Date: 22/06/2020
Version 1.2 – 20

CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

CITY OF LONDON POLICE

Police Intellectual Property Crime Unit

Operation Ashiko Suspension Policy

CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

1. Background

Criminal activity online has continued to evolve with technological advances and more simplistic ways to carry out day-to-day operations with automation, and instant transactions to goods and services occurred in seconds, without having to leave the comfort of your own home.

Enterprises began to see the benefits of transitioning sales activities online. No longer was it necessary to have a physical store paying millions of pounds worth of rent and employing staff to work on shop floors when they could be achieving the same productivity using automation.

Additionally, consumers were now able to access products which could never have been possible due to logistics, such as their current geolocations.

A buyer now had the opportunity to purchases goods anywhere in the world at the press of a button, and it would require no physical interaction. All that was needed was to type in the relevant e-commerce site, click on what you wanted, add it to a shopping cart and then complete the transaction using personal and financial data.

The seamless nature of this type of transaction led to the popularity of online shopping expanding dramatically. By 2021, over 93% of internet users will shop online in the United Kingdom, while a similar trend replicated globally.

However, as the popularity of online shopping continued to grow so did the attraction Organised Crime Groups (OCG's) to exploit this successful business structure and opportunists began to set up e-commerce platforms to commit fraudulent activities.

With technology progressing and the ease of setting up an online website ever-increasing, criminals were able to purchase domain names that purported to be a brand.

Criminals began cloning the original platform templates to provide an air of authenticity, and the only disparity was the substantial difference in the price of the product and the lack of "Contact Us" information displayed on the illicit website.

There were two fundamental reasons for this – firstly, by advertising the lowest price, criminals would offer counterfeit products a competitive value, in many cases up to 70% off the original amount. In turn, this made the website more likely to attract a consumer to carry out a purchase, where they believed they had the best deal possible.

Secondly, by removing all contact data and providing inadequate communication, it would mask the identity of the suspects.

A principal criminal objective is not to be identified or apprehended, and this was a perfect way to anonymise themselves. They also knew that most online shoppers

would not know to investigate further into their whereabouts if transactions failed to materialise.

For OCG's, the lucrative e-commerce business was immensely appealing with no face-to-face interaction. Sales would be carried out on the website itself and then harvested for other fraudulent purposes. It was an easy way fraudulently sell counterfeit goods online, steal data, and sell it to other crime groups for other criminal purposes.

In 2019, the Organisation for Economic Co-operation and Development (OECD) reported that illicit goods relating to counterfeiting and piracy accounted for 3.3% of world trade, reflecting the extent of this type of criminal activity and its impact on the global economy and money laundering.

The sale and distribution of counterfeit goods pose a significant challenge not only with intellectual property, with laundered funds attributed to the facilitation of other illicit activities including terrorism, narcotics and human trafficking.

2. Introduction

The Police Intellectual Property Crime Unit (PIPCU) is run by the City of London Police Economic Crime Directorate to combat criminality, with a focus on offences committed online.

Protecting the UK PLC interest is a crucial factor, mainly due to the emergence of cyber-enabled intellectual property crime, which strongly focuses on the sale and distribution of illicit counterfeit goods.

The PIPCU currently receives numerous reports of counterfeit websites from various sources, including enforcement agencies, such as Europol, Trading Standards and the National Fraud Intelligence Bureau, where customers have registered criminal complaints.

Additionally, the PIPCU also receives intelligence and evidence from individual brands requesting the assistance of the unit to disrupt and prevent the continuation of websites selling counterfeit products online.

Criminals now use the internet as part of their modus operandi, allowing OCG's to reach previously unattainable consumers.

With professionally designed, realistic-looking websites whose sole purpose is to fool victims into believing they are purchasing legitimate goods.

The domain(s) will accept payment for the product with or without fulfilling the actual order. Any items that do arrive are of significantly inferior quality.

To combat this emerging threat, the PIPCU created Operation Ashiko. This operation targets explicitly the sale and distribution of counterfeit websites with a focus on the .uk ccTLD.

