;
- bring to bear our experience of conducting similar assignments in a range of industries; and
- incorporate international best practice from our Grant Thornton international network.

For more information on the contents of this report, please contact a member of our team.



Brendan Foster
Partner Business Consulting and Advisory
E brendan.foster@ie.gt.com



Elaine Daly
Director, Business Consulting
E elaine.daly@ie.gt.com



Colin Fearon
Manager, Business Consulting
E colin.fearonl@ie.gt.com



Nadia Pustoshilova
Consultant, Business Consulting
E nadia.pustoshilova@ie.gt.com



Sheila Duignan
Partner, Regulatory Advisory Services
E sheila.duignan@ie.gt.com



Mike Harris
Partner, Cyber Security
E mike.harris@ie.gt.com



Paul Jacobs
Partner, Forensic & Investigation
E paul.jacobs@ie.gt.com



Patrick D'Arcy
Director, Forensic & Investigation
E patrick.darcy@ie.gt.com

Notices

The information in this report is based on publicly available information and reflects prevailing conditions and our views as of this date, all of which are accordingly subject to change. In preparing this report, we have relied upon and assumed, without independent verification, the accuracy and completeness of any information available from public sources.

The information in this report is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no such guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

This report and the associated conference provides recommendations based on an analysis of certain publicly available information, the inclusion or exclusion of certain factors and/or issues should not be viewed as a definitive recommendation for or against any actions and we would recommend that thorough due diligence is performed prior to making any decisions.

This report has utilised a combination of information and data from previously published reports together with unpublished data and consultations. We would like to thank the many individuals, organisations and companies for their support and contribution in putting this report together. We have accredited source data where possible and apologise if omissions have occurred in error.

While the information presented and views expressed in this report and oral briefing has been prepared in good faith, Grant Thornton accepts no responsibility or liability to any party in connection with such information or views.

Bibliography

- ¹ Grant Thornton analysis
- ² Grant Thornton, Retail Ireland, 2013 "Illicit trade in Ireland: Uncovering the cost to the Irish economy"
- ³ The European Patent Office, the Office for Harmonization in the Internal Market, 2013, "Intellectual property rights intensive industries: contribution to economic performance and employment in the European Union, Industry-Level Analysis Report, September 2013"
- ⁴ The European Patent Office, the Office for Harmonization in the Internal Market, 2013, "Intellectual property rights intensive industries: contribution to economic performance and employment in the European Union, Industry-Level Analysis Report, September 2013"
- ⁵ International Chamber of Commerce, Global Impacts Study 2011
- ⁶ World Economic Forum, IP rights in the global creative economy, 2013
- ⁷ WIPO, 2002, "Intellectual Property On The Internet: A Survey Of Issues"
- ⁸ WIPO, Global Congress on Combating Counterfeiting and Piracy
- ⁹ European Commission, 2013, "Report on EU Customs enforcement of intellectual property rights. Results at the EU border 2012"
- ¹⁰ World Economic Forum, 2013, "The Global Competitiveness Report 2013–2014"
- ¹¹ Grant Thornton estimate, 2014
- ¹² World Cancer Report 2014, Edited by Bernard W. Stewart and Christopher P. Wild
- ¹³ Presentation by Ibec to Oireachtas Committee on Health and Children, 6 February, 2014
- ¹⁴ Pamela Newenham, 2013, "Tánaiste says data breach a wake-up call on cybercrime", The Irish Times 16 November. Available from www.irishtimes.com ,
- ¹⁵ Gavan Reilly, 2012, "US woman gets six-year sentence for hiring 'Lying Eyes' hitman", The journal.ie 16 January. Available from www.thejournal.ie
- ¹⁶ RTE News, 2005, "Whelan given life sentence for wife's murder", RTE News 12 April. Available from www.rte.ie
- ¹⁷ Conor Pope, Elaine Edwards, 2013 "Over 1.5 million affected by Ennis data breach", The Irish Times 12 November. Available from: www.irishtimes.com
- ¹⁸ An Garda Síochána, Garda Warning in relation to Computer Scam "Police" Trojan – Ransomware
- ¹⁹ Rupert Steiner, Sam Greenhill, 2014, "Turmoil at Barclays as whistleblower reveals 27,000 customers personal details were sold on black market", 9 February, This is Money. Available at: www.thisismoney.co.uk
- ²⁰ Ken Westin, 2013, "Stolen Target Credit Cards and the Black Market: How the Digital Underground Works", 21 December, The State of Security. Available at: www.tripwire.com
- ²¹ Verizon, Data Breach Investigations Report 2013
- ²² Annual Report 2013, Data protection commissioner
- ²³ Annual Report 2013, Data protection commissioner
- ²⁴ IPSO, 2013, "ROI Card Payment Fraud Statistics 2012"
- ²⁵ IPSO, 2013, "ROI Card Payment Fraud Statistics 2012"
- ²⁶ We have worked from the fact that the Irish economy accounts for about 0.34 of the world GDP and scaled our national estimates up or down as appropriate.
- ²⁷ Measuring the cost of cybercrime, university of Cambridge- 2012
- ²⁸ Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"
- ²⁹ Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"
- ³⁰ Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"
- ³¹ Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"
- ³² RSA, EMC2, 2013, "Phishing kits – the same wolf just a different sheep's clothing"
- ³³ BSA, 2012 "Shadow market 2011 BSA global software piracy study", Ninth edition
- ³⁴ BSA, 2012 "Shadow market 2011 BSA global software piracy study", Ninth edition
- ³⁵ Noel Baker, 2010, "Online piracy 'will cost music industry millions'", 12 October , Irish Examiner. Available at: www.irishexaminer.com
- ³⁶ IFPI, 2006, "The recording industry 2006 piracy report"
- ³⁷ Ireland, UK, and World – Grant Thornton estimates based on operation Pangea 2013 results.
- ³⁸ Mr Alan Shatter T.D., 2011, "Minister Alan Shatter gives details of his Department's anti-money laundering and terrorist financing initiative", Department Of Justice And Equality 17 October, Available from: www.justice.ie
- ³⁹ Mary Everett, Joe McNeill and Gillian Phelan, 2013, "Measuring the Value Added of the Financial Sector in Ireland", Quarterly Bulletin, 2 April. Available from: www.centralbank.ie

