Devon & Cornwall Police

Produced in Partnership with:

Safer Devon, Safer Cornwall, Safer Plymouth and Safer Communities Torbay

Serious and Organised Crime Local Profile

- Cyber Crime, Fraud and Counterfeit goods -

2017 Update

Executive Summary

Authorising Officer: **T/ACC Jim Colwell**

Author: **Strategic Analysis Team**

Performance & Analysis Department

With additional input from key stakeholders across the Peninsula

This Executive Summary can be shared with individuals or organisations working to help tackle the problems of Cyber Crime, Fraud or Counterfeit Goods. It is not to be shared with members of the general public or the press/media. Please contact the authors at **StrategicAnalysisTeam@devonandcornwall.pnn.police.uk** if you have any queries.

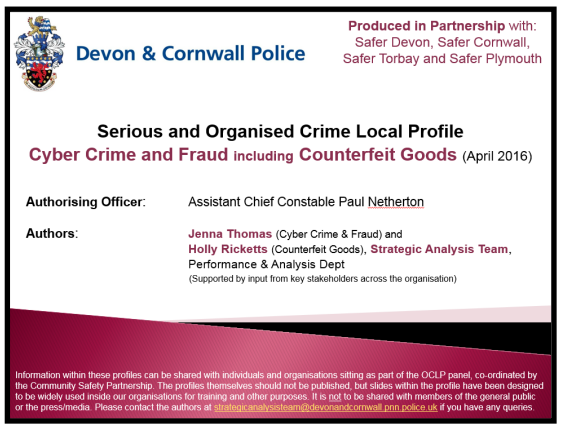
Introduction

In November 2014, the Home Office published guidance on their expectation that every Police force in England and Wales would lead the production of an annual **Serious and Organised Crime Local Profile** in collaboration with **local multi-agency partnerships**. The aims of the local profile are to:

- Develop a common understanding among local partners of the threats, vulnerabilities and risks relating to serious and organised crime;
- Provide information on which to base local programmes and action plans;
- Support the mainstreaming of serious and organised crime activity into day-to-day policing, local government and partnership work; and
- Allow a targeted and proportionate use of resources.

The profile was expected to address the Serious and Organised Crime topics of: Modern Slavery, Human Trafficking, Child Sexual Abuse and Exploitation, Cyber Crime, Serious Fraud, Counterfeit Goods, Organised Acquisitive Crime, Trafficking of Drugs, Trafficking of Firearms and Organised Immigration Crime.

Devon and Cornwall Police took this request seriously and decided, in consultation with partners, to produce a series of **thematic** local profiles, that would provide sufficient information and detail to achieve the above aims. The first profile to cover **Cyber Crime, Fraud and Counterfeit Goods** was written in 2015/16 and published in April 2016.


Devon & Cornwall Police

Produced in Partnership with: Safer Devon, Safer Cornwall, Safer Torbay and Safer Plymouth

Serious and Organised Crime Local Profile
Cyber Crime and Fraud including Counterfeit Goods (April 2016)

Authorising Officer: Assistant Chief Constable Paul Netherton

Authors: **Jenna Thomas** (Cyber Crime & Fraud) and **Holly Ricketts** (Counterfeit Goods), **Strategic Analysis Team**, Performance & Analysis Dept
(Supported by input from key stakeholders across the organisation)

