Counter Fraud Strategy

November 2015

Contents

Background

The National Fraud Authority published a report in May 2013 which estimates the loss to the public sector in the UK from fraud to be £20 billion. As SAAS now receives most of its applications for student support using online systems that are linked across the worldwide web, our exposure from fraud is global. It is therefore likely that we are more exposed to fraud than in the past and must be fully prepared to counter the threat.

SAAS is an Executive Agency of the Scottish Government (SG) giving financial support to all eligible students studying a course of higher education in the UK. On behalf of Scottish Ministers, the Agency manages substantial student support budgets in excess of £900 million and receives over 250,000 applications for student support each year. SAAS is committed to maximising the funding that is available for our students to support them through their higher education journey. By minimising our exposure to, and losses from, fraud we are able to do this effectively.

In 2014 we commissioned a "health check" on a sample of our own data using fraud prevention tools to identify:

1. what our likely exposure to fraud is;
2. where we may be exposed, and;
3. how we can act to reduce that exposure.

From the results of the health check it was estimated that 0.5% of our applications should be considered as fraudulent. The health check also concluded that the SAAS Fraud Team has a detailed knowledge of the methods that applicants use to obtain funding fraudulently and that robust processes are in place for investigating suspected fraud and presenting cases for prosecution. The results give us confidence that we have measures in place that are effective. However, the health check also identified ways in which we can improve our resilience against fraud and has informed the development of our Fraud Response Plan. The report confirms that we have previously focused on reactive investigations that are often triggered by referrals from caseworkers, members of the public or from checks and data sources that are used to establish the validity of an application. There is therefore a need to move towards prevention and deterrence of fraud.

The implementation of additional effective counter fraud measures will require further investment by SAAS to aid in the prevention and detection of fraud.

Introduction

Aims

The purpose of this Counter Fraud Strategy is to articulate how we respond to the threat we face from fraud, now and in the future. The strategy outlines our commitment to minimising the risk of loss to SAAS as a result of fraud.

The goals outlined in this document support the strategic goals and responsibilities outlined in the SAAS Corporate Plan[1]. We will continue to provide a high quality service, minimise the inconvenience to our customers and take full advantage of secure digital options to safeguard public funds.

Definition of fraud

The SG Counter Fraud Policy defines "fraud" as a term commonly used to describe a wide variety of dishonest behaviour such as deception, forgery, false representation, and concealment of material facts. It is used to describe the act of depriving a person or organisation of something deliberately by deceit, which may involve the misuse of funds or the supply of false information.

Most of the fraud that we see is committed by:

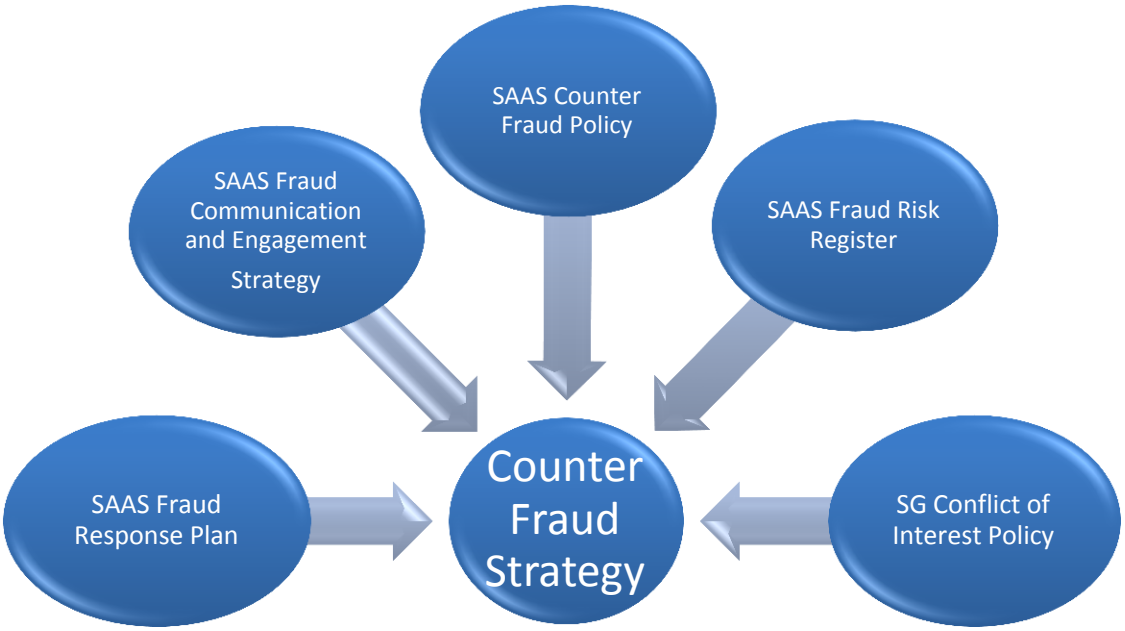
1. Opportunistic fraudsters; those who see an opportunity to gain extra money by providing false information or misrepresenting the facts.