⁴⁰ UNODC, July 2012, “New UNODC campaign highlights transnational organized crime as a US\$870 billion a year business”, Available from: www.unodc.org

⁴¹ Cormac O’Keeffe, 2012, “Callinan: 25 organised crime gangs in country”, Irish Examiners, 22 November. Available from: www.irishexaminer.com

⁴² FATF, 2014, What is money laundering? Available at: www.fatf-gafi.org

⁴³ European Parliament, 2013, “Cracking down on organised crime, corruption and money laundering”, 23 October. Available at: www.europarl.europa.eu

⁴⁴ Friedrich Scheneider, Turnover of Organised Crime and Money laundering: some preliminary empirical findings, 2008

⁴⁵ FATF, 2014

⁴⁶ The World Bank, 2014, Assessments. Available from: web.worldbank.org

⁴⁷ UNODC, 2014, UNODC on money-laundering and countering the financing of terrorism. Available from: www.unodc.org

⁴⁸ Interpol, 2014, Money Laundering. Available from: www.interpol.int

⁴⁹ European Commission - MEMO/13/64, 2013, “Frequently asked questions: Anti-Money Laundering”, 5 February

⁵⁰ FATF, 2013, Mutual Evaluation of Ireland: 11th Follow-up Report

⁵¹ Central Bank of Ireland, 2013, “General comment by Director of Enforcement, Derville Rowland, on the Central Bank’s enforcement activities”, 19 February. Available from: www.centralbank.ie

⁵² Anti-Money Laundering Compliance Unit, Money Laundering/Terrorist Financing, Statistics report 2011, 2012

⁵³ Anti-Money Laundering Compliance Unit, Money Laundering/Terrorist Financing, Statistics report 2011, 2012

⁵⁴ Main crime

⁵⁵ Secondary offence

⁵⁶ Anti-Money Laundering Compliance Unit, Money Laundering/Terrorist Financing, Statistics report 2012

⁵⁷ Anti-Money Laundering Compliance Unit, Money Laundering/Terrorist Financing, Statistics report 2012

⁵⁸ Part II Sectoral Guidance for credit unions

⁵⁹ Anti-Money Laundering Compliance Unit, Money Laundering/Terrorist Financing, Statistics report 2011, 2012

