Foreword
T/Commander David Clark

According to the Crime Survey of England & Wales, fraud was the most commonly experienced offence in 2016. Her Majesty's Inspector of Policing, Sir Tom Winsor, referred to this demand on policing as a "tsunami of online fraud" in his State of Policing report.

There is a huge gap between the figures quoted in the crime survey and the half a million reports which go through the National Fraud and Cyber Reporting Centre every year. This under reporting leaves fraud and cyber victims at a significant disadvantage because resources are allocated against a partial picture of the threat and impact.

In the past year we extended our service for reporting of live cyber incidents to provide 24/7 coverage. Through this service, we provided advice to over 160 companies on how to minimise the impact and allocated their reports to the most appropriate law enforcement agency for action. We also used this information to help individuals protect themselves against future fraud associated with theft of their personal data.

In 2017 we will be continuing to improve our service to make it easier for single and bulk reporting to the National Fraud and Cyber Reporting Centre. A new analytics system will improve our ability to link crimes and criminals and share real time information on offenders and victims with law enforcement partners. The new system will be far more advanced, dynamic and able to meet the needs of victims, forces and the private sector.

We continue to work with police forces investigating serious and complex fraud on their behalf and helping them to improve their fraud capabilities. From training by our Economic Crime Academy on the fraud investigation model, to processes for identification and management of vulnerable victims. We provide nationally co-ordinated crime prevention advice and are developing a toolkit of best practice.

We are working with the Government to identify legislative and policy changes to reform fraud prevention and the criminal justice system's ability to respond. We are working with the Cabinet Office to professionalise public sector fraud investigation.

With 80 percent of fraud and cyber crime preventable, behavioural change and designing out systematic weaknesses remains paramount. Education of the risks and how they can be prevented is the responsibility of not just policing, but individuals, government and business. The relevance and timeliness of our own crime prevention advice has resulted in a 64 percent increase in digital engagement on last year.

With the materialisation of the internet of things, driverless cars and smart cities, criminals will continue to seek low risk, high reward opportunities to commit fraud and cyber crime. We will continue to work with our partners in 2017 to transform our collective ability to meet these challenges.
ECD in Numbers

The estimated cost of fraud to UK economy is £193bn

£360m saved last year through telephone, email, websites and bank account disruption requests.

£650m in financial losses.

We are currently investigating over 700 fraud cases involving more than £650m in financial losses.

For every £1 spent we prevent £44 in fraud losses.

80% of fraud could be prevented through simple protection steps.

Fraud crimes 3.6 million
Cyber crimes 2.0 million
Other crimes covered by this survey numbered 6.2 million

Source: The Annual Fraud Indicator 2016
National to local roles and responsibilities agreed for fraud investigation

Through work with the National Police Chiefs’ Council and a sustained programme of engagement with police forces (we have visited and peer reviewed 19 forces in the last year), we are providing practical advice on managing and servicing fraud demand. An important first step in formalising coordination of national law enforcement activity was agreement of a grid setting out roles and responsibilities of the National Crime Agency, Serious Fraud Office, City of London Police, regional organised crime units and local police forces. This was agreed on behalf of policing by the National Police Chiefs’ Council on 25 January 2017.

Nationally coordinated, locally delivered crime prevention

Our Economic and Cyber Crime Prevention Centre continues to develop fraud and cyber prevention advice based on the latest crime trends. This advice is disseminated to local communities through a network of local and regional crime prevention officers and through online and offline media channels. We are also the national lead for post-incident cyber messaging following high profile attacks on businesses including Tesco, Wonga, Friend Finder and Camelot.