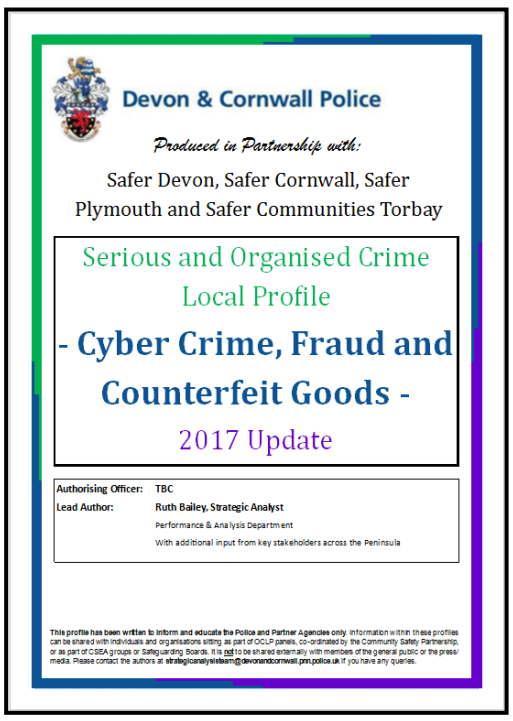
Information within these profiles can be shared with individuals and organisations sitting as part of the OCLP panel, co-ordinated by the Community Safety Partnership. The profiles themselves should not be published, but slides within the profile have been designed to be widely used inside our organisations for training and other purposes. It is not to be shared with members of the general public or the press/media. Please contact the authors at strategicanalysisteam@devonandcornwall.pnn.police.uk if you have any queries.

This first profile provided detailed **definitions** and **explanations** of the different types of cyber crime and fraud. If readers of the 2017 Update are unfamiliar with any of the terms used, then they should refer back to the 2016 document for further explanation.

The first profile covered **cyber enabled crime** as well as cyber dependent crime. It identified that while most crime types can be cyber-enabled, the most serious impact of this is seen in the facilitation of **sexual offences**, and that this is of greatest concern when this impacts on **children** and **young people**. As this is a topic explored in some depth in the **Child Sexual Exploitation and Abuse SOCLP**, the decision was made to focus the 2017 Update on **cyber dependent** crime alone.

The first profile also contained many **case studies** demonstrating the impact of cyber crime and fraud on businesses and **vulnerable people**, particularly the **elderly**.

The 2017 Update provides a fresh analysis of Action Fraud data to examine whether there has been any change in the **key demographics** being affected by the different types of cyber crime and fraud in Devon and Cornwall. It also provides a greater focus on the impact of these crime types on **businesses** by breaking down the data down into crimes affecting individuals versus crimes affecting businesses.


Devon & Cornwall Police

Produced in Partnership with:

Safer Devon, Safer Cornwall, Safer Plymouth and Safer Communities Torbay

Serious and Organised Crime Local Profile

- Cyber Crime, Fraud and Counterfeit Goods -

2017 Update

Authorising Officer: TBC
Lead Author: Ruth Bailey, Strategic Analyst
Performance & Analysis Department
With additional input from key stakeholders across the Peninsula

This profile has been written to inform and educate the Police and Partner Agencies only. Information within these profiles can be shared with individuals and organisations sitting as part of OCLP panels, co-ordinated by the Community Safety Partnership, or as part of CSEA groups or Safeguarding Boards. It is not to be shared externally with members of the general public or the press/media. Please contact the authors at **strategicanalysisteam@devonandcornwall.pnn.police.uk** if you have any queries.

The **key messages** are very similar to the first profile: there are different crime types that affect three different audiences (younger people, older people and businesses), therefore **awareness-raising** needs to be **targeted** accordingly. **Large sums of money** are being lost across the two counties, which can have a devastating impact on the business or individual concerned.

However, these crimes are **preventable**. Throughout the document, relevant **resources** are highlighted where appropriate **advice**, **guidance** and **support** can be accessed. **All of our partners** can help the Police to **prevent** cyber crimes and frauds from occurring, by finding **new** and **innovative ways** of ensuring that these resources are accessed and used by the relevant audiences.

As a starting point, **Devon and Cornwall Police's own website** has a page with resources and advice on online safety and fraud for individuals and businesses, with links to further resources: **https://www.devon-cornwall.police.uk/advice/your-internet-safety/**

Finally, there are a number of other ways in which **partner agencies** can support Devon and Cornwall Police in tackling cyber crime and fraud:

- Have an **identified cyber/fraud lead** who can represent the agency at a **strategic** level;
- Participate in an agreed single process for the **collection** and **sharing** of **intelligence**;
- Work together to **safeguard potential victims** and to give them the **information** and **skills** they need to better **protect** themselves;
- Frontline staff who regularly engage with vulnerable people can **raise awareness** with them about how frauds work, how they draw people in and the risks of engaging in this, as well as what they should do if they are approached in this way, i.e. **who** to **report** to and **how**.