2. Organised fraudsters; those who have intent to commit fraud and plan how they will do it.

We also see cases where applicants provide misleading or incorrect information and ultimately gain funding fraudulently but are naïve to the fact that they have committed fraud.

Associated documents

This Counter Fraud Strategy consolidates a series of interrelated policies, plans and procedures designed to prevent and manage any attempted fraudulent or corrupt act. These include:

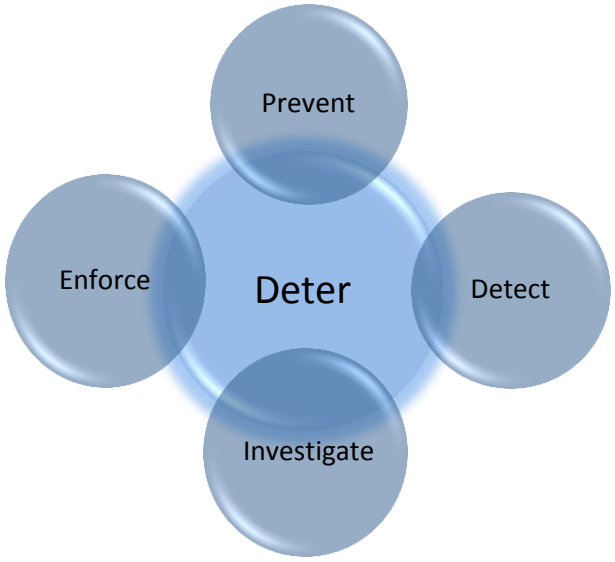


[1] The SAAS Corporate Plan provides full details of our strategic goals and priorities.

Objectives

Our objectives align closely with the Scottish Government's "Protecting Public Resources in Scotland"[2].

[2] 'Protecting Public Resources in Scotland' is a Scottish Government 2015 publication which outlines its 5 strategic objectives to counter fraud, bribery and corruption.



Deter

Promoting clear ethical standards

We promote clear ethical standards through a formal counter fraud policy, including the prevention of bribery and corruption. All staff are bound by the Civil Service Code of Conduct which requires all staff to act, at all times, with integrity, honesty, objectivity and impartiality. We also have a guidance document that explains the application of the SG Conflicts of Interest Policy which requires that staff declare any potential conflict of interest. This is particularly important for frontline staff who should not process awards for themselves, family members, friends or associates.

Awareness of these policies will be promoted throughout the Agency using all available tools such as presentations, intranet articles and training. SAAS has an induction program for all new staff entering the Agency which includes fraud awareness training delivered by the SAAS Fraud Team. This ensures that key policies are disseminated to all new employees and ensures they are aware of their responsibilities.

Raising awareness among stakeholders

We aim to deter fraud by raising fraud awareness both internally among staff and externally among the public and partner organisations. We will increase publication of successful prosecutions to maximise awareness of our zero tolerance approach. We also advertise our participation in the National Fraud Initiative data matching exercise on our website.