3. Values

As part of the City of London Police, the PIPCU will continue to uphold and demonstrate the principle values of the force:

Integrity

Integrity to us means acting in accordance with the values of the organisation. It is about being trustworthy, reliable, and committed, and there is an expectation that staff have the confidence and support of their colleagues to challenge behaviour that falls below expected standards.

Our behaviour, actions and decisions will always support the public interest and those we work in partnership with. We value public trust and confidence in policing and to earn this we will be open to scrutiny and transparent in our actions. We will respond to well-founded criticism with a willingness to learn and change.

We will ensure that the public can have confidence in the integrity of the data used and published by us.

We will make sure that all crime is recorded ethically and in accordance with all current guidance.

Fairness

We are an organisation that believes in openness, honesty, and fairness. We believe in mutual trust and respect, and in valuing diversity in our role both as an employer and as a public service provider.

We will support equality by creating an environment that maximises everyone's talents in order to meet the needs of the organisation and those of the community we serve.

Professionalism

Professionalism is a quality that we value highly. We will investigate crime professionally and thoroughly, doing everything in our power to protect those at the greatest risk of harm.

We expect our staff to be dedicated to professional development, both for themselves and the people they are responsible for, and empowered to use discretion and common sense to make appropriate operational decisions.

Our professionalism ensures that we meet the needs and demands of our customers to deliver high quality, fast, effective, and efficient service

4. Core functions

Operation Ashiko provides a core function to protect the intellectual property rights of brands, rights holders and interested parties within the .uk country code top-level domain (ccTLD). Additionally, this aim is to create a safer environment for consumers to shop online without purchasing counterfeit, dangerous and illegitimate products online within the UK branded online marketplace.

Operation Ashiko facilitates prevention, detection, and **disruption** of criminal activity online.

To meet this objective, the following principles as part of the **Prevent**, **Pursue, Protect** and **Prepare** strategy:

- **Prevent** and protect the safety of the public
- **Prepare** and create a safer environment for consumers on the internet
- **Disrupting** online criminal activity
- **Prevent** any economic loss to members of the public
- **Protect** industries from organised crime
- **Prevent** economic loss to any firms/ stakeholders concerned in the criminal activity
- **Disrupting** the sale and distributing counterfeit goods online (suspension of websites)
- **Protect** the integrity of the .uk domain tree
- **Prevent** criminal activity by gathering intelligence to deter the continuation of crime
- **Pursue** any reasonable lines of enquiry that may lead to the apprehension of suspects and the prevention and detection of crime.

Protecting the UK PLC interest and industry is a crucial factor, primarily due to the emergence of cyber-enabled intellectual property crime, which strongly focuses on the sale and distribution of illicit counterfeit goods.

To achieve this the City of London Police and PIPCU work in line with .uk registry Nominet to assist the suspension of the domain names in question.

Nominet's primary role is to maintain the registry for the .uk, .wales and .cymru respectively.

Working closely with Nominet, the City of London Police has agreements in place to suspend illicit websites within the .uk namespace that breach the registries terms and conditions without the need of a Court Order.

This agreement is on the mutual understanding that PIPCU will investigate and carry out strict due diligence assessing counterfeit websites using .uk domain names for criminal activity.

If confirmed, the PIPCU will transmit a formal notice to Nominet requesting a domain suspension of twenty-four months.

5. Rationale for suspension & other considerations

The PIPCU uses two key elements to assist the suspension of domains used in a crime.

Criminal Activity:
The PIPCU undertakes responsibility for the prevention, investigation, detection, and prosecution of criminal offences, including the safeguarding against any threat to public security.

Should any domain be found committing unlawful activity contrary to United Kingdom legislation, the PIPCU will certify suspension.

Compromised domains and websites used for criminal purposes:
The PIPCU will also take action to suspend domains where we have reason to believe a domain has been compromised without the original owner's knowledge.

The suspension is solely carried out to protect the original domain owners and members of the public from detrimental reputational and financial harm both to themselves and/or their business.