SECTION 1: NATIONAL UPDATES AND REPORTS

Headlines from the National Cyber Security Strategy 2016-21 and the NCA's Cyber Crime Assessment 2016

The **scale** and **impact** of technological change is **accelerating**. While this is beneficial for society, it offers more opportunities to those who seek to compromise our systems and data. **Malicious cyber activity knows no international boundaries**. Cyber criminals are seeking higher value payouts while terrorists and their sympathisers are conducting low-level attacks. This poses challenges for the UK's collective response to cyber crime. Cyber criminals targeting the UK include **international serious organised crime groups** as well as smaller-scale **domestic criminals** and **hacktivists**. Much of the serious cyber crime continues to be perpetrated by **financially motivated**, Russian-language organised crime groups in Eastern Europe, but threats are growing from South Asia and West Africa as well as from within the UK itself. It is often difficult for the UK and international law enforcement agencies to prosecute key individuals when they are located in jurisdictions with limited, or no, extradition arrangements.

As an increasingly **computer-literate generation** engages in **extremism**, there may be a greater volume of low-sophistication disruptive activity. The potential will increase for a number of skilled extremist **lone actors** to emerge, or **terrorist groups** may seek to enlist an **established insider**.

Examples of Major Cyber Dependent Attacks

Talk Talk were breached in October 2015, putting the data of 157,000 customers at risk. This cost Talk Talk an estimated £60m and the loss of 95,000 customers, as well as a drop in their share price. This illustrates why businesses are often reluctant to report cyber attacks, due to the reputational damage they could suffer. In May 2017 the UK faced its largest cyber attack to date, when a global ransomware attack known as **WannaCry** hit the **NHS**. The NHS had been warned it was vulnerable to this type of attack but had not taken the necessary steps to protect themselves.

Focus on Business

All businesses hold data or provide services and this comes with a **responsibility** to safeguard their assets and protect their services. **Data breaches** are among the most common cyber crimes committed against businesses. Many organisations continue to use **vulnerable systems**, with **older software** which can be exploited by attackers. While cyber awareness is improving in the UK, it only takes one private individual to become infected and they in turn can then pass the infection on to businesses and other individuals.

Employees may **accidentally** cause harm through inadvertently clicking on a phishing email or downloading unsafe content from the internet. They can also become a **malicious insider**: a trusted employee of an organisation, with access to critical systems or data, who can use their access to steal, damage or delete data or systems. Organisations need to be aware of the threat from disaffected employees, fraud in the workplace and industrial espionage.

Directors of businesses should challenge their business management teams to go **beyond compliance** with minimum cyber security standards to ensure that rapidly evolving cyber security and resilience challenges are addressed and the threat to the UK is reduced.

Under-reporting continues to obscure the full impact of cyber crime on the UK. Directors of businesses have an important role in addressing this under-reporting. The NCA has urged businesses to report when they are victims of cyber crime and to share more intelligence, both with law enforcement and each other.

The new **General Data Protection Regulations** (GDPR) which are being introduced in 2018 will increase the responsibility on organisations to protect their data, and will introduce an obligation for companies to report any breaches of personal data held.

Crime Survey for England and Wales

New questions were added to the survey from October 2015 to incorporate fraud and cyber crime. It has been estimated that there are **5.6 million incidents** a year, but only **one in five victims** said they had reported the crime. Of the victims, 62% said they had lost money or goods as a result, but 43% had received a reimbursement. Victims of fraud are different to most other types of crime: they are likely to be older (45-54 most common), more affluent and in a managerial or professional occupation. Experian estimates that **£190 billion** is lost each year in the UK to fraud.

National Fraud Intelligence Bureau

Action Fraud have seen an **increase** in reports of fraud, particularly in the reporting of cyber-dependent offences. They found that 59% of frauds were committed against businesses. Losses reported totalled **£2.2 billion**, with a mean average loss per report of £7,400. The most common fraud type was 'cheque, plastic card and online bank accounts' and the most common cyber-dependent crime was 'malware infection reports'.