Our Communication and Engagement Strategy details how we will work in partnership with other government bodies and with other departments in SAAS such as Policy and Engagement, Funding Awareness and Communications to convey our commitment in dealing with fraud and to state how we will raise awareness of our policies to all staff and stakeholders.

Through the use of a wide range of communication tools we will ensure that students in particular are educated and informed about the actions we take against fraudsters and the long term consequences of committing fraud. We will expand our work with colleges and universities to ensure that this is communicated to students and that key messages are promoted.

Prevent

Review of controls

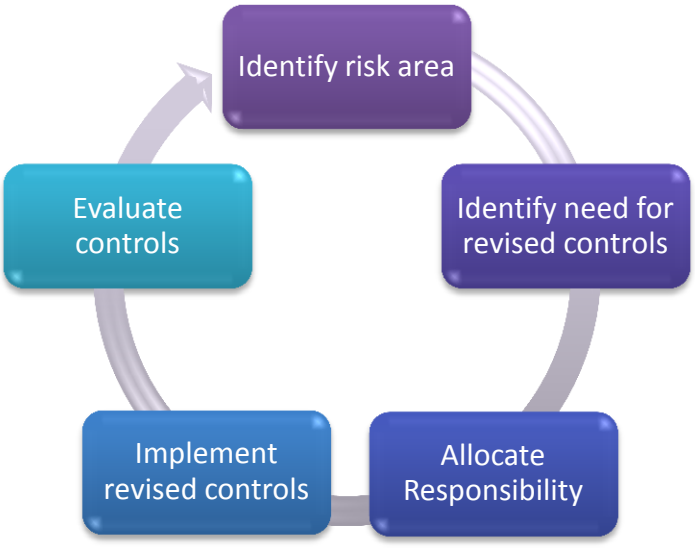
Our key risk areas have been identified and will be kept under review to identify new threats as they emerge.

We are shifting our focus to preventative measures to reduce the opportunity for fraud to be committed against us by designing out any weaknesses in our systems.

As we continue to learn lessons from the fraud investigations we carry out, we will act quickly to improve controls and preventative measures to minimise the risk of recurrence. We will keep controls under continuous review to allow us to develop and enhance when necessary.

We will focus primarily on verification and confirmation of entitlement with validation being carried out, where possible, without inconvenience to applicants.

Reviews conducted by the Fraud Analysis Team will identify trends and weaknesses in our systems. Effective feedback from investigative work will be used to evaluate procedures and will be used to inform decisions regarding changes to systems and procedures.



The Agency has a Fraud Task Force[3] which meets regularly and has operational representation from all areas of SAAS. The group reviews emerging findings and discusses lessons learnt from fraud investigations. The group reviews internal controls and system vulnerabilities and makes recommendations to the Senior Management Team to improve awareness and to stop identified frauds from being repeated.

In addition, each operational area will have a 'Fraud Champion'. The introduction of Fraud Champions will strengthen and support the Fraud Team's objectives by leading and maintaining an anti-fraud culture within their respective department. Their role will include communicating key messages to their team and ensuring that new policies and procedures are understood. They will act as a connection between the Fraud Team and operational area to share best practice for preventing and detecting fraud and will act as a point of contact for those who have a suspicion or concern about fraudulent activity.

Embedding an anti-fraud culture

The success of the Counter Fraud Strategy requires all staff to be aware of fraud issues within SAAS.

It is the Fraud Team's responsibility to make all SAAS employees aware of their obligations concerning fraud. This will be done through continuous learning and development to enhance their knowledge and awareness of fraud.

