Using financial information

This page is from APP, the official source of professional practice for policing.

First published 23 October 2013 Updated 27 July 2023
Written by College of Policing
15 mins read

There are many forms of financial information and these can be related to more than one aspect of a person's life. It can be difficult for investigators to know what type of financial information is useful or needed for their investigation. Investigators are, therefore, advised to contact their financial investigation unit (FIU) to discuss the financial planning element of their case and to find out what assistance they can offer.

The following subsections list the sources and types of financial information, and how they can be accessed.

Accessing financial information

Financial investigators (FIs) have direct access to banking institutions and information held in suspicious activity reports (SARs). They also routinely collect financial information through production orders and requests for disclosure of personal information.

Tips for requesting financial information

When tasking FIs to collect financial information, officers should be specific about what they wish to achieve. Investigators should be able to tell the FIU:

- what information they already hold
- what information they would like to obtain
- why that information is required
- what they intend to do with the information obtained
- how the information is to be disseminated
- exactly how they would like the FI to help

Investigators should also refer to their local force policy.

Information held by financial institutions

Information held by financial institutions can show the lifestyle of a person and whether they are living beyond their means. This includes information from:

- bank accounts
- credit and debit slips
- supplementary information such as managers' written notes
- identity documents used to open accounts (banks must be satisfied that the person opening an account is who they say they are)
- account opening forms
- bank statements
- direct debits
- standing orders
- deposits
- withdrawals
- safety deposit boxes
- copies of ledgers of business
- credit and charge card accounts
- credit and charge card statements
- pensions
- insurance schemes
- mortgages
- loan applications
- other previously unidentified accounts

These can inform an investigator of associations and payments to and from other people, the lifestyle of the individual (their wealth, the turnover in their account), their spend patterns (for example, where they went on holiday, their travel, meals, hobbies and other interests) and any financial problems.

Automatic teller machines (ATMs)

ATMs can provide mini statements and information on balance enquiries. Although these enquiries do not appear on a bank statement, this information can be used to pinpoint the geographical

location of a subject or establish routine. If such information is relevant to the investigation, an FI should be consulted.

Tasking financial investigators

FIs can obtain information about a person's basic financial status from money laundering reporting officers (MLROs) that work in the regulated sector, see **the ELMER database** (suspicious activity reports).

This information is channelled through the financial intelligence gateway. It is, however, only information/intelligence and cannot be used in evidence.

Any information gathered at this point has to be followed up with the relevant authority, such as a production order, to allow its use in the evidential chain.

Requesting information

Information must be legally obtained to be used in evidence. This may be through use of the Data Protection Act 1998 (DPA) or a relevant production order or search warrant obtained under **Proceeds of Crime Act 2002 (POCA)**, the **Police and Criminal Evidence Act 1984 (PACE)** or the **Drug Trafficking Act 1994**.

The authority to be used is determined by the type of investigation, for example, a production order under POCA would be used in a confiscation or money laundering investigation. The source of the information (for example, bank or credit reference agency) would also have a bearing on the type of order used.

Production orders

Investigators can use production orders and search and seizure warrants to make material available under:

- **POCA section 345 and 352** (applying to confiscation, money laundering and civil recovery investigations only)
- **DTA sections 55 and 56**
- **PACE section 9** and **Schedule 1**, although production orders under PACE cannot be served on a government body

Investigators may use production orders to access information held by the regulated sector or service providers. The process involves the appropriate officer (a constable, customs officer or an accredited financial investigator) gathering information in support of an application for a production order and making an application to court for a production order.

An authority from an officer of inspector rank or above should be obtained for all applications. The material requested can include any information held by the institution.

In addition to production orders, investigators have powers under POCA to obtain account monitoring orders and customer information orders.

For further information on accessing information held by public sector providers, for example, HMRC or DWP, please contact your local Economic Crime Unit or Financial Investigation Unit.

Account monitoring orders

Account monitoring orders (**POCA section 370**) are a powerful but underused investigative tool that should be considered for use in all proactive investigations. These orders can provide live intelligence on a suspect's bank accounts for up to ninety days at any one time. They require a financial institution to submit reports on the suspect's financial activities as directed by the police. Compliance is labour-intensive for the regulated sector.

