



Social Protection Reform Project
中国欧盟社会保护改革项目

COMBATTING FRAUD AND PREVENTING ERRORS IN SOCIAL SECURITY

Component 1

The Chinese social security system growing economic and social importance makes it all the more necessary that no efforts be spared to ensure that public moneys and insured persons' or enterprises contributions invested in social security be duly accounted for, and spent in accordance with legal provisions. Further, to ensure both the sustainability and the public credibility of the system, public authorities need to be in a position to guarantee that, to the extent possible, all those amounts due to social security by enterprises or individuals are duly collected, and that only those legitimately accrued benefits are actually paid. Over the last decade, specific efforts and measures were made by Chinese social security administration to strengthen fight against fraud and errors under social security. The first EU-China Social security reform project supported these efforts, notably with Beijing municipality. The present Note summarizes some salient features of fight against fraud and error in European social security, which might be used as an inspiration for further improvements in Chinese social security governance.

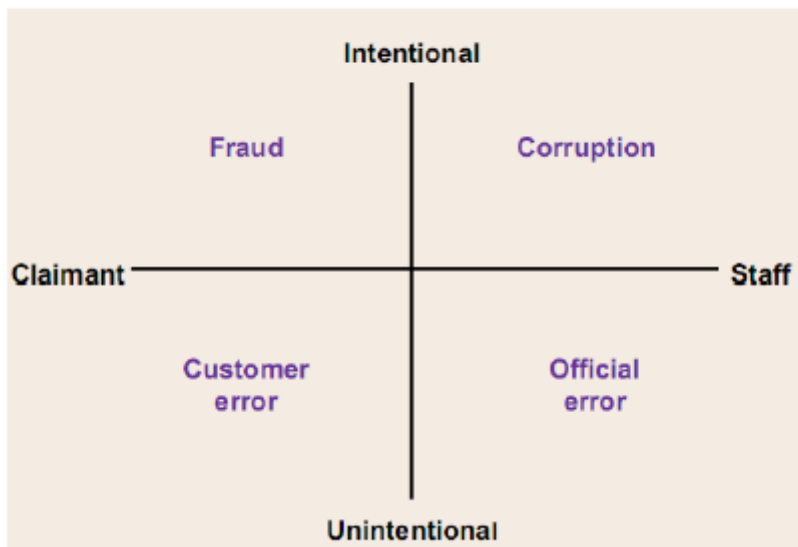
The magnitude of fraud (or errors) and its influence over social security finances (including use of staff time to address consequences) are not to be underestimated. According to a study submitted to the World Bank in 2007 (International Benchmark of Fraud and Error in Social Security Systems, RAND Europe) when data available, rates of fraud and error often range between 2 and 5% of benefit amounts which corresponds to amounts superior to typical management fees.

Although fraud and errors are usually counted jointly for statistical purposes, not all cases are the same – fraud or error may be or not intentional, it may be attributable to client, or to staff.

Taxonomy of fraud and error

Combating fraud takes place either as preventative action, as detecting action, or as deterrent action.

Taxonomy of fraud and error



Prevention

The most efficient preventative actions against fraud include the following, according to international experience:

- Launching Information campaigns
- Prepayment investigations
- Insisting on rights and obligations
- Detection
- Detecting fraud attempts is most efficiently conducted through:
- Gathering information from the public (tip-offs)
- Data-matching which includes crossing references within a scheme or across schemes
- Regular payment checks (controls)
- Risk-based assessments to organise reviews
- Random and time-based reviews
- Inter-agency compliance activities

Deterrence

Deterring tempted individuals – insured persons, beneficiaries, family members, enterprises, staff members – from attempting fraud may be obtained through:

Making punishment more severe, considering fraud or attempted fraud as criminal offence, expanding sanctions from those facilitating fraud to those using it or benefiting from it on equal footing – e.g. imposing same level of sanctions to sellers of fake social security documents and buyers of such documents

Publicizing potential sanctions, and actual sentences.