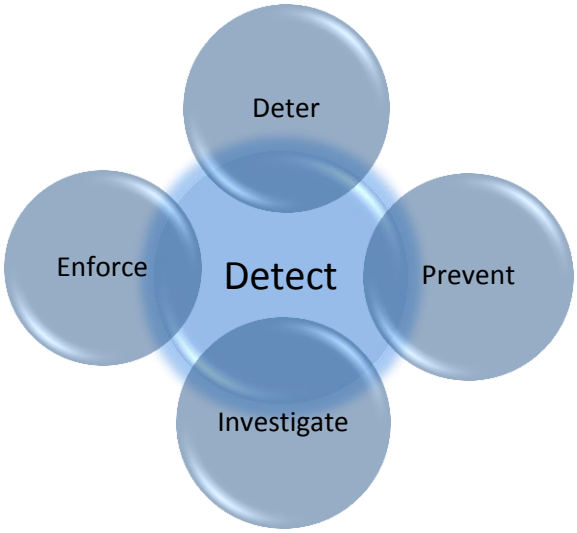
Our induction programme for new SAAS employees includes fraud awareness training and places emphasis on our anti-fraud culture. The training aims to inform new staff about the common types of fraud that are attempted against SAAS and highlights that all staff members have an active role to play in the prevention and detection of fraud.

In-depth training will be held for SAAS employees with specific responsibilities to include identity document verification, residence criteria and legislation and where possible we will work with partner organisations to deliver this training.

We will increase our engagement with our external stakeholders as outlined in our Communications and Engagement Strategy by providing support and advice in order to improve fraud awareness and encourage fraud reporting. By working closely with colleges and universities we aim to prevent fraud by sharing knowledge of best practice and updating our colleagues of any fraud trends.

Training will be reviewed and updated regularly to take account of the latest fraud activity. We will use the Fraud Task Force to provide managers with specialist support in reviewing internal controls.

[3] The Fraud Task Force is chaired by the Fraud Investigations Manager and has representatives from different business areas.



Detect

Reporting fraud

We have a dedicated fraud hotline and e-mail address that any member of the public can use, anonymously, to tell us if they have a suspicion that a fraud has been committed. This contact information is currently available on the SAAS website but we aim to publicise these details using social media and other digital platforms as part of the Communication and Engagement Strategy.

In addition, all frontline staff are encouraged to report anything that looks suspicious to the Fraud Team. We have in place internal procedures for reporting fraud including the fraud mailbox, the fraud hotline and fraud referral arrangements.

Analytical techniques

We use analytical techniques to examine our applications data and data shared by partners to identify suspicious activity and potential fraud. We are enhancing our skills and resource in this area to place more emphasis on the detection of attempted fraud based on known and emerging risk factors and will use data and technology efficiently in current and future systems to combat fraud and error.

Fraudulent activity is reported, quarterly, to the SAAS Audit Committee. In addition, a summary annual report is provided to the SG's Senior Risk Manager and any unusual or exceptional activity is also reported when it takes place.

An annual program of work is also carried out by the internal audit department of the SG which advises the Audit Committee on findings and gives the committee assurances on the Agency's operational controls. In addition, the Agency's external auditors review the operational controls annually and present their findings to the Audit Committee.

Teamwork

It is generally understood that an individual who commits fraud against one organisation will, most probably, commit fraud against another or multiple organisations. For example, someone who fraudulently claims student support from SAAS may also, fraudulently, claim income support from the Department for Work and Pensions (DWP).

We will encourage greater integration and partnership working across other organisations and the public sector to share information and develop a collaborative approach.

Arrangements are in place, and are expanding, to facilitate the exchange of information and partnership working with counter fraud colleagues on a national and local level. We currently participate in the SG's Cross Sector Counter Fraud Forum, their annual Counter Fraud Conference and also attend Scottish Local Authority Investigators Group (SLAIG) meetings to share knowledge of fraud trends, best practice and lessons learnt. We are looking to work more closely with our counterparts in the Student Loans Company (SLC), NHS Counter Fraud and other non-government organisations such as Cifas

We also maintain close relationships with key personnel at universities & colleges to share lessons learnt when frauds do occur. We do this by providing information and advice to those involved in assessing entitlement based, and discretionary, funding.

Data matching and sharing

We have data sharing arrangements in place with related bodies including UCAS (University and College Application Service) who alert us to individuals that may have provided fraudulent information to support their university or college applications.

The sharing of knowledge and data with our partner organisations who include universities & colleges, UCAS, SLC, DWP, NHS, the Home Office and local authorities is instrumental to our success.

