Co-published feature

Data protection and money laundering explained

By Taek Rim (Terry) Oh, Shin & Kim

With the aim of bolstering social welfare programmes without increasing taxes, the new president of Korea has pledged to focus on expanding tax revenue by policing and normalising black markets. This increase in tax revenue is expected to pour KRW2.7 trillion into the social welfare annually.

Jumping on the bandwagon of the new government's effort to regulate the underground economy, various government agencies have begun to ask for broader access to financial data held by the Korea Financial Intelligence Unit (KoFIU). The agencies argue that increased access to financial data will enable them to expand the tax base and prevent tax evasion.

For instance, the National Tax Service (NTS) reported to the presidential transition committee on January 13 2013 that tax evasion in black markets could be cut down drastically if they are allowed broader access to the data provided by financial institutions to the KoFIU. The NTS analysed that using such financial data would allow the government to bring in at least KRW450 billion more in taxes. According to the NTS, the volume of financial data it obtains through the KoFIU is far from sufficient to detect the sources of funds flowing into black markets. To address the problem, a member of Congress proposed last year that the NTS be allowed to use for taxation purposes information on transactions exceeding KRW20 million that are reported to the KoFIU.

Furthermore, the Korea Customs Service, in its policy briefing to the presidential transition committee on January 16 2013, vowed to clamp down on foreign currency-related crimes as part of its efforts to find hidden assets with the help of the KoFIU's aggressive and comprehensive data collection process.

These proposals and requests have sparked controversy over, among other things, privacy concerns. According to a civic group, for example, providing the NTS with more access to financial data kept by the KoFIU would not only infringe on people's privacy but also effectively grant too much authority to the NTS. The civic group also predicted that, although increased access to and more expansive monitoring by the KoFIU may initially increase the government's tax revenue, it would eventually drive more economic

These proposals and requests have sparked controversy over privacy concerns

activities to go underground off the radar of the tax authority. The Financial Services Commission, which oversees the KoFIU, also voiced its concern that it would not be appropriate for the KoFIU, which was initially founded to regulate financial crimes, such as money laundering, to provide information for taxation.

Against the foregoing backdrop, we discuss below how the KoFIU, which has recently become a political hot potato, is operated to enforce anti-money-laundering law in Korea. In addition, we discuss what legal issues would arise in connection with allowing broader access to the KoFIU's financial data.

KoFIU – the data hub

The KoFIU collects financial data from financial institutions for crime control purposes. The KoFIU was established in 2001 following the Act on Reporting and Use of Certain Financial Transaction Information to regulate money laundering and terrorism financing. The Act requires financial institutions to report to the KoFIU suspicious transactions relating to money laundering and terrorism financing (STRs) and currency transactions exceeding a monetary threshold set by the implementing regulations of the Act (CTRs). The KoFIU is responsible for collecting and analysing STR and CTR information and then forwarding information deemed related to illegal transactions to domestic investigative agencies for further investigation.

Under the Act, financial institutions are required to report STRs to the KoFIU if funds of a financial transaction equal to or exceeding KRW10 million (or $5,000 or an equivalent amount in any other foreign currency) and there is a reasonable ground to suspect that the funds are "illegal assets or that the customer is involved in a "money–laundering" or "terrorism financing" activity. The reporting requirement is also triggered when a financial institution has reported to a domestic investigative agency about criminal proceeds or money-laundering. A financial institution and/or its officers and employees violating the Act may be subject to imprisonment or a fine.

The CTR is a reporting requirement imposed on a financial institution where a person deposits or withdraws KRW20 million or more in cash within one day. Moreover, the CTR requirement also applies when there is a reasonable ground to believe that a series of transactions are conducted in smaller amounts to circumvent the KRW20 million threshold. In a CTR, a financial institution is required to report to the KoFIU the identity of the person who made such transaction(s), as well as the date, time and amount of each such transaction. The CTR requirement was put in place in light of the limitation of the STR that primarily relies on financial institutions' subjective assessment.

