CIPFA The Chartered Institute of Public Finance & Accountancy

Barclays and CIPFA Counter Fraud Centre

identity fraud

CIPFA COUNTER FRAUD CENTRE

BARCLAYS

Introduction

Identity fraud has been on the increase in the last decade. An Experian survey estimated the increase to be 12% in just one year, with current accounts being the biggest target for fraudsters.[1] This is a fraud that can cause issues for both public sector organisations and their customers and, according to research by the University of Portsmouth, the annual cost of fraud in the UK could be as high as £195bn a year.[2]

In January 2016, Barclays and the CIPFA Counter Fraud Centre hosted a roundtable discussion on identity fraud. Delegates included practitioners from local authorities and central government departments and other public sector organisations. They discussed issues around identity fraud, the risks to their organisations and how to mitigate against financial and reputational damage.

While there seems to be a strategic and coordinated response to identify fraud within central government departments, the response within local authorities is less coordinated. CIPFA and Barclays would like to thank the contributors to the roundtable discussion for their insight into the issue.

What is identity fraud?

The Home Office defines identity fraud as "the use of a false or stolen identity in criminal activity to obtain money, credit, goods or services by deception". Cifas adds more depth to this description by noting that identity fraud involves "the use of personal information to apply for products and services in a victim's name – such as bank accounts, credit cards, loans and mobile phones – or create fictitious identities to achieve this".[3]

Identity fraud is growing. In 2015, almost 170,000 cases of identity fraud were reported to Cifas; an increase of nearly 50% in 12 months. One reason for the increase is the rising availability of personal data online, giving fraudsters the opportunity to use someone else's identity to open bank accounts for the purpose of money laundering, or to gain access to benefits, housing or employment.

For local authorities, the drive to provide information and services with increasingly reduced budgets has led to a greater reliance on online dissemination. This has been encouraged by the Government's digital strategy and growing demand from residents to be able to access services wherever and whenever they want; to pay their council tax, to check their bin collection, to confirm their right to vote. However, this access leaves a data trail that increases the risk of identity fraud.

The number of individuals misusing their own accounts for fraudulent purposes remained relatively stable in 2015.[4] However fraudsters are more likely to steal a genuine identity to get products and services, and bank accounts are the biggest target.[5]

1 Experian Fraud Survey 2015, available at: **www.experian.co.uk/identity-and-fraud/fraud-statistics**

2 **www.port.ac.uk/centre-for-counter-fraud-studies**

3 **www.cipfa.org/services/counter-fraud-centre/resource-bank/articles/understanding-and-combatting-identity-fraud**

4 Cifas, Fraudscape 2014, **www.cifas.org.uk/research_and_reports**

5 Cifas, Fraudscape 2016, **www.cifas.org.uk/research_and_reports**

How identity fraud affects the public sector

Individual

Creating false identities is, according to the National Crime Agency, a global business where 'specialist providers' offer counterfeit identity documents such as passports and driving licences.

Identities can be stolen by raiding bins to find personal documents such as bank statements or discarded bills, using publicly available data, stealing post from post boxes or through the false redirection of mail.

By using falsified documents and identities, individuals can make fraudulent claims for benefits, housing, employment or healthcare services.

In August 2015, Carl Jones was sentenced to 28 months in prison after using his brother's details and those of a friend to claim pension, housing and council tax benefits worth £200,000. His brother passed away in 1967 and his friend had no idea his name and address were being used to make the claims.[6]

Organisational

Despite verification processes, it is possible for an individual using false or manipulated identity documents to gain employment within an organisation. Once employed, an individual can gain privileged access to customer data, financial information and other valuable assets. Information and data could be used for their own fraudulent purposes or be disclosed to a third party. Fraud committed by an employer is sometimes referred to as 'insider fraud' and the result can be the loss to the organisation of both money and reputation.