Note: full references/links for all of the documents summarised on this page are available in the full OCLP document.

SECTION 2: PENINSULA OVERVIEW OF THE DATA

Offences Against Businesses

In 2016-17 there were **74** cyber dependent crimes reported which affected businesses. **Hacking** offences were most common. The greatest financial loss was reported from **'hacking of social media and email'** offences. There was **427** cyber-enabled frauds reported and **187** more traditional frauds, most commonly **'retail fraud'**. Engagement with businesses is needed to encourage more reporting, as without a full understanding of the problem it is difficult for law enforcement to find effective responses to the problem. There are resources available designed to help businesses protect themselves from cyber crime and fraud.

Offences Against Individuals

In 2016-17 there were **500** cyber dependent crimes reported which affected individuals. Most commonly reported were **'computer virus/ malware/spyware'** offences, followed by **'hacking of social media and email**'. Older people were more likely to report the former and younger people the latter, so this indicates how prevention messages could be targeted.

There were **4,817** cyber-enabled frauds reported, with **'computer software service fraud'** the most common (reported by older people), and with **'online shopping and auctions'** causing the most reported losses (reported by younger people). There are a number of other types of fraud which are more likely to be experienced by younger or older victims, so again different prevention messages are needed for these different age groups.

There were **291** traditional frauds reported, with **'ticket fraud'** being the most common - this affects younger people more than older people. Older people were more likely to report being victims of **'door to door sales and bogus tradesmen'**.

Comparison of CSP Areas

There were small differences in the types of crime reported in greater/lesser proportions within the four CSP areas. Where these differences exist it is most likely due to the different **age demographics** in the four areas. Where there is a slightly greater proportion of older residents, they are more likely to be reporting the frauds/cyber crimes which affect the elderly more; and conversely where there is a slightly younger population they are more likely to report the fraud/cyber crimes affecting younger people.

Counterfeit Goods

Police recorded fraud is very low volume. There were **330** crimes recorded in 2016-17 that were classified as 'forgeries'. The most common of these was **'Other Forgery'**, of which 84% related to **'pass as genuine a thing knowing it was a counterfeit of a currency note / protected coin'**. Fake £20 and £50 notes were being passed over, most commonly in shops, cafes or bars, to buy a very low value item and take the genuine change. The Bank of England provides detailed advice and guidance for recognising counterfeit currency.

There were also very low volumes of **intelligence** around counterfeit goods. Counterfeit **tobacco** was most commonly mentioned. There were small numbers of references to counterfeit aftershave/perfume, clothes, shoes and handbags, DVDs, alcohol and money.

The National Banking Protocol

The **Financial Fraud Action UK** are leading a nationwide initiative referred to as The Banking Protocol: a crime prevention initiative delivered in partnership with financial institutions, law enforcement and Trading Standards designed to identify victims in branch who are in the process of completing a face-to-face financial transaction; this may be a withdrawal, transfer or loan application, which is suspected to be linked to 'rogue trader' type offences or frauds involving an element of social engineering such as romance frauds, investment frauds or courier fraud.

In the first four months of operation in Devon and Cornwall, **£820,000** of financial fraud was thwarted. Nationally the Protocol has stopped more than **£9 million** of potential fraud in a year.

Cyber Network for Reporting, Advice and Guidance

There are resources available at all levels to help with the problem of cyber crime. At the **national level**, the **National Cyber Security Centre** was set up to protect our critical services, **Action Fraud** is available for reporting and advice, and **Get Safe Online** are a leading source of advice on online safety.

At a **regional level**, the **Regional Cyber Crime Unit** are a small team of specialist cyber crime investigators who provide support to local Forces for more serious cyber-related attacks. The **South-West Cyber Security Cluster** is a not-for-profit collaboration raising cyber security awareness and best practice in the South West. It exists to raise the profile of cyber security issues and help the region's businesses and organisations take steps to counter the threats.