We are co-ordinating a series of regional events aimed specifically at educating UK businesses facing an escalation from the threat, risk and impact of cyber crime. The first of these events took place in the City in November 2016 and was attended by over 150 small and medium sized enterprises. We worked with other law enforcement agencies and industry partners to deliver this cyber security and resilience roadshow which took an inside-out approach to reinforce the message that organisations cannot only rely on technology alone to safeguard them from data breaches. From April 2017, a regional roadshow is planned for each month and will follow a very similar format.
The National Fraud and Cyber Reporting Centre received several reports from businesses that had been sent online extortion demands threatening a cyber attack. Following consultation with partner agencies, we issued a same day alert to warn businesses of the threat and what action to take if they were contacted. The alert was shared on the National Crime Agency’s Facebook page which has 64,000 followers. We emailed the alert to our business contacts and the Cross-Sector Safety & Security Communications platform sent the alert to its 14 million members. Within one afternoon of issuing the tweet there were 199 posts on Twitter about the article generating 680,222 impressions. Police forces, Trading Standards, individuals and small and medium sized enterprises also shared our tweet. The tweet was ranked number 7 in the UK for Government tweets by MeasuredVoice.

**Do You Really Know?**

In January 2016, we launched a campaign on common threats relating to fraud and cyber crime. These included press releases every three weeks on threats associated with public wi-fi, email ‘spoofing’, dating fraud, money mules and holiday fraud. The campaign reached over 10 million people across Twitter and Facebook alone. Third party advocates helped to extend the reach of the campaign on social media and there were over 1,487 different supporters of the campaign on Twitter including police, Trading Standards, local authorities and key partners.

**Real time prevention advice**

Over 14 million business contacts were sent the alert

680,222 Twitter impressions

6,839 Facebook impressions
Nationally Coordinated, Local Policing

Sharing good practice
Through our national police working groups, we have identified examples of good practice from our own force and others that can be adapted to meet local force profiles. We are encouraging forces to implement these locally. This includes the Fraud Investigation Model, disruption tactics, Operation Signature (created by Sussex Police) and the Banking Protocol (developed by the Metropolitan Police Service in collaboration with the retail banks). Operation Signature protects the elderly from repeat fraud victimisation and the Banking Protocol, seeks to protect vulnerable and elderly people who are being defrauded from withdrawing large cash sums from banks with a police response to capture offenders. Our own Economic Crime Victim Care Unit is being promoted by Her Majesty’s Inspectorate of Constabulary as a best practice model in victim care. In the coming year, we will be augmenting our good practice toolkit with a resourcing model based upon three pillars (specialist fraud capability, mainstream fraud capability and support capabilities), and national tasking.

Up-skilling the public and private sectors
Our Economic Crime Academy has continued to provide a range of learning programmes to meet the demand from across law enforcement and the public and private sectors to up-skill their staff. This includes providing fraud investigative training to Greater Manchester Police, West Yorkshire Police and Metropolitan Police as well as counter fraud training to the Competition & Markets Authority, KPMG and Grant Thornton. We also provided training on the disclosure process to the Financial Conduct Authority and training on bribery and corruption to the National Crime Agency. We continue to work with international law enforcement and have delivered anti-money laundering training for Horn of Africa countries and training in fraud management and anti-bribery to Dubai Police.

In October, delegates from 11 countries working for Standard Chartered Bank completed the Economic Crime Academy’s core investigative techniques programme designed to counter financial crime and equip delegates with the skills, knowledge and ability to combat a crime threat causing significant harm and loss across the globe.
Economic Crime Academy

1,027 trained delegates from private, public and not for trade sectors

97% of delegates satisfied with the content and delivery of courses

4,093 delegate days delivered

www.academy.cityoflondon.police.uk

Proud to deliver an exceptional policing service
Victims remain at the heart of our service. We provide advice to prevent individuals and businesses from becoming victims, and in some instances repeat victims. We share intelligence, enabling banks and other organisations to freeze accounts, take down websites and disconnect phone lines linked to fraudulent activity. We are seizing criminal assets and returning this money to their victims.