⁶⁰ Mark Hennessy, 2013, “Ireland to get ‘world-class’ whistleblower law, Howlin says”, The Irish Times, 2 November. Available from: www.irishtimes.com

⁶¹ Mark Hennessy, 2013, “Ireland to get ‘world-class’ whistleblower law, Howlin says”, The Irish Times, 2 November. Available from: www.irishtimes.com

⁶² Grant Thornton, Retail Ireland, 2013, “Illicit Trade in Ireland: uncovering the cost to the Irish economy”

⁶³ EU Oil Bulletin, January 2014

⁶⁴ EU Oil Bulletin, January 2014

⁶⁵ Revenue Commissioners Headline Results, 2012,2013

⁶⁶ Revenue Commissioners Headline Results, 2012,2013

⁶⁷ Revenue Commissioners Headline Results, 2012,2013

⁶⁸ Revenue Press Releases, 2013

⁶⁹ Oireachtas Written Answers – Fuel Rebate Scheme, November 2013

⁷⁰ Revenue Commissioners Headline Results

⁷¹ Revenue Commissioners, Press & Media office, by e-mail on 21 February 2014.

⁷² Department of Health, Tobacco Free Ireland

⁷³ Pre-Budget Submission 2014, Joint Committee on Finance, Public Expenditure and Reform

⁷⁴ Joint Committee on Health and Children: Public Hearings on the Public Health Bill 2013

⁷⁵ Joint Committee on Health and Children: Public Hearings on the Public Health (Standardised Packaging of Tobacco) Bill 2013, 23 January 2014

⁷⁶ Houses of the Oireachtas, 2013, “Black Market: Discussion with National Federation of Retail Newsagents (Continued)”, 13 March.

⁷⁷ UN Comtrade

⁷⁸ Cracking Counterfeit, 2010, Pfizer

⁷⁹ Revenue Commissioners Headline Results 2012

⁸⁰ CSO, Goods Exports and Imports, December 2012, December 2013

⁸¹ Oliver Mangan, 2014, “Data points to economy on strong growth path”, 18 March, Irish Examiner. Available at: www.irishexaminer.com

⁸² UN Comtrade, 542 Medicaments, 2013

⁸³ Irish Examiner, 2013, “Purchasing drugs - High prices fuel risky online trade”, 17 September, Irish Examiner. Available at: www.irishexaminer.com

⁸⁴ IMB, 2013 Press release: “IMB, Customs and Gardaí in global INTERPOL operation targeting counterfeit and illegal medicines”, 27 June

⁸⁵ Irish Medicines Board, Annual Report 2012

⁸⁶ EFPIA, The pharmaceutical industry in figures, 2012

⁸⁷ Irish Examiner, 2013, “Purchasing drugs - High prices fuel risky online trade”, 17 September, Irish Examiner. Available at: www.irishexaminer.com

⁸⁸ Pfizer, Counterfeiting & Importation, Available at: www.pfizer.com/products/counterfeit_and_importation/counterfeit_importation#4

⁸⁹ BSA, Global Software Piracy

⁹⁰ Grant Thornton estimates, 2013

⁹¹ EMI (plaintiff) v UPC (defendant) – October 2010, Irish High court.

⁹² European Communities Trade Mark Association, EMI v UPC

⁹³ Louise McBride, 2014, “Sony sues UPC over music piracy move”, 16 February, Independent.ie. Available at: www.independent.ie

⁹⁴ Department of Jobs, Enterprise and Innovation, 2013, Press release: “Term of Protection for Musicians’ copyright extended from 50 to 70 years – Minister Sherlock”, 5 November

⁹⁵ Grant Thornton estimates, 2014

⁹⁶ Mar Carolan, 2014, “Legal action to stop UPC users downloading illegally”, 10 February, The Irish Times. Available at: www.irishtimes.com

⁹⁷ Gordon Deegan, 2013, “Losses double at music arm of Sony”, 4 December, Irish Examiner. Available at: www.irishexaminer.com



© 2014 Grant Thornton Ireland. All rights reserved.

Member of Grant Thornton International Limited (GTIL)

Authorised by Chartered Accountants Ireland ("CAI") to carry on investment business.