Account monitoring orders require the authorisation of an officer of at least the rank of inspector. They can be obtained in relation to confiscation or money laundering proceedings at any stage.

The complex nature of this process and the risk of inappropriate usage (with institutional as well as personal consequences) mean that only FIs should apply for account monitoring orders.

Customer information orders

Customer information orders (**POCA section 363**) are used in proceeds of crime investigations (for example, a money laundering investigation) to determine if an unidentified account exists.

They are time-consuming for financial institutions to comply with and require the authorisation of a superintendent or above. Application for these orders should be as a last resort and proportionate to the matters under investigation. There must also be intelligence and a rational reason to believe

that an unidentified account exists. The financial institution usually requires as much detail as possible, at least the suspect's name and postcode, in order to be able to supply the information.

Customer information defined by section POCA 364 as 'information whether the person holds, or has held, an account or accounts at the financial institution'. If an account is held, customer information includes the following:

- relevant account number(s)
- the person's full name
- the person's date of birth
- their most recent address and any previous addresses
- the date(s) of account opening and/or closing
- evidence of identity (obtained by the financial institution for the purpose of money laundering regulations)
- any personal details of joint account holders (name, date of birth, addresses)
- account numbers of any other accounts to which the individual is a signatory and details of the account holders

Customer information on companies also exists, including details such as VAT numbers, registered offices and personal details of individual account signatories.

The complexity of applying for a customer information order means that, in practice, only FIs make an application.

Disclosure of personal data

To access information held by other agencies and companies, an investigator must use a request for disclosure of personal data under the **Data Protection Act 1998**. The power to disclose information exists where disclosure is required for:

- the prevention or detection of crime (section 29)
- the apprehension or prosecution of offenders (section 29)
- the purpose of, or in connection with any legal proceedings (section 35), or
- reasons of national security (section 28) to the extent that non-disclosure of the requested information would be likely to prejudice one or more of those same purposes

In cases where it may not be appropriate to claim the exemption, a court order for the disclosure may be sought.

Any officer may make a request, although it must be authorised by an officer of the rank of inspector or above. A request must:

- contain details of the criminal investigation to which it relates and must seek specific details, namely current address, assets, investment accounts or details of income
- be necessary for one of the purposes set out in **paragraph 2 of Article 8 of Schedule 1** to the Human Rights Act 1998
- be proportionate to the purpose for which the information is requested

Legal professional privilege (LPP)

All information that a solicitor discovers about a client in the course of a retainer is confidential, whether that information is also privileged is a separate legal issue.

For further information see:

- **Law Society website**
- **Crown Prosecution Service website**

Finding information

Table showing where financial information is held, listed by service.

Merchant service providers	• Applications for services. • Account information on a person's address, date of birth, bank account number and sort code, telephone numbers, marital status, credit cards held and expenditure.

Retailers	• Information from points of sale. • Loyalty cards providing information on lifestyle, location and time of expenditure.
Other service providers - for example, gambling establishments, social clubs and associations, gyms.	• Customer or client information such as addresses, telephone numbers, the person's associates, routines and their location.
Solicitors	• Conveyancing files. • Other related matters. Material recovered from solicitors or accountants can be the subject of legal professional privilege.
Accountants	• Reports and other full notes. • Accountancy records. Material recovered from solicitors or accountants can be the subject of legal professional privilege.

Merchant service providers

Merchant service providers, such as mobile phone companies, utility companies or companies that deal with merchants' claims for reimbursement of credit or debit card payments by customers, hold a variety of information which is of potential use to an investigation. This can include a person's location at a certain time or details of any electronic payments.

Investigators can apply for production orders to obtain information from the financial institution that administers the chip and PIN or swipe systems (such as Link).

Government departments and agencies

The following government agencies and departments hold financial information that may be useful to a police investigation.

Department for Work and Pensions (DWP)

The DWP holds information on benefits such as income support, jobseekers allowance and incapacity benefit.