**24/7 live cyber incident reporting and triage service**

Through funding from the National Cyber Security Programme, the National Fraud and Cyber Reporting Centre launched a 24/7 live cyber incident service in October 2016. This ensures that victims receive support from the law enforcement agency (e.g. National Cyber Crime Unit, National Cyber Security Centre, regional or local policing units) that is best placed to manage or investigate the incident. It also ensures victims have access to advice on how to minimise the effects of cyber attacks through fast-time action to mitigate further losses in trade, personal information and reputation. This service has helped to reduce demand on 999 services.

**Making it easier to bulk report**

In response to the demand for an easier method of submitting multiple crime reports, we created the bulk reporting tool. This allows businesses and law enforcement to submit up to 200 crime reports at a time. This will increase to 1,000 reports at a time when the new ICT platform for the National Fraud and Cyber reporting Centre is launched in 2017. Since the launch of the bulk reporting tool in late 2015 there has been a 70 percent increase in the number of reports received by users.

**Understanding the threat and targeting prevention advice across different communities**

We produce an assessment for each force outlining both the local and national threat from fraud and cyber crime equating to 258 bespoke profiles per annum. The aim of these products is to provide an outline of the frauds and cyber crimes impacting on the local area, information on victims and methods used, so forces can target crime prevention activities more effectively.

We also produce victimology reports which assess which public group or businesses are vulnerable to specific types of frauds or criminal methodologies. These profiles are shared with government partners and law enforcement agencies who use the information to inform their victim support and crime prevention strategies.

The Fraud Defence Test (www.frauddefencetest.com) was launched in January 2017. It helps to inform the public of their vulnerability to fraud and signposts them to prevention advice. The test was funded through the Police Innovation Fund, developed in partnership with the Home Office and is supported by the Financial Fraud Action UK ‘Take 5’ campaign. It is available for all partner agencies to use with their local communities.
Supporting victims of economic crime

The Economic Crime Victim Care Unit operates in partnership with the Metropolitan Police Service. It has continued to provide tailored support for London victims of economic crime and prevent repeat victimisation. This has resulted in a number of positive interventions. For example, this year eight vulnerable victims who had received support from the unit were able to identify subsequent attempts to defraud them. They used the information we provided to recognise the fraud and sought further advice resulting in the frauds being prevented.

1,683 intelligence products and alerts disseminated to industry partners and the public.

£1.4m Assets recovered and returned to 558 victims.

8/10 victims reported they felt better able to protect themselves after receiving advice from ECVCU.
Innovation in Policing

Criminals are increasingly using new ways to steal personal and financial information and are constantly adapting to get ahead of security measures put in place by law enforcement and industry. Innovation is essential to efficient and effective delivery of policing in the digital age.

Improving digital evidence analysis and disclosure

The proliferation of digital devices has resulted in significant increases in the amount of information that needs to be reviewed and disclosed for evidential purposes as part of an investigation. While the criminal justice system tries to limit the length of complex trials to three months, the time taken to bring a fraud case to trial often takes years. This year, we initiated a project funded by the Police Innovation Fund, to test how new technology can improve the effectiveness and speed of digital evidence analysis and disclosure in complex economic crime investigations. The project is being trialled on a significant pension liberation fraud and aims to provide significant time savings for investigating officers, improve the integrity of audit trails, lower the risk of undermining the prosecution case due to failures in data management, and to provide improved access to intelligence held on digital devices.

Hoax website set up to change consumer behaviour

This year, in partnership with Getsafeonline and the Society of Ticket Agents and Retailers, we launched a national ticket fraud campaign designed to show the public just how easy it is to fall victim to ticket fraud. In the last three years more than 21,000 people have reported falling victim to ticket fraudsters and the majority of these reports concern the secondary ticket market and other secondary sources such as social media or independent ticket websites.