Tackling errors may be achieved either through upgrading skills levels and staff motivation, or through systemic upgrading.

Actions targeting staff

A powerful tool for limiting the number of errors committed by staff is to reward these staff in case of absence of errors (Results-based management approach)

Proper staff training and training oriented towards early identification and avoidance of errors and mistakes remains however the prominent means of achieving improvements in error limitation. This training or skills upgrading has to be coupled with a managerial organization ensuring that control, coaching and monitoring by higher level of the hierarchy is conducted as a daily operation in the vicinity of front line staff members, while managers themselves are being held responsible for non precociously detected errors or mistakes committed by staff under their supervision.

Systemic upgrading

Proper use of information technology is at the core of all efforts for limiting the occurrence or impact of errors

To be efficient in avoiding errors and mistakes, IT systems should reconcile at least four core characteristics, namely:

- reliability,
- comprehensiveness,
- uniqueness,
- self-detection.

Safeguarding against the risk of corruption

Corruption does not appear usually as a major cause for social security fraud in Europe.

Reasons for this low incidence include:

- Very precise eligibility criteria;
- Separation between assessment and payment;
- Protection of systems processing payments;
- High level of staff training, and high consideration to management;
- Investigators and reviewers not assigned cases where familiarity is suspected;
- Very active internal and external audits.

The Human - Machine Twinning

Combating fraud cannot be a matter of computers only. The use of computer technology in conjunction with human investigation greatly strengthens the latter, and makes it reach unprecedented levels of efficiency in fighting fraud and tackling errors.

The physical inspection notably of enterprises remains extremely efficient, even more efficient with computer support – a visit of an HR Department by someone accustomed to work in that area would

usually allow for an immediate, instinctive detection of possible mishaps or misconducts, and this detection might be dramatically improved thanks to efficient customers' support.

Collaborative efforts

To efficiently combat fraud or detect errors, social security agencies should not work in isolation.

Partnership among social security agencies – Here, the intention is to share data concerning registration, the basis for contributions, information on benefit awards ... among various social security institutions operating in the same realm, to ascertain that insured persons known to one scheme be known also to others

Partnership with other official bodies – A variety of other Government and official bodies have interest in collaborating with social security Agencies to also find support in their own combat against fraud (tax authorities, social welfare schemes, private insurance agencies, institutions keeping vital records, public security, etc.)

Partnership with enterprises – Automatic exchange of data and information is less costly to enterprises than manual processing, and entails less paper work for the social security institution. Automatic transmission of data also minimizes the risk of involuntary errors, permits to install safeguards in terms of automatic controls and warning signals in case of unlikely evolution over time, and allows for more sophisticated and systematic controls easily performed as desk operation by trained social security staff.

Partnership with other regions – The production of employment certificates from another region to support quick access to benefits, or the receipt and undue accumulation of benefits from various locations, or the declaration of unemployment in one city and that of work in another are all typical circumstances leading to fraud against the social security system as a whole. Exchange of data between Provinces or other pooling levels to better monitor migrant workers claims and records can prove to be a very efficient means of action to combat fraud and ensure early detection of fraudulent attempts.

The European institutional approach

At the European level, an agreement was reached on a format for safe and secure electronic transmission of data with the objective “to ensure that all the information exchanges currently taking place through the use of nearly one hundred paper E (European) forms (nearly 2000 E forms in total when taking account of the various language versions) will be undertaken by electronic means in 2009.”

In 1999, a Code of conduct had been adopted for improved cooperation between social security authorities of the Member States concerning the “combating of transnational social security benefit and contribution fraud” and “undeclared work”, as well as the “transnational hiring-out of workers”.

Member States were to encourage cooperation between their competent bodies in respect of data transmission and requests for information, while protecting the right to privacy in the processing of personal data.

Recent national measures

A number of national measures were taken over the recent years, all aiming at giving force to the provisions embodied in the Code of conduct, and to help fulfilling its objective to combat social security fraud, notably through combating clandestine work.