At a **local level**, Devon and Cornwall police have a **Digital Capabilities Unit** as part of the Serious and Organised Crime branch. It has responsibility for the investigation of complex and serious internet related crimes. Within this team, a new role has recently been introduced: a **Cyber Protect Officer**. They work with all the different functions described above and use their knowledge to proactively engage with businesses to help raise awareness and deliver prevention advice.

SECTION 3: LOCAL UPDATES

Devon and Torbay

Devon, Somerset & Torbay Trading Standards (DSTTS) have been taking the lead in responding to the first iteration of the Cyber Crime, Fraud and Counterfeit Goods SOCLP on behalf of Safer Devon Partnership. They have attended and held events for consumers and community groups to highlight cyber crime as a means of fraud. They have appointed an officer to be responsible for advice and warnings through social media. They are working with the **Adult Safeguarding Boards** to help them support those with care needs to avoid financial advice and they are developing a website resource for carers.

They have pursued **13 prosecutions** in a year, including a man selling counterfeit tobacco, a rogue trader conning the elderly, a fraudulent builder and a carpet cleaner found guilty of fraud. They have identified an issue with online selling platforms enabling individuals to import goods from overseas and sell them through the internet direct to the consumer, without them ever seeing/touching the goods sold - this makes it harder to intercept.

They have continued to be successful in identifying and stopping **rogue traders** who prey on the elderly and vulnerable. They have also continued to work with victims of **postal scams** and **lotteries**.

Plymouth

The findings of the previous SOCLP were incorporated into the **Plymouth Trading Standard's Action Plan**. They have provided more training for staff relating to frauds and scams, and the team now has an accredited **Financial Investigator** and two accredited **Counter Fraud specialists**. They have worked with victims of fraud and believe that for those who have been visited twice, the success rate is around 30%, in preventing them from losing further money, and for those who have received extensive support, the success rate is around 90%. The problem is the volume of fraud victims who would benefit from a visit, but Trading Standards are now working with Police to achieve this.

A **Scams conference** was held at the Plymouth Guildhall to raise awareness with partners about how the vulnerable can become victims of scams. They have also presented to a wide range of agencies, including Plymouth Community Homes, sheltered housing wardens and PCC staff so that they can identify and refer potential victims.

They have been monitoring Plymouth traders selling **illegal goods on Facebook** and sent warnings to those selling counterfeit goods. Six warrants were executed and counterfeit goods seized. They have worked with **HMRC** on a large-scale regional operation to target illicit tobacco. They also undertake regular checks at car boot sales and markets.

They had a successful prosecution of an eBay seller of counterfeit and unsafe cosmetics. A man was selling a fake lipstick which had over 300 times the legal amount of lead in it.

Cornwall

Cornwall's Trading Standards have continued with 'business as usual' as they felt their existing priorities and plans already reflected the concerns of the first SOCLP. **Trading Standards Volunteers** have been recruited to conduct at home interventions with suspected victims of mass-marketing scams. They aim to intervene with at least 120 suspected victims per year. Such interventions might require multiple visits, to earn the trust of the victim and to wean them off what can become an addiction. Where possible, support is sought from family, friends or community groups.

A **joint operation** with the Police was successful at stopping itinerant sellers of counterfeit goods at a tourist hot-spot on Perranporth beach. Fake clothing and handbags were being openly sold by street traders, as well as boots, perfumes, sunglasses, speakers, headphones and sportswear.

Cornwall Council's Corporate Fraud Team has engaged in partnership with **Cornwall Housing Ltd** to investigate instances of **Tenancy Fraud**. Since August 2014 they have recovered 70 properties, successfully prosecuting seven individuals for tenancy fraud related offences, including fraudulent "Right to Buy" applications. They also investigate instances of **Council Tax Support** and **Single Person Discount Fraud.** The Council also has a **Forensic Services team** who monitor and investigate cyber crime, focusing on internet misuse, computer misuse and investigation. The team aims to raise awareness of fraud, bribery and corruption across the Council and its partners so that everyone is aware of the risk of fraud and their responsibility towards managing it.