In such cases, the PIPCU will look to carry out remedial action with the original domain owner so any compromise can be rectified, such as the removal of unauthorised Unique Resource Locators (URL's).

6. National Crime Reporting Standards (NCRS)

The overall majority of website domains suspended by the PIPCU concern organised crime that has been committed from abroad on the .uk domain tree.

In order to comply with Home Office National Crime Reporting Standards (NCRS), a crime report will not be completed for each website domain suspension, where it has been established criminal activity is being committed from outside the United Kingdom.

Any offences disclosed, that have been committed within the jurisdiction of the United Kingdom (U.K) will be recorded in line with Home Office National Reporting Crime Standards (NCRS) accordingly, should they meet the relevant criteria.

7. Suspension notices

A suspension notice will include the following information:

- Operation Title
- Domain registrar
- Suspension request date
- The grounds on which PIPCU is making the request
- Registrant point of contact information for the PIPCU
- The reason for the closure
- Authority agreed to suspend the website
- Manifest of domains requested for suspension.

The PIPCU will inform the Registrar that by allowing the domain name to resolve, they are facilitating serious crime.

The PIPCU, therefore, will request the Registrar to investigate these domain name(s) for breach of their terms and conditions and, if a violation is found, take steps to prevent the domain name(s) from being used for a minimum period of 24 months (or the expiry of the domain name(s) if sooner).

In the event that the Registrar fails to take action within 48 hours of receipt of this request, the PIPCU will request Nominet investigate these domain name(s) for breach of their terms and conditions and, if a violation is found, take steps to prevent the domain name(s) from being used for a minimum period of 24 months (or the expiry of the domain name(s) if sooner).

8. False registry and identity theft

To counteract identity theft, the PIPCU has established the following initial processes to disrupt these activities:

Should investigations identify and conclude that personal data has been misused to register a domain for criminal activity, the following steps will be considered:

Suspension of the domain name - The Registry Nominet, together with the Registrars, are provided with a notification informing them of the current criminal activities, with a request to suspend the domain name in accordance with their policies.

Notify the Registrar - Individual registrars are contacted to inform them of the abuse of registry (WHOIS) data to prevent any further websites being falsely registered.

Provide Crime Prevention Advice – Providing advice on how to protect them from purchasing counterfeit items online, cybercrime and fraud.

Confirming Infringements – If necessary, the PIPCU will contact brands, representatives and/or trade bodies are contacted to provide a statement confirming infringements on the illicit websites in question.

9. Authority

All domains submitted for suspension are authorised by the Detective Chief Inspector of the Police Intellectual Property Crime Unit (PIPCU) run by the City of London Police.

10. Right to challenge a suspension

Should a registrant believe that their website and associated domain has been reported for suspension in error, they should contact the PIPCU directly using the contact information provided on the suspension notice within the first 48 hours.

Email: opashiko@cityoflondon.pnn.police.uk
Address: Operation Ashiko - Police Intellectual Property Crime Unit, City of London Police, Prevention & Disruption, Economic Crime Directorate, Bishopsgate Police Station, PO BOX 36451, 182 Bishopsgate, London, EC2V 4WN
Telephone: (+44) 0207 164 8250

The PIPCU will then re-assess the domain in question and establish if there has been an anomaly.

Additionally, this will allow remedial action to take place, should it be necessary.

For confidentiality and data protection, the PIPCU will only respond to the named registrant or representative documented on the official WHOIS information.

Any challenge should include the following:

1) Operation reference
2) Name, address, contact email and telephone number
3) Proof of domain registration
4) Grounds of the challenge.

11. Complaints and appeals

Complaints are an important way for us to learn where we are falling short as a service and correct it as quickly as possible. Find out about our complaints process, how to make a complaint, how we deal with them and what you can do if you are not satisfied with the way your complaint was handled.