In addition to the STR and CTR, financial institutions are required to conduct customer due diligence. Among other things, for a customer opening a new account or conducting a transaction in an amount equal to or exceeding KRW20 million (or $10,000 or an equivalent amount in any other foreign currency), a financial institution should verify not only the name and real name of the customer, but also his address, other contact information, etc. Further, if a customer is suspected of money laundering, a financial institution should verify the beneficial owner of the funds at issue and the purpose of the transaction. These reporting requirements will be enhanced with amendments to the Act to come into effect as of March 22 2013. To comply with the amended Act, financial institutions will have to establish anti-money laundering compliance programmes, and the KoFIU will be granted the authority to supervise and take appropriate measures in cases where a financial institution does not comply with the KoFIU's orders. The KoFIU can even request relevant authorities to issue an order to suspend the business operation of non-compliant financial institutions.

Legal concerns

Considering the wide spectrum of financial data the KoFIU collects, it is understandable that government agencies like the NTS feel tempted to obtain access to and use the data for their own purposes. Even under the current system, the KoFIU may provide to the NTS certain financial data for investigating tax crimes. However, what the NTS is asking for now is to use KoFIU data for pure taxation purposes.

Such expansion of access is not without legal issues. First, as mentioned above, allowing the NTS broader access to KoFIU financial data may violate privacy laws in Korea. The Act was enacted as a narrow exception to privacy laws in order to combat financial crimes. However, if KoFIU data were to be used not only for crime control but also for taxation, it may open the floodgates to a variety

About the author

Taek Rim (Terry) Oh
Partner
T: +82 2 316 4020
E: troh@shinkim.com

Taek Rim (Terry) Oh is a partner at Shin & Kim and his main areas of practice include white collar defence and FCPA/internal investigations. He has served as a public prosecutor for 14 years and has worked in the Special Investigation Department of the Prosecutors' Office and the Central Investigation Department of the Supreme Public Prosecutors' Office which handle investigations and indictments of white collar crimes. During his term in office as a prosecutor, he has conducted multiple investigations and was involved in various criminal trials for white collar crimes, particularly bribery, corporate crime, securities fraud, and accounting fraud.

His representative cases include: various bribery cases involving relatives of the former Presidents, mayors, congressmen, CEOs of state-owned companies and port trade union members; an accounting fraud case involving conglomerate companies in conspiracy with accounting firms and; a securities fraud case relating to M&A transactions. He has expertise in anti-bribery and accounting regulations and broad experience in investigating and prosecuting cases in the field.

He joined Shin & Kim in October 2011 and has been actively involved in the white collar defence team. In addition as the head of the FCPA/internal investigation practice group, he assists clients with internal investigations, FCPA due diligence and anti-corruption training.

> The general public sentiment is that the NTS already wields (almost) uncontrolled power and authority and that it does not need more

of personal privacy infringements. Also at risk is the legal principle requiring a valid warrant for any search or seizure. This principle is stipulated in the Constitution as a means to protect right to privacy and freedom from arbitrary invasions. Allowing the NTS unrestricted access to KoFIU financial data would be a violation of the legal principle.

Furthermore, a report by the National Assembly Research Service anticipates that unfettered access given to the NTS would effectively allow the agency to monopolise personal information. The report also points out that out of the seven countries that have the CTR requirement, only two (the US and Australia) allow their tax agencies to use information on a very limited basis. The general public sentiment is that the NTS already wields (almost) uncontrolled power and authority and that it does not need more. In fact, in accordance with the National Taxes Act, the NTS rarely releases information regarding tax audits, citing confidentiality concerns, even when Congress makes an information request.

With the black markets able to avoid taxes, it is true that legalising and levying taxes on private businesses in the underground market would expand the government's tax base. In order to get a grasp on the underground market, the size of which is estimated to be approximately KRW400 trillion to KRW500 trillion, strengthening the financial information system and boosting transparency in transactions would surely be the key. However, as seen from above, it would not be an easy task balancing the need to combat financial crimes against the legal mandate to protect privacy.

It remains to be seen how various issues would be resolved. Nevertheless, now with momentum building up for the new administration to increase the tax base and restrict tax evasion, it is certain that the voice emphasising the need for more financial information would continue to grow.