We also take part in the National Fraud Initiative (NFI) that is led by Audit Scotland, to share data across public sector bodies. We are looking to expand our participation further to include data matching with more organisations and government bodies in the next exercise in 2016/17.

We are exploring partnership working opportunities further by looking to join the Cifas national fraud database. Cifas has the UK's most comprehensive database of confirmed fraud and has an extensive range of fraud prevention services. We are seeking to join the 300 current members from the public and private sectors, to share information and prevent further fraud. Membership of Cifas includes representation from the banking, grant awarding, finance and insurance sectors.

Investigate

SAAS is a non-police Specialist Reporting Agency (SRA) and submits fraud cases directly to the Crown Office Procurator Fiscal Service (COPFS). We work closely with COPFS when seeking prosecution and will work jointly with other government departments where a fraud has also been committed against their organisation.

We take a zero tolerance approach to fraud and apply the same response, irrespective of whether fraud is committed by opportunist fraudsters or by organised criminals.

We investigate all potential frauds that come to our attention and a comprehensive and coordinated approach is applied to all allegations of fraud in accordance with our Fraud Response Plan.

Due to the specific nature of our cases, investigations are carried out by SAAS fraud investigators who have detailed knowledge of the Agency's policies and procedures and the legislative framework for student support. Our investigators have an in depth understanding of the eligibility requirements, the support packages SAAS provides and the application process. We will work closely with our delivery and policy colleagues to ensure our knowledge and understanding is maintained and kept up-to-date.

Our investigators are Police College Scotland trained to appropriate standards and we are developing an on-going training program to ensure continuous investment in their skills and professional development. Investigators will also keep their skills and knowledge up to date by attending relevant conferences and specialist events.

For cases that are more complex or may involve organised criminals, multiple agencies or give rise to a potential conflict of interest, we will agree with our police colleagues whether it is appropriate for us to pass the case to them for further action. Our police colleagues also provide support to us when their powers of arrest and detention are required.

Enforce

The successful application of sanctions following investigation demonstrates a zero tolerance of fraud against SAAS. We will seek to apply all appropriate sanctions when evidence proves that fraud has occurred.

Appropriate sanctions can be used either independently of each other or together depending on the circumstances of each case.

The measures we use to take action against fraud and attempted fraud are:

- **Notice**– we take a serious view on attempted fraud. Where we have strong suspicions that fraud has been attempted we will enter into formal dialogue with the student in order to deter further attempts.

- **Criminal prosecution** – fraud is a crime and we investigate and present cases to the COPFS for criminal prosecution.

- **Repayment** – in addition, we routinely take civil proceedings to recover monies to supplement the sanctions decided by the criminal courts. The recovery of such money sends out a clear message that those guilty of or contemplating fraud can see that there is no benefit to be gained from such activity.

- **Not fit for support** – finally, we can deem those who have, or have attempted to, defraud us as 'not fit for support[4]' This would mean that they would no longer be entitled to support from SAAS. Those who have been deemed as not fit for support will receive no further financial support and their name will be placed on a register indefinitely.

[4] The 'Not Fit for Support' sanction is supported by our 'Not Fit for Support' Policy.

Evaluation

Counter fraud arrangements will be evaluated following the implementation of the strategy and through the outcome of audit work. Progress will be monitored by the SAAS Audit Committee and will be reported through the Annual Governance Statement.

An annual program of work is also carried out by the internal audit department of the SG which advises the Audit Committee on findings and gives the committee assurances on the Agency's operational controls. In addition, the Agency's external auditors review the operational controls, annually, and present their findings to the Audit Committee.

These governance arrangements provide the Chief Executive, as the accountable officer for the Agency, with the assurances required to complete the annual governance statement which is published with the Annual Report and Accounts.

The Agency will evaluate its counter fraud maturity against the SG Counter Fraud Maturity Model (Annex A) with a view to progress through the stages of the life cycle to become a 'leading organisation'. In view of the current policies and procedures that are in place we consider the Agency to be at the 'established' stage of the model. With a shifting of emphasis to deterrence and prevention of fraud and with the addition of new tools to aid detection such as Cifas membership, it is anticipated that over the next 2 years the Agency will progress through the Maturity Model reaching an advanced stage of 'progressive' or early stage of 'leading'.