His Majesty's Revenue and Customs (HMRC)

HMRC provides information on:

- tax status (note: this requires the authority of an inspector)
- child benefit
- employment
- third-party information on individuals which includes interest-bearing accounts, ISAs, and other items on which tax is due

A two-way gateway allows exchange of information between the police and HMRC. Investigators should consult their own force policy on accessing information from HMRC.

Local authorities (LAs)

LAs provide information on:

- housing benefit
- council tax
- the amount of time a person has spent at an address and who else lives there

Information is available to the police from LA fraud departments by using requests for intelligence under section 29 of the DPA. Production orders under the appropriate Act must be obtained if intelligence from an LA is required in evidential form. Local memorandums of understanding and informal arrangements may also exist.

Investigators should contact the FIU and/or FIB for assistance.

Land Registry

The Land Registry can provide information on:

- property owned, solicitors used and any associates
- value of property
- mortgages relevant to property

Investigators are advised to contact the FIU for access to Land Registry information.

Companies House

Companies House holds information relating to any business owned by the suspect including:

- current and previous directorships
- registered business addresses and home addresses
- accountant’s details
- bank details
- original signed documentation

Investigators are advised to contact the force intelligence unit for access to information held by Companies House.

Credit reference agencies

Credit reference agencies provide data access systems that can be used in criminal investigations, allowing authorised officers to obtain information on an individual’s financial relationships and status, companies, company directors and secretaries. This information can assist in the prevention or detection of crime and apprehension and prosecution of offenders, or the assessment or collection of any tax or duty.

Credit reference agencies in the UK include:

- Experian
- Equifax
- Callcredit (mostly based in the UK and primarily concerned with high street credit ratings)

These agencies provide information including:

- financial history and credit status

- repossessions
- payment history
- account number
- names of financial associates
- address checking
- electoral roll data
- insurance information
- cars, purchases (hire purchase information)
- properties
- county court judgments
- telephone numbers and a list of all credit searches that have been carried out on a person, including identity verifications
- relevant information on fraud linked to a particular address, and details on repossessions
- information on business proprietors (including cross-referenced business registrations using address and telephone number data, and directors' names)
- information relating to companies, company directors, company secretaries, trading addresses, and credit summaries

Dun and Bradstreet also hold information on companies including:

- company directors
- multiple company directorships
- a director's former earnings
- company secretaries
- trading addresses
- company files
- names of disqualified directors

The credit industry fraud avoidance system (CIFAS) is the UK's fraud prevention service. CIFAS keeps information on multiple credit applications that are suspected of being fraudulent. They also maintain other fraud databases.

Accessing credit reference agency information

Many forces limit access to credit reference agency databases to FIs because of administration costs. There is also a certain level of training required to understand the report generated.

All investigators should, however, be aware of the potential for credit agency information to assist an investigation, and should seek the support of their FIU to obtain access, if necessary.

The ELMER database

All forces have access to a database called ELMER that is usually located in the FIU or FIB (or both). ELMER contains data from suspicious activity reports (SARs).

SARs can be a useful source of intelligence for investigators. They are produced by the regulated sector (the financial industry and other businesses that deal with large volumes of money). These businesses are legally required to train all staff to recognise and report any suspicions that arise concerning money laundering or terrorist activity. SARs are sent to the National Crime Agency (NCA), which then disseminates them to forces via ELMER. A large amount of financial information and intelligence is available to forces, ELMER should be readily used by the service to investigate crime.

Investigators can search ELMER using money.web access via their force FIB or FIU, seeking information on a person or persons by:

- name
- postcode
- date of birth
- address
- previous SARs

Note – disclosures are made on transactions that financial institutions and other organisations in the regulated sector suspect to be unlawful, however many are actually legitimate and not linked to criminal activity.

Access to suspicious activity reports

The source of information from SARs must not be revealed to the subject or anyone else.

SARs are usually put on the sensitive disclosure schedule and their existence is only disclosed by a judge following a public interest immunity (PII) hearing in exceptional circumstances.

The NCA is the custodian of SARs and if PII becomes an issue during the trial it must be consulted before any final decision is made regarding disclosure or otherwise.

The highly confidential nature of SARs means that investigators do not have direct access to them. Only FIs or accredited intelligence officers (deployed in the FIU or FIB) can access and handle SARs. These officers have a duty to protect the discloser and may not pass on information that has not been sanitised.