Should you wish to make a formal complaint regarding police conduct details can be found on the City of London Police website using the following link:

https://www.cityoflondon.police.uk/advice/advice-and-information/c/complaints/

12. Management of information, personal data, and privacy notice

The use and disclosure of personal data is governed in the United Kingdom by the Data Protection Act 2018 (the Act). Under the Act the Commissioner of Police for the City of London is registered as a data controller. In the rest of this privacy notice the Commissioner of Police for the City of London is referred to as we or us.

This privacy notice explains:

- how we collect, store, use, disclose, retain and destroy personal data through the website at cityoflondon.police.uk (those activities are also referred to as processing personal data);
- the steps we take to ensure personal data we process is protected properly; and
- the rights individuals have when we process their personal data.

We will treat information you provide to us in using this website treated in confidence and we will not disclose it to third parties unless we are required to do so by law, or as explained in this privacy notice.

What is personal data?

Personal data is any information we handle that relates to an identified or identifiable natural person. An 'identifiable natural person' is anyone who can be identified, directly or indirectly from information, including by reference to a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Our Contact Details and Data Protection Officer

Our Information Management Services Unit manages our data protection compliance. Our Data Protection Officer is the Director of Information.

We take our data protection responsibilities seriously. We take great care to ensure we process your personal data properly to maintain your trust and confidence. You can contact our Information Management Services Unit or our Data Protection Officer if you have any questions or concerns about how we process your personal data.

Post:
Information Management Services
Bishopsgate Police Station
182 Bishopsgate
London
EC2M 4NP

Telephone: 0207 601 2222
Email: dataprotection@cityoflondon.police.uk

Why do we process your personal data?

We have a legal duty to uphold the law, prevent crime, bring offenders to justice, and protect the public. To do this we process your personal information for carrying out a range of activities commonly known as the 'policing purpose'.

These include:

- preventing and detecting crime;
- apprehending and prosecuting offenders;
- protecting life and property;
- preserving order;
- maintaining law and order;
- assisting the public;
- safeguarding national security;
- defending civil proceedings; and
- fulfilling any other police duties or responsibilities arising under common or statute law.

We also process personal data for purposes in support of the policing purpose.

These include:

recruitment; administration of current and former employees, contractors, and volunteers; property and asset management; financial management; media relations management, complaints handling; research, including surveys; and provision of educational programmes and support.

Whose personal data do we process?

We process information relating to a range of individuals, including:

- victims of crime;
- witnesses to crime;
- people convicted of an offence;
- people suspected of committing an offence;
- complainants, correspondents and enquirers;
- advisors, consultants and other professional experts;
- suppliers;
- current and former employees, cadets, agents, temporary and casual workers, and volunteers;
- representatives of individuals in this list, such as parents, other relatives, guardians, and people with power of attorney.

What types of personal data do we process?

We may process personal data relating to or consisting of the following categories:

- personal details (such as name, address and biographical details);
- family, lifestyle and social circumstances;
- education and training details;
- racial or ethnic origin;
- political opinions;
- religious or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- offences (including alleged offences);
- criminal proceedings, outcomes and sentences;
- physical identifiers (including DNA, fingerprints and other genetic or biometric samples)
- sound and visual images (e.g. from body worn cameras or facial recognition software);
- financial details;
- goods or services provided;
- licences or permits held (e.g. driving licences or firearms certificates);
- criminal intelligence;
- information identifying user vulnerability, persistent targeting, and/or hate crime status;
- references to manual records or files;
- information relating to health and safety;
- complaint, incident, and accident details.

The types of personal data we process will vary depending on the purpose.

We aim to process the minimum amount of personal data necessary for the relevant purpose.

You should not assume that we hold personal data in all of the categories identified for every person whose personal data we process.

The categories identified may not be complete as occasionally we may gather personal data in other categories for the purposes described.

Where do we get the personal data we process?