During the next 2 years, reporting mechanisms will be improved to ensure that the costs and losses associated with fraud are better captured and reported.

Conclusion

We will minimise our exposure to fraud by investing further in fraud prevention, detection & investigation measures. By continuing to expand our knowledge and expertise, we will also enforce our zero tolerance approach and send a clear message to opportunist and organised fraudsters.

In addition we will invest further in digital preventative measures, prioritising those that we estimate will give us the greatest return on investment without impacting on the excellent customer service we provide for our students.

We will use the Counter Fraud Maturity Model as a benchmark for the measures that we have in place to monitor our progress and development.

Review date: 2 Years from publication

Annex A: Counter Fraud Maturity Model

Counter Fraud Controls	Initial	Developing	Established	Progressive	Leading
Ethics	Ethical standards are in place and communicated but are not comprehensive.	Clear ethical standards are in place including a formal counter fraud policy.	Clear ethical standards are in place through a formal counter fraud policy, and codes of conduct.	Clear ethical standards are promoted through a formal counter fraud policy, and codes of conduct including the prevention of bribery and corruption.	Counter fraud policy is embedded within the overall organisational strategy and business planning.
Policies	A fraud response plan is in place.	A fraud response plan is in place alongside other policies such as register of interests.	A fraud action plan is in place alongside other policies such as register of interests.	Fraud is dealt with effectively through implementation of a comprehensive fraud action plan, and other policies such as register of interests.	Focus is on continual improvement in updating policies regularly to respond to, and communicate, any changes to governance standards.
Training & Development	Guidance in preventing fraud, bribery and corruption is available to staff.	Guidance in preventing fraud, bribery and corruption is available to staff. Training is promoted but not supported corporately.	Guidance and training in preventing fraud, bribery and corruption is available to staff.	All staff and stakeholders are supported in their responsibilities in preventing fraud, bribery and corruption through guidance and	Knowledge and skills are updated regularly keeping up to date with any changes to professional standards.
Risk Assessment	Fraud risk assessments are ad hoc.	Fraud risk assessments are undertaken in key areas of the organisation.	Fraud risk assessments are undertaken across the organisation.	Fraud risk assessments are comprehensive and undertaken across the organisation.	Fraud risk assessments are embedded within the overall organisational risk assessment processes.
Monitoring Controls	Designing, operating and reviewing internal controls are not integrated.	Managers are encouraged to counter fraud designing, operating and reviewing internal controls.	Support is available for designing, operating and reviewing internal controls.	Managers are provided with specialist support in designing, operating and reviewing internal controls.	Using data, and technology, efficiently in current and future systems, to combat fraud and error.
Reporting Arrangements	Processes for reporting suspicions of fraud are not clear.	A process is in place for reporting suspicions of fraud.	Protecting members of staff through a robust process for reporting suspicions of fraud.	Members of staff are protected through a robust process for reporting suspicions of fraud, bribery and corruption.	Quantitative and qualitative reporting of fraud metrics is in place for the organisation.
Investigation & Response	Allegations of fraud are investigated as a priority as resources allow.	All allegations of fraud are investigated.	All allegations of fraud are investigated by skilled staff.	A comprehensive and coordinated approach is applied to all allegations of fraud including professional investigation by skilled staff.	High-risk areas are proactively assessed and analysed for potential fraud by professionally trained staff.
Communication	Communications to deter fraud are issued occasionally to staff.	The commitment to deter fraud is communicated by raising awareness of policies to staff.	The commitment to deter fraud is communicated by raising awareness of policies to all staff on a regular basis.	The commitment to deter fraud, bribery and corruption is communicated by raising awareness of policies to all staff on a regular basis.	Comprehensive communication lines in place to deter fraud, bribery and corruption by raising awareness of policies to all staff and stakeholders.