Investigating officers should never be in possession of the confidential information contained in a SAR other than via a sanitised information or **intelligence report**, which protects the source of the information (the disclosing institution). Each force has its own policy on receipt, initial analysis, development and further dissemination of SARs.

SAR Confidentiality Breach Line

A dedicated telephone line has been established by the NCA called the SAR Confidentiality Breach Line. This allows the reporting sectors to raise any concerns about the inappropriate use of SARs (by end users) or breaches of SAR confidentiality.

The SAR Confidentiality Breach Line number is available from the NCA website UKFIU page. The freephone number operates from 09:00 to 17:00 Monday to Friday.

Information contained in intelligence systems

Information, including bank account details and telephone numbers, may be held on the Police National Database (PND).

Where an individual is the subject of an outstanding confiscation order that has not been paid in full, a force has the ability to place an asset marker (shown as AS) on both the Police National Computer (PNC) and the PND. This assists law enforcement agencies to keep track of the individual.

When obtaining details on an individual who has such a marker against their name, officers may discover assets that could be subject to confiscation. If such a situation arises, the officer must not seize the asset but should consult with a financial investigator at the earliest opportunity.

Use of financial intelligence

Intelligence development includes:

- SARs
- recording and managing financial intelligence
- partnership working

Maximising financial intelligence

Financial investigation opportunities should be used as early as possible in an investigation. As financial material can be used as intelligence or evidence, officers and staff should closely follow the rules of evidence gathering so that all material may be used later in court.

Officers should immediately consider the potential for gathering financial material on arrest of a suspect. The golden hour is when the detainee is first in custody and potential evidence has not been removed or contaminated prior to search and/or seizure. Consequently evidence that has the potential to unlock further investigative opportunities, may be found more easily.

What should I look out for?

- Evidence of unexplained wealth.
- Information from the suspect’s bank/building society account statements, and those of their family.
- Account numbers from cheque books and bank or credit cards.
- Information from financial documents regarding pensions/investments/mortgages.
- Information from business documents suggesting a working relationship between the suspect and a business or company.
- Expenditure information from bills including utility bills/receipts/car/house insurance documents.

Think about whether the suspect’s lifestyle matches their income. Do they have expensive televisions, clothes, jewellery, pets, cars, bicycles, motorbikes or household furnishings? Are there photographs showing the suspect at a holiday home, or does the suspect’s passport show evidence of travel?

What should I collect?

If in doubt, record account numbers – do not collect huge piles of paper.

Think carefully about how financial material can help you. It might provide new lines of enquiry or tell you about other criminality, and in some cases asset recovery may be possible. Talk to your financial investigator, who can give advice about what to do with the material seized.

Suspicious activity reports

Once SARs have been entered onto ELMER (the national database) they are available for use and can then be viewed, evaluated and, where appropriate, developed at force level. Forces should recognise the value of information contained within the body of the SAR such as telephone numbers and associates.

SARs are of considerable value to the police service and provide:

- intelligence on which to base investigations
- intelligence to assist and develop existing investigations into criminal activity
- intelligence about criminals and their networks, which may be of value in the future as part of the general intelligence gathering process
- reliable information to identify criminals with assets obtained from their criminality

Each force should have a policy on how SARs are used.

Recording and managing financial intelligence

SARs can be used effectively in two main ways by:

- developing the SAR to instigate an investigation
- using the ELMER database as an investigative tool, to identify SARs as part of the intelligence gathering process or when conducting investigations

ELMER should be used in the same way as any other intelligence development tools.

Covert relationships

All enquiries using open and closed sources of financial information can leave their own footprints.

If an FI makes an enquiry with a money laundering reporting officer (MLRO) at a financial institution, the institution will make a note of the enquiry, including its purpose. The investigation being conducted may involve the use of covert investigation techniques. As such, financial enquiries could result in those investigations being compromised.

Prior to making the relevant financial enquiry, consideration must be given to the type of investigation being undertaken. Any enquiries should, therefore, be progressed in consultation with the FIU.

Tags

Investigation