During a series of Facebook flash sales, over 1,500 people tried to purchase music tickets from a fake ticket sales website we created called ‘Surfed Arts’. Adverts were targeted at fans of Adele, Ed Sheeran, Iron Maiden, Coldplay and Bruno Mars. Those who clicked through to the Surfed Arts website were immediately told that they were not able to purchase the sold out event tickets and advised on how to protect themselves from falling victim to real ticket fraudsters in the future. The purpose of the hoax was to try and directly affect consumers’ online behaviour and make them think twice before buying tickets from illegitimate secondary ticket sites.
Operation Creative responsible for 64 percent drop in UK advertising on illegal sites

The ground-breaking Operation Creative which disrupts illegal streaming sites has seen major success. Operation Creative set up an Infringing Website List in 2013 to discourage advertising on these sites. A report by the Digital Citizens Alliance estimated that in 2013 piracy websites generated $227 million from advertising. Research conducted by a global data company in 2016 showed that there had been a 64 percent decrease in advertising from the UK’s top ad spending companies on copyright infringing websites over 12 months.

Leading international approaches to combating online intellectual property crime

In early March, we gave evidence on the innovative tactics we have developed to combat intellectual property crime committed on the internet in a Danish Parliamentary Public Hearing.

To coincide with World Intellectual Property Day, we also showcased the work undertaken by our Police Intellectual Property Crime Unit to Chinese officials. This involved a tour of China with the UK Intellectual Property Office to share our approach to tackling online intellectual property crime with government, law enforcement agencies, academia and business.

A first of a kind guide for investigation of fraud and economic crime

This guide forms one of a series of manuals for law enforcement on how to investigate a range of crime types. At the centre of the book is the Fraud Investigation Model, an effective framework encompassing multi-agency working, recovery of evidence and victim management. It also includes a range of useful features designed to demystify fraud terminology and provide accessible operational guidance. Over 100 of our people contributed their knowledge and experience to write this guide.
Working With Partners

We work with partners across the public, private and third sectors. By working together, we strengthen the UK’s defences and make it harder for offenders to reach and harm our communities. Our partners support us in the fight against fraud through funding, resources and expertise.

On behalf of policing we work with government to identify policy and legislative measures that improve our capability to reduce fraud and cyber crime.

A cross-border public private partnership tackling card not present (CNP) fraud

The two year European Commission funded (90 percent) Project Skynet concluded in December 2016. The project aimed to provide a more in depth understanding of e-crime in the payments sector and how law enforcement needed to evolve to have the greatest impact in tackling this fraud. It was led by our Dedicated Card and Payment Crime Unit (DCPCU) and included staff exchanges between the UK banking industry and DCPCU. This partnership working extended to European law enforcement and DCPCU staff visited colleagues in Hungary, Finland, Romania, Austria and Iceland. These secondments have resulted in international co-operation, through intelligence sharing and joint investigations against crime groups involved in CNP fraud. DCPCU has actively engaged with retailers/merchants impacted to develop intelligence sharing and improve law enforcement capability to investigate.

This partnership is the first of its kind and the number of retailers/merchants sharing fraud data, along with the banking industry through the Skynet intelligence hub has grown across a number of sectors including clothing, electrical, gaming and telecommunications.

In June and October 2016, DCPCU initiated two weeks of action with the retail industry. Intelligence supplied by retailers/merchants and the banking industry was analysed by the Skynet intelligence hub and developed into operational packages targeting CNP fraudsters. This two week operational activity included participation from other UK police forces and supported a co-ordinated European law enforcement response led by Europol. The pan EU weeks of action will continue to be supported throughout 2017.

Through Project Skynet, DCPCU investigated 42 organised crime groups resulting in 79 arrests. 27 defendants were charged and seven convicted. Project Skynet provided the platform for collaborative partnership working across industry and the development of a united international law enforcement response to CNP fraud.