We collect personal data from a variety of sources, including:

- individuals who visit the website and interact with it (including by filling in and submitting forms), and their relatives, guardians and other persons associated with them;
- businesses (including security companies, and other supplies of goods and services) and other private sector organisations working with the police in anti-crime strategies;
- voluntary sector organisations;
- local authorities, national and local government departments and agencies (including the Home Office, HM Revenue and Customs, and private safeguarding agencies);
- other law enforcement agencies and bodies (including international ones);
- partner agencies involved in crime and disorder strategies;
- legal representatives, prosecuting authorities, courts, and prisons;
- licensing authorities;
- approved organisations and people working with the police;
- ombudsmen and regulatory bodies (including the Independent Police Complaints Commission, and Her Majesty's Inspectorate of Constabulary);
- auditors;
- Police and Crime Commissioners;
- emergency services;
- current, past or prospective employers of individuals;
- healthcare, social and welfare advisers or practitioners;
- education, training establishments and examining bodies;
- business associates and other professional advisors;
- our employees, agents, and other temporary and casual works;
- persons making enquiries or complaints;
- financial organisations and advisors, and credit reference agencies;
- survey and research organisations;
- trade, employer associations; and professional bodies;
- the media; and
- our own CCTV systems and body worn cameras.

What is our lawful basis for processing personal data?

Where we process personal data for the policing purpose our legal basis for processing is that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.

Our functions and the official authority vested in us are set out, in the main, in the Police and Criminal Evidence Act 1984, the Police Act 1996, and the Police Reform Act 2002.

Where we process personal data relating to criminal convictions and offences, that processing is necessary for reasons of substantial public interest and involves the exercise of a function conferred on us by an enactment or rule of law.

We have an appropriate policy document (as required under the Act) for that processing.

Where we process personal data for purposes other than the policing purpose our legal basis for processing will vary depending on the circumstances. Ordinarily, the relevant legal basis is that the processing is:

- necessary for performing a contract;
- necessary to comply with a legal obligation (including employment law);
- in the public interest or for official purposes;
- in our legitimate interests (and those interests are not overridden by your interests or fundamental rights and freedoms);
- necessary to protect your vital interests;
- with your explicit consent (which you may withdraw at any time).

What security measures do we use when processing your personal data?

We take the security of all personal data under our control seriously. We comply with our legal obligations regarding security, relevant parts of the ISO27001 Information Security Standard, and where appropriate the College of Policing Authorised Professional Practice guidance on Information Assurance.

We ensure that appropriate policy, training, technical and procedural measures are in place, including audit and inspection, to protect our manual and electronic information systems from data loss and misuse.

We only permit access when there is a legitimate reason and under strict guidelines on what use may be made of any personal data contained within them.

We continuously manage and enhance our compliance with relevant standards and guidance to achieve adequate and up-to-date personal data security.

What disclosures do we make of your personal data?

We may disclose personal data to a wide variety of recipients in any part of the world (including outside of the United Kingdom and the European Economic Area), including to those from whom we originally obtain personal data. Recipients may include:

- law enforcement agencies;

- businesses (including security companies, and other supplies of goods and services) and other private sector organisations working with the police in anti-crime strategies;
- partner agencies working on crime reduction or safeguarding initiatives;
- agencies and other third parties concerned with the safeguarding of and investigation relating to international and domestic national security;
- local authorities, national and local government departments and agencies (including the Home Office, HM Revenue and Customs, the Serious Fraud Office, the Child Maintenance Service, the National Fraud Initiative, and private safeguarding agencies);
- Police and Crime Commissioners;
- legal representatives, prosecuting authorities, courts, prisons, and other partners in the criminal justice arena;
- victim support service providers;
- bodies or individuals working on our behalf;
- authorities involved in offender management;
- ombudsmen, auditors and regulatory authorities;
- other bodies or individuals where required under any legislation, rule of law, or court order;
- other bodies or individuals where necessary to prevent harm to individuals; the media.

We decide on disclosure case-by-case, disclosing only the personal information that is necessary and proportionate to a specific purpose and with appropriate controls and safeguards in place.

If we make disclosures outside of the United Kingdom and the European Economic Area to locations which do not have as extensive data protection laws we ensure that there are appropriate safeguards in place to certify that the personal data disclosed is adequately protected.

How long do we retain your personal data?

We keep your personal data for as long as necessary for the particular purpose or purposes for which we hold it.

