Home Office

Voluntary guidance for businesses on procedures for supplying specialist printing equipment and materials

This guidance is designed to support businesses in protecting themselves from becoming victims of payment fraud and reducing their risks of inadvertently supplying specialist printing equipment and materials for use in criminal conduct.

Background

Identity fraud costs UK adults an estimated £3.3 billion each year[1]. False documents[2] are a key enabler of this crime, allowing organised criminals to escape monitoring mechanisms and maintain the profits from their illegal activity. Criminals require specialist printing equipment and materials to make false documents such as passports, driving licences and credit cards. While the possession and use of such false documents is illegal, there is currently no specific offence of supplying such equipment for use in criminal conduct and it is difficult to prosecute those who knowingly supply equipment for these purposes. The Specialist Printing Equipment and Materials (Offences) Bill seeks to close this legal loophole by creating a new criminal offence of knowingly supplying specialist printing equipment and materials to those who intend to use them for criminal conduct. This would act as a deterrent to such supply, making it more difficult for criminals to obtain the equipment and materials necessary to create false documents, and so will reduce incidences of identity crime.

The Metropolitan Police Service's Project Genesius was set up in 2007 and operates jointly with the specialist printing industry to prevent the supply of such equipment and materials for use in criminal conduct. The Project agreed a voluntary Code of Conduct for suppliers of specialist printing equipment and materials.

Building on the voluntary Code of Conduct, the Home Office and Project Genesius have developed this guidance to businesses on procedures they can voluntarily adopt to reduce the risk of supplying equipment for use in criminal conduct. There is evidence that adopting these procedures helps protect businesses from becoming victims of payment fraud, as criminals who exhibit suspicious behaviours when attempting to obtain specialist printing equipment and materials are also more likely to evade payment or make purchases with stolen credit cards. Responses to the public consultation showed that businesses had found that applying these procedures significantly reduced their incidence of becoming victims of payment fraud, mostly as a result of adopting the procedures from the Code of Conduct used by Project Genesius.

Home Office, September 2013

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205612/Annual_Fraud_Indicator_report_v12_WEB.pdf

[2] False documents comprise of forged, counterfeit and fraudulently obtained genuine documents.

Suggested procedures

1) Keep records of transactions for at least six years.

This allows businesses to track customers, compare new enquiries with past orders, and is in line with normal good business practice of keeping records for six years, to cover businesses for the full limitation period on breach of contract claims. In cases of suspected criminal activity, these records may be useful for the police in their inquiries. The records should include details of:

- the equipment purchased, including the make, model and all serial numbers;
- the price paid;
- verified customer's contact details; and
- all order forms, invoices and delivery notes relating to the order.

2) Profile customers by checking for any fraud indicators.

It is recommended that businesses check for at least 5 of these, but this will depend on the nature of the business, its size and the equipment or materials it supplies. The checks outlined below should enable a business to satisfy itself that a potential customer's intended use of the product is for a legitimate purpose, and what that intended purpose is.

Potential indicators of fraud include:

- The potential customer's address does not tally with the telephone number given.
- The potential customer does not supply a company name/headed paper. This may indicate that they are unable to provide verification that they are a legitimate representative of the company.
- The potential customer is unwilling to supply a contact address.
- The potential customer supplies an address that is a serviced office.
- The potential customer supplies an address that is a residential address.
- The potential customer supplies an address which is actually a house for sale. This can be checked through websites such as zoopla.com and rightmove.co.uk. However, not being listed on one of these websites does not confirm that a house is NOT for sale.
- The potential customer gives details that do not match the website of the business that they purport to represent.
- The potential customer supplies a telephone number that does not work when you ring it back.
- The potential customer is only able to supply a mobile telephone number.
- The potential customer supplies a telephone number beginning with '070' - this is a premium rate platform telephone number and is known to be favoured by criminals.
- The request from the potential customer comes from an email domain that does not match that of the real company.
- The potential customer purports to be from a company that does not have a valid credit reference or fails an identity verification check. This check can be carried out via a credit reference agency which would charge per enquiry or on an annual contract. This would be usual when setting up a new customer account or potential new dealer, especially where a credit account is requested or anticipated.
- The potential customer purports to be from a company that is not registered with Companies House, or when checking with Companies House the details do not match, for example, the age of the company and directors' names are not correct, the registered office address and registered company number given are not correct, or the company is not trading. The name and home address of at least one director could also be verified,

as well as trade and bank references. Where the potential customer is an individual, the home address and trading address could be verified. Basic information can be obtained free of charge through the WebCheck service: http://wck2.companieshouse.gov.uk//wcframe?name=moreCompanyInfo