10th Annual International Intellectual Property Crime conference

In September we co-hosted Interpol’s 10th annual International Law Enforcement IP Crime Conference. The conference is designed to build stronger partnerships and develop best practice amongst a variety of public and private organisations from around the globe. It also highlighted a decade of success and explored more effective ways to tackle the criminal networks behind trafficking illicit goods and counterfeiting. This included emerging crime trends and technologies, transnational organised crime, internet-based IP crime and effective training strategies. The conference was attended by 500 delegates from more than 80 countries.
Exploring criminal pathways

Working with the Universities of Cardiff, Portsmouth and Warwick, we undertook research into pathways and profiles of fraud offenders. The project aimed to establish any common pathways into and out of fraud offending and to suggest interventions to improve the evidence base of what works in fraud policing. Data was collected through a number of measures, including a national survey of policing and detailed interviews with fraud offenders in locations across the country. The findings from the survey identified there were a substantial group of fraud offenders with previous convictions, highlighting the importance of robust vetting procedures by organisations where there are opportunities for a fraud to be committed. The overwhelming motivation to commit fraud was identified as being to secure money for a materialistic lifestyle, and according to occupational codings, all sections of society seem to be engaged in fraud. Significantly, one of the biggest impacts on fraudsters was the negative media coverage of them and their crimes and the impact this had on their relationships with family and friends.
Motor manufacturers assist in analysis of suspected counterfeit airbags

Motor industry safety experts are assisting our Police Intellectual Property Crime Unit in the detailed analysis of suspected counterfeit airbags and components seized during a raid in 2016. At the time of the arrest, we alerted 680 people who were believed to have purchased counterfeit and potentially dangerous airbags and airbag covers on eBay. A number of those purchases were made by a wide range of small and medium sized businesses and individuals. Every individual was advised to make contact with their local dealership immediately so their vehicle could receive the necessary checks to ensure its safety.

Our investigation was launched in January 2016, following a referral from Honda Motor Europe, who identified counterfeit airbags were being sold on eBay. We have since taken action to suspend the vendor’s sales sites by working closely with Nominet, the UK’s central registry for all .uk web domains.

Collaboration and cooperation with the Financial Conduct Authority

We have signed a new memorandum of understanding with the FCA which provides a framework for collaboration including secondments, exchanging best practice and sharing information and intelligence. Our first secondment into the FCA is focussed on in 2016 intelligence processes for whistleblowing.

Professionalising national and international counter fraud capabilities

Through our Economic Crime Academy we are working with the Cabinet Office to introduce a Counter Fraud Profession for central government departments and advised on Counter Bribery and Corruption Standards. We are also working with the College of Policing to develop and embed fraud training into the new police career pathway.

Working with the National Crime Agency we undertook a review of the investigation and management of criminal and terrorist financing in Pakistan. We produced a training needs analysis to improve effectiveness of law enforcement and federal agencies in Pakistan in relation to the complex and challenging area of counter terrorist financing and anti-money laundering legislation.
Pursuing Criminals

We continue to bring offenders to justice. With the geographical complexity of international criminal gangs and money trails, our work reaches across national and international borders. We are conducting numerous joint operations involving police and judicial authorities around the world. Here are just a few successful investigations from the past year.

Two City traders sentenced in complex £141 million fraud

Two traders were sentenced for conspiring to defraud a Russian bank of more than £141 million in a series of complex frauds in January 2017. The investigation involved three sets of court actions in the case – our criminal action, a criminal action in Switzerland and a civil action in the UK. The case was investigated in our capacity as the national lead force for fraud and the officer in charge was commended for his diligence and expertise by the Judge on “this long, complex and challenging case”.

The first part of the fraud was carried out between 2010 and 2011 when work on behalf of a Russian-owned company Otkritie Securities Ltd was manipulated into paying approximately US$25 million under false impression. Further frauds were subsequently committed by trading financial products called Argentinean warrants and fooling their employer into purchasing the warrants from other conspirators for four times their value. The traders then pocketed the difference and transferred their gains to bank accounts out of the UK. By manipulating the trade in financial products in this way the defendants stood to gain in excess of a further US$150 million.