If we place any of your personal data on the Police National Computer it will be retained, reviewed and deleted in accordance with agreed national retention periods, which are subject to periodic change.

We will retain records containing personal data relating to criminal investigations, intelligence, public protection, and custody in accordance with the College of Policing guidance on the Management of Police Information:

https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information

What are your rights over your personal data we process, and how can you exercise them?

Under the Act you have a number of rights that you can exercise in relation to personal data we process about you. You do not have to pay to exercise your rights (other than a reasonable fee if a request for access is clearly unfounded or excessive but we agree to fulfil it anyway).

We sometimes need to request specific information from you to help us confirm your identity and ensure your authority to exercise the rights.

Right of Access:
You can request access to the personal data we hold about you free of charge. Normally we will provide it within one month of receipt of your request unless an exemption applies. You can request access to the personal data we hold about you using the contact details in this privacy notice.

Right to be Informed:
You are entitled to be told how we obtain your personal information and how we use, retain, and store it, and who we share it with. This privacy notice gives you that information, as well as telling you what your rights are under the relevant laws.

Right to Rectification:
If we hold personal data about you that is inaccurate or incomplete you have the right to ask us to correct it. You can ask us to correct your personal data using the contact details in this privacy notice. We will reply to you within one month unless the request is complex.

Right to Request Erasure:
Under certain circumstances you have the right to ask us to delete your personal data to prevent its continued processing where there is no justification for us to retain it.

The circumstances most likely to apply are:

- where holding your personal data is no longer necessary in relation to the purpose for which we originally collected and processed it;
- where you withdraw your consent to us holding your personal data if we are relying on your consent to hold it;
- where we are relying on legitimate interests as our basis for processing and you have objected and there is no overriding reason for us to continue processing.

The right of erasure does not apply if we are processing your personal data:

- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for the establishment, exercise or defence of legal claims;
- to exercise the right of freedom of expression and information;

- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to make it impossible to carry out or seriously impair that processing.

If you want to ask us to delete your personal data you can do so using the contact details in this privacy notice. We will respond to you within one month unless the request is complex.

Right to Restrict Processing:
Under certain circumstances you have the right to ask us to restrict the processing of your personal data.

This may be in cases where:

- you are contesting the accuracy your personal data while we are verifying the accuracy;
- your information has been unlawfully processed and you oppose its erasure and have requested a restriction instead;
- where we no longer require your personal data but you need it to establish, exercise or defend a legal claim and do not want us to delete it.

You can ask us to restrict processing of your personal data using the contact details in this privacy notice.

Right to Data Portability:
You have the right to obtain and reuse your personal information for your own purposes, transferring it from one environment to another. This right only applies to personal data provided by an individual, where the processing is based on their consent or for the performance of a contract and when that processing is carried out by automated means. If you wish to discuss this right, you can do so using the contact details in this privacy notice.

Right to Object:
You have the right to object to:

- processing based on legitimate interests or performance of a task in the public interest and or exercise of official authority;
- processing of your information for scientific and historical research and statistics;
- direct marketing.

Any objection must be on grounds relating to your particular situation.

If you want to exercise your right to object you can do so using the contact details in this privacy notice.

Rights related to automated decision making and profiling:

You have the right not to be subject to a decision when it is based on solely automated processing (including profiling) and which produces a legal effect or similar significant effect on you. This right does not apply if the decision is authorised by law, is necessary for entering into or performance of a contract, or is based on your consent. We are unlikely to carry out automated decision making because our processes involve some type of human interaction and decision-making. Profiling is any form of automated processing of personal data intended to evaluate certain personal aspects about you to predict things about you such as your behaviour, interests, movements or performance at work. We do not currently carry out automated profiling. If you have any questions about automated decision-making or automated profiling you can raise them using the contact details in this privacy notice.

How you can complain:

The Information Commissioner's Office (ICO) regulates the processing of personal data. You can complain to the ICO if you are unhappy with how we have processed your personal data.

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113
Website: www.ico.org.uk/concerns