- The potential customer asks to pay a large amount in cash, and if so, is this normal behaviour?
- The potential customer asks to collect the equipment personally, and if so, is this normal behaviour?
- The potential customer wants business equipment/supplies delivered to a non-business address.
- The potential customer asks for the equipment urgently, without good reason. This may indicate that the buyer is attempting to buy the equipment or materials using a compromised credit card with a limited lifespan.
- The potential customer does not ask for receipts/invoices.
- The potential customer does not want a contract for repairs/servicing, and is this normal behaviour?
- The potential customer does not attempt to negotiate over the price, and is this normal behaviour?
- Where the order relates to custom stamps, the design is suspicious, e.g. because it purports to be an official stamp from a Government Agency or Embassy.

As these are potential indicators only, any suspicions raised may not always be related to intended criminal use. Further advice on these fraud indicators is available from the Metropolitan Police Service's Project Genesius at: **projectgenesius@met.pnn.police.uk**

3) Report any suspicions from the above checks to the police.

You should do this before any sale takes place, or at the earliest point at which you have reason to become suspicious. This can be done through the local police force, either via the local police station or by calling 101. Alternatively, companies can contact Project Genesius at **projectgenesius@met.pnn.police.uk.**

4) Dispose of obsolete equipment responsibly and securely.

This means dismantling/disabling equipment and materials before disposing of it, in a way that it cannot be used to manufacture false documents. It is also recommended that businesses keep a record of the make, model and serial numbers of equipment being disposed of.

In order to be effective, business' procedures applying any of the above should be clear, practical, accessible, easily and effectively applied by its employees, with appropriate oversight and regularly reviewed. A business should ensure that its procedures in line with the above are embedded and understood throughout the organisation through internal and external communication, including training, which is proportionate to the risks it faces.

Any examples in this guidance of particular types of conduct are provided for illustrative purposes only and do not constitute exhaustive lists of relevant conduct.

Businesses supplying specialist printing equipment and materials should adopt a risk-based approach to managing the risk of supply of equipment and materials for use in criminal conduct. A risk-based approach will serve to focus the effort where it is needed and will have most impact, and this recognises that the procedures followed and threats faced by businesses in this industry may vary depending on size, turnover and equipment or materials supplied. The language used in this guidance reflects its non-prescriptive nature.

Examples:

Preventing payment fraud

1. In the public consultation run by the Home Office, 89% of Project Genesius members reported having been victims of payment fraud before they had adopted the checks recommended in this guidance. Only 28% reported being the victim of payment fraud again after adopting the checks. This shows that by adopting the checks, 61% effectively protected themselves from becoming the victims of subsequent payment fraud.

Stopping criminal behaviour

2. A member of Project Genesius was approached via their online shop with a request to purchase a single, bespoke identity card. The card requested was a secure telecoms card which could have allowed access to sensitive Government buildings, including those used by the Security Services. The customer had provided his home address instead of that of a business premises, which, when checked, was found to be near to sensitive Government buildings. This raised the suspicions of the Genesius member, who passed the information on to Project Genesius. Project Genesius did further research into the customer and found that he had been purchasing a selection of chemicals that, when combined, could be used to make Improvised Explosive Devices (IEDs). Police attended the customer's home address and caught him in the act of making IEDs. The street was evacuated by police and further explosives were found in the garage of the property. The customer was arrested, charged with explosive offences, and subsequently sentenced to two years and six months in prison.

3. A member of Project Genesius was approached for consumables for a specialist printer and repair of the printer. The customer had asked for the printer to be sent by courier to a given address. On checking the delivery address given, it was found to be a virtual office. When the engineer examined the specialist printer, he noticed that the serial number had been filed off it. When he looked at the printer ribbon inside, he found that it had been used to print cards that looked like driving licences. Details of the customer were sent to Project Genesius and were found to match details already on their database. The police traced the individual concerned to another property, where a full document factory was found to be in operation, producing counterfeit passports from scratch. The three principals were arrested and subsequently received prison sentences totalling 11 years and nine months.