The Internal Fraud Database held by Cifas records instances of such fraud in the UK. In 2014, the database showed a 46% increase in one year in applications that were successful before the fraud was discovered. Fraudulent job applications accounted for 63% of recorded internal frauds.[7]

Supplier

Stealing the identity of a trusted supplier, pretending to be an organisation that an authority pays regularly, sending invoices requesting payment for fake services or gaining business as an insolvent company who has re-emerged under a new name can all cost an authority a lot of money if verification processes are not in place.

Mitigating against the risk

When left unchecked, identity fraud can challenge the financial integrity of a local authority, along with its reputation. It is not merely the role of an internal fraud or audit team to manage the risk, but the responsibility of all staff to keep an eye out for areas where fraud can be carried out.

6 **http://blog.cps.gov.uk/2015/08/benefits-cheat-convicted-for-using-details-of-brother-who-died-in-1967.html**

7 Cifas, Fraudscape 2014, **www.cifas.org.uk/research_and_reports**

Developing a robust counter fraud culture

It is vital to set a 'tone from the top' that fraud and corruption is not tolerated, that counter-fraud activity is embedded in the day-to-day running of the organisation and that staff are empowered to tackle fraud.

Customers and service users can be encouraged to help counter the risks by protecting their identity online and offline. Help can be provided by having posters and leaflets in public facing areas and information on the website.

Training frontline staff on the signs of fraud

There are time pressures on frontline staff to process claims and deliver good customer service and, as a result, this may make it hard to recognise fraud. Regular training on the signs to look out for will help, and building checks into processes and manuals, will make preventing fraud part of the routine.

Risk assessments

Assessments should be carried out by each business unit to analyse the risk of identity fraud to their business and systems, with processes drawn up to counter the risk. The business unit manager is usually responsible for the risk register and any identity fraud that emerges should provide learning opportunities and a chance to improve process.

The risk register should cover the likelihood of tenders and procurement needs. Sub-contractors should be identified as part of a contract, with staff involved checked for any conflict of interest. Spend patterns should also be monitored to ensure that costs are kept at agreed limits.

Using verification tools and software

The Government has set up Verify, a website to keep an identity secure and access government digital services via a single log in.[8] Agencies such as the police, border and immigration control, and HM Passport Office (HMPO) enable Verify to perform additional checks to prevent fraudulent use of government services.

Passports and documents from the European Union can be checked using Public Register of Authentic Identity and Travel Documents Online (PRADO).

Some authorities use document scanners to establish the authenticity of identity documents. The scanned documents can be checked against established databases, such as the Metropolitan Police's Amberhill database that keeps a record of false documents. Of course, it is important to note that anyone using a genuine identity document may not be exposed using this system.

Pre-employment screening

Most organisations carry out a number of checks as standard before employment is offered. It is expensive to recruit someone, but a dismissal process can be equally costly and making sure identity checks are carried out will hopefully prevent fraud. In addition to following up references and checking official documentation, an authority could carry out a general internet search, use criminal record checks and check social media to create a picture of the applicant that may not be covered by an application form.

Conclusion

Identity fraud can impact services where money or a service can be obtained; it affects both a business and its customers. If not checked and avoided, fraud can be damaging to both the finances and reputation of a public sector organisation. With identity fraud increasing year upon year, it is important that authorities in particular assess their own capabilities in managing this risk and work with other agencies to uncover fraud.

8 www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

Further reading

- Cifas, a not-for-profit company working to protect organisations and individuals from financial crime, **www.cifas.org.uk**
- Action Fraud **www.actionfraud.police.uk**
- Guidance on examining identity documents, 2015, Home Office National Document Fraud Unit
- Slipping through the net: staff vetting guide for local authorities, Cifas

CIPFA Counter Fraud Centre

The CIPFA Counter Fraud Centre leads and coordinates the fight against fraud and corruption across local and central government, the health, education and charity sectors. We are committed to helping organisations:

- prevent, detect and recover financial loss
- protect their reputation
- develop counter fraud skills amongst staff.

Contact us to find out more: **www.cipfa.org/services/counter-fraud-centre**

CIPFA
77 Mansell Street, London E1 8AN
www.cipfa.org
T: 020 7543 5600 F: 020 7543 5700