Men behind a boiler room operation that ripped off 193 victims, defrauding them of £7.5 million jailed for 35 and a half years in October 2016

Francis Byrne set up a boiler room in 2008, which was initially named ‘Paramount Land’ but the name changed several times during its three-year existence. The defendants subsequently set up numerous umbrella companies in order to move money around. Fellow directors, Sam Exall and Michael Foran assisted with the running of the operation while Max Jeffreys was a prolific salesman making calls to victims. Paramount Land bought agricultural land for low prices and then sold it for far more than it could ever be worth by making false guarantees as to the future value. They also sold land that they did not own. They then convinced investors that the only way they could get their money back was to invest more money so their portfolio could be bought out by a nameless conglomerate that never existed. Banking material demonstrated the defendants made large sums of money from the fraud totalling £1.6 million. Through the asset recovery procedure, we will now recover as much of their ill-gotten gains as possible, to compensate victims for some of their losses and ensure these criminals do not benefit from their offending. The investigation into accomplices also continues.
**Successful outcomes**

**Fraudster jailed for five years and four months for running a counterfeiting factory from his home**

Officers from the Dedicated Card and Payment Crime Unit found significant items which could be used in the counterfeiting and production of cheques and credit cards in May 2016. Items included counterfeit and stolen cheques and blank documents for vehicle registrations and immigration certificates. Documents and pictures thought to be related were also found on a computer following analysis, as well as paraphernalia associated with counterfeiting was also found. The total value of the fraud was estimated to be £1.7 million. The fraudster was further charged with conspiracy to possess or manufacture articles to defraud.

**Insurance fraud prosecution becomes case law**

The Insurance Fraud Enforcement Department has had a number of firsts this year. This includes the first bribery convictions for providing customer data relating to ‘crash for cash’, and guilty verdicts for six solicitors and accomplices who orchestrated an insurance fraud sham. An IFED prosecution also formed part of case law as judges were asked to determine if the friends of Britain’s most prolific ghost broker, Danyal Buckharee, were money laundering. They opened accounts and then handed over control of the accounts to Buckharee. The judges determined that they were guilty of money laundering.
Pursuing Criminals

Wanted fraudsters arrested through the Joint Fraud Taskforce

The Joint Fraud Taskforce is a collaboration between law enforcement, the Home Office and banks to reduce fraud. In July 2016 we published a list of ten wanted fraudsters which received significant media coverage.

One suspect who had his image circulated was arrested by Metropolitan Police officers in September as he disembarked a flight from San Francisco. American authorities assisted in the deportation after he was identified by San Francisco Police.

A suspected serial ATM fraudster was arrested by officers in Kent in July as he attempted to leave the UK. This arrest came less than 48 hours after his image was circulated to national and international media as part of a widespread appeal to identify ten suspected fraudsters wanted for committing fraud worth £20 million.

Another criminal wanted by police for defrauding an elderly victim who was duped into paying close to £100,000 for bogus building work was arrested by Police Scotland in September. He was also wanted by officers from Greater Manchester Police and has since been recalled to prison. In 2011 he had received a six year prison sentence for committing a number of burglaries during which he targeted and gained access into homes of elderly victims dressed as a fake utility company member of staff.

A new wanted fraudsters campaign will commence in 2017.
Economic Crime Directorate

National Coordinator for Economic Crime
T/Commander David Clark
D.Clark@cityoflondon.pnn.police.uk

Head of Economic Crime Directorate
T/Detective Chief Superintendent Glenn Maleary
Glenn.Maleary@cityoflondon.pnn.police.uk

Funded Units
Operations
Economic Crime Academy
National Coordination Office

National Fraud and Cyber Reporting Centre
NFIB
Action Fraud
Strategic Delivery Unit

Annual Review 2016 - 17