Country Example 1 – Belgium

A data warehouse – joint data system – created within the framework of anti-fraud project between inspection services of various social security institutions and employment service.

Goal is to facilitate carrying inspection on the basis of indicators of potential fraud.

Joint control brigades established on local basis corresponding to one legal district

Targeting 4 sectors: Agriculture; Bars and Restaurants; Shops; Construction

Sources: <http://www.epractice.eu/en/cases/oasis>

Country Example 2 - United Kingdom

Four structures cooperate to fight against social security fraud: Benefit Fraud Inspectorate (central); Local Authority Investigation Officers Group; National Antifraud Network (exchange of data); Department for Work and Pensions Fraud Investigation team (undeclared work)

Have online fraud reporting form and 24-hour fraud hotline number

Sources: <http://www.gateshead.gov.uk/Benefits%20and%20Council%20Tax/Benefits/Fraud.aspx>

Country Example 3 – Bulgaria

Under a MATRA Project (accession countries, financed by Government of the Netherlands) promotion of fraud prevention approach through a triangle Labour, Benefits and Inspection (data sharing; focus on undeclared work)

Also includes a component to promote collaboration between social security agencies, the inspectorate, the police and the judiciary.

Sources: http://www.devco.government.bg/LANGen/public/portal/prj_view.php?id=2095

Country Example 4 - France

A national Committee and a National Delegation for Fraud Fighting (joint public body) were established grouping tax authorities, employment services, social security bodies.

Social security bodies may have direct access to third party information. Working on automatic data crossing within each institution, across institutions, between institutions and other bodies

Tougher penalties, with statutory minimum have been adopted under control of the National Committee on Computerization and Freedom.

Sources: <http://www.securite-sociale.fr/institutions/fraudes/fraude.htm>

Country Example 5 – Austria

Austrian Employers Federation and Workers' Union agreed that employers should be obliged to register workers with social security before commencement of work (special target: construction industry).

Organized tax and social fraud is considered as criminal offence (imprisonment up to 5 years against employers)

Sources: <http://www.eurofound.europa.eu/eiro/2007/05/articles/AT07050191.htm>

Country Example 6 - Germany

Fraud fighting more focused on non declared work. Allegedly, 20% of those in receipt of unemployment benefits work undeclared.

Tools used are: Unemployed have hours were compulsorily at home to make control easier; More frequent home controls; Crossing tax and social security data; Establishing a special inspection body (6.000 inspectors for 3.000.000 unemployed): Controlling bank situation of beneficiaries.

Sources: http://www.cnas-icsw.org/sources/seminaires/synthese_ministere_26.03.09.pdf

Country Example 7 - The Netherlands

Fight against undeclared employment. Private Banks have to supply the tax authorities with information on all savings accounts. Measures taken to legalize cash-at-hand part time work such as domestic workers.

Trade Unions act as partners of the Government in controlling that employers comply with legislation, especially not hiring undeclared workers

Sources:

http://bancadati.italialavoro.it/BDD_WEB/bdd/publishcontents/bin/C_21_Benchmarking_408_documenti_itemName_0_documento.pdf

Whichever its importance, fraud should however not lead to paranoia.

Systematic fighting against fraud should not run counter the fundamental objective of social security, which is to serve clients promptly, efficiently and accurately.

Furthermore, beyond fraud, clerical mistakes are also responsible for losses – and many clients make mistakes, without attempting to defraud the institution.

In that respect, computerization is useful to not only detect fraud, but also help staff apply the rules – and allow for workers as well as employers to better understand and respect those same rules.

Combating fraud is more than an ethical concern – it saves money, restores public confidence in social institution. Further, when conducted including through upgrading of IT systems, combating fraud or preventing errors represents a powerful vehicle for achieving overall improvement in governance records. Fraud affects all social security clients - All have therefore to be associated in anti-fraud programmes and strategies, which is per se positive for overall governance.

JV Gruat, 2010-2017