SUMMARY AND RECOMMENDATIONS

Since the production of the first Cyber Crime, Fraud and Counterfeit Goods profile in 2016, it has been identified by Community Safety Partnerships that these topics are **less of a priority** to local areas than other Serious and Organised Crime topics such as Child Sexual Exploitation and Abuse, and Modern Slavery, which have an easy to identify impact on **vulnerable people**. As such, much of the local activity that has taken place in relation to fraud has been conducted by **Trading Standards**, as part of their day-to-day work on frauds affecting the **elderly**. However, this leaves some **large gaps**, such as frauds affecting **younger people**, **businesses** and **cyber dependent** crimes. Tackling this problem cannot be Trading Standards alone, but it also does not require a large investment of extra resources. Fraud and cyber crimes are **extremely preventable** - it just requires people to be **educated** to recognise scams and to take appropriate steps to **protect** their computers and devices. The advice is already **freely available** as demonstrated by the **links to resources** provided throughout this document.

Recommendations for Community Safety Partnerships:

- Review your actions plans and communication strategies etc. for other areas and consider how **cyber dependent** and **fraud prevention messages** could be **incorporated** into those existing plans/strategies.
- Liaise with Devon and Cornwall's **Cyber Protect Officer** to understand what activity she is undertaking in your area and where the gaps are that you could assist in delivering.
- Build/develop working relationships with your local **Trading Standards Officers** to ensure you really understand which aspects of these problems they are tackling and which they are not, and to understand how you might support/build on some of their initiatives etc.
- Consider: Are you confident that **other than Trading Standards**, are the organisations working with older people in your area **sufficiently trained** in identifying the indicators of/vulnerability to scams?
- Consider: The **demographics** of people vulnerable to higher levels of economic fraud are likely to be more affluent middle- to late-middle aged people, living in more rural areas (very different to other traditional crime types) - can you use this information to **target** communications/ awareness raising?
- Consider: How can you raise awareness with **young adults** about the types of cyber/fraud they are most vulnerable to?
- Consider: How could you encourage **practitioners** and **communities** to **register** for the **free** Devon and Cornwall Police **alert system**, which includes updates on frauds/scams at https://alerts.dc.police.uk/ ?

There is national guidance around cyber security, such as the National Cyber Crime Strategy 2016-21.

- Review the guidance and ensure recommendations are being implemented locally.

Cornwall Trading Standards have identified that there is an issue with police call centre staff and officers not always responding in the most appropriate way to calls regarding **doorstep trading fraud** or **mass marketing scams** etc. They sometimes refer to Action Fraud instead of **notifying Trading Standards** who can respond much more quickly.

Recommendations for the Police:

- It is suggested that a half-hour's briefing/explanation from an **operational level Trading Standards officer** should be incorporated into all Police **call-centre training**. This would provide call-handlers with a basic knowledge of the triggers for when to refer to Trading Standards – an A5 size poster, suitable for display within Police call-centres that explains these triggers is available from Cornwall Trading Standards.
- Similarly, an opportunity to input into **initial police training** would have a positive effect on officers knowing from day one how they should deal with doorstep crime and who they can call for assistance.

We would like partners to support us in the fight against cyber crime and fraud by encouraging their frontline staff who encounter vulnerable people to provide them with advice and guidance on how to protect themselves against these crimes. However, it may not be realistic for all frontline staff to receive full training in these areas and to have the knowledge necessary to provide this guidance.

Recommendations for the Police:

- Consideration should be given to how we can best support partners in being able to provide this guidance to potential victims. For example, **Corporate Communications** could consider whether it's viable to produce a short series of leaflets (one for older people, one for younger people and one for businesses) which partners could distribute, which gives clear advice and guidance on how to **recognise** fraud/ cyber crime and **who** to **report** to under different circumstances.

Please note:

The full OCLP document is available in the **Publication Library** on Devon & Cornwall Police's intranet site at the following address:

http://intranet/PerformancePortal/By%20subject%20area/Forms/Modified%20DESC.aspx under **Strategic Publications**

If you do not have access to our intranet, please email your request for the document to:

StrategicAnalysisTeam@devonandcornwall.pnn.police.uk