Ex- Director held liable for misappropriation of the source code of the software by hacking

The Indian company and the local company at the South East Asian country entered into MOU along with an Equipment supply Agreement for supply of Caller Ring Back Tone, according to which the Indian Company shall sell and local company shall purchase the Caller Ring Back Tone System (CRBT); Management System for Monitoring, Managing and provisioning of services for installation and commissioning of the system at the South East Asian country. Incidentally, the agreements etc. were signed by the Ex-Director on behalf of the Indian Company.

The software development team of the Indian company and other software engineers under the employment of the Indian Company designed and developed the software solution, called "Caller Ring Back Tone System" (CRBT) to be deployed in the South East Asian Country via the local company as per the tender requirement. The CRBT which is commonly known as personalize ring back tone is a service by which a subscriber (mobile user) can choose a ring tone (the tone heard by the caller when making a call indicating that other person's phone is now ringing) of his choice. This ring tone can be in a form of a song, musical tune, devotional songs, dialogues or any other recording and the said technology is very common and is a popular value added service provided by most of the leading mobile operators under various brands for instance; AIRTEL, a major telecom operator provides CRBT service in the name of Hello Tunes.

The aforesaid software CRBT was designed and developed to support 5,00,000 subscriber base and software license was issued to local company at South East Asian Country for 1,00,000 subscribers initially extendable to support 5,00,000 subscriber base. To control the subscription base of licensed capacity of 1,00,000 subscriber, the software team of the Indian company also designed and developed the license key generator software and also implemented this key in the core CRBT software to check the licensed capacity of the system, so that the system cannot be operated beyond licensed capacity. The Indian Company stored the source codes of the aforesaid software including the license key generator software in the CVS installed on two machines in the software development lab situated at its one of office based at Delhi. The limited access was granted to the technical team (including Ex-director) to the software and software license control mechanism comprising of software control key for the purpose authorized by the Indian company only. This key was not part of deliverable to client as purpose of this software is meaningful to control the license. Only the license key was implemented in database servers installed at client sites.

It would be meaningful to mention here that the software solution christened "Caller Ring Back Tone System" (CRBT) along with the license key generator software is a "computer programme" within the meaning of Section 2 (ffc) of the Copyright Act, 1957 and thus a "literary work" as defined u/s 2 (o) of the Copyright Act, 1957 and therefore, is a copyrightable subject matter u/s 13 of the Copyright Act, 1957. It is an established law all over the world now that source code or object code of computer program constitute an original literary work and therefore

copyrightable. Further, the copyright of the aforesaid software vests with the Indian Company as the same has been developed by its in-house software development team in the course of employment for remuneration paid, under contract of service, thus Indian company is the copyright owner within the meaning of Section 17 (c) of the Copyright Act, 1957.

Soon the development team comprising of Ex-director & other members went to the South East Asian Country for deployment of CRBT project where the software key for equivalent to 100,000 subscribers was implemented. This key was stored in database and whenever any subscriber wishes to subscribe to this CRBT service, a license check mechanism is implemented in software modules to check if licensed capacity is not exhausted.

Thereafter, a very important development took place, the said ex-director resigned from the company citing personal reasons and formed a partnership firm by the name very similar to the name of the Indian company and at the very first appearance, and one would confuse the same with that of the Indian company and think that both are related or same entity. Some other employees/officers left the Indian company and joined the Ex-director in his partnership firm. The partnership firm owned by the ex-director and his associates represented/disguised themselves to Telecom authority of the South East Country as the Indian Company and not only that they also misused the email and website of the Indian company to disguise themselves as so to the concerned authorities in that South East Asian Country.

Soon the Telecom Authority in the South East Asian Country placed an additional order for additional 4,00,000 subscribers for right-to-use license under existing contract. The partnership firm floated by the ex-director and his associates grabbed the same in connivance with the local company who were local representatives of Indian Company at such South East Asian Country.
The management of the Indian Company was surprised to learn that the firm with a very similar name is supporting the CRBT system at South East Country along with its ex-director and other ex-officials who were once part of software development team. The management of the company when contacted the Telecom authorities at the South East Asian Country, the concerned authority sent an email to the management and the content of the email revealed that software have been upgraded by the accused persons from existing installed capacity of 1,00,000 subscribers to 5,00,000 subscribers by hacking/ cracking the software code of the software belonging to the Indian company through their partnership name having deceptively similar name as that of Indian company and thus posing itself as the constituent of Indian company. The management of the Indian Company was surprised in the backdrop of the fact that they have implemented a very robust license control software mechanism so that system cannot be operated beyond licensed capacity. The management of the Indian Company contacted its local representative and the concerned Telecom Authority at the South East Asian Country which confirmed the fact that they have upgraded the license capacity with the technical support of the partnership firm run by the ex-director and his associates, once part of software development team of the Indian Company. This technical support was not possible without having source code of the software. Also, providing the license key to support 500,000 subscribers, cannot be possible without License key generation Software, which was the proprietary software of the Indian company and was a closely guarded secret maintained at its

server based at Delhi. It can be only generated by someone having the key generator software and knowhow of how to use the key generator software and complete know how of the system that where this key has to be updated in servers running at Telecom Authority at South East Asian Country.

The accused persons have opened bank accounts with different banks, where they transferred the funds they received from the illegal up gradation of the licensed capacity by hacking the software of the Indian Company. The bank account statement reveals the transfer of funds from the South East Asian Country to the concern of the accused persons. Further, there are Emails between the accused persons and the concerned authorities at the South East Asian countries which reveal the offence committed by the accused persons.

The aforesaid sequence of events revealed that the ex-director and other ex-employees illegally accessed the computer system situated at one of the office of the Indian Company at New Delhi and illegally copied the source code of the software and license key generation software, its source code and misused the same in upgrading the licensed capacity of the subscriber base from existing installed capacity of 1,00,000 subscribers to 5,00,000 subscribers at the South East Asian Country causing huge revenue loss to the Indian Company. The illegal activity which can be aptly described as misappropriation, also infringes the copyright which the Indian Company has over its proprietary software which was developed by the software development team comprising of the ex-director and his other accomplices in the course of employment for remuneration paid, under contract of service. The accused persons by unauthorized accessing the computer system of the Indian company and hacking the computer system by way of unauthorized accessing and down loading and copying the software's which is the property of the Indian company, the accused persons have also committed an contravention under Section 43 Information Technology Act, 2000 and also an offence u/s 66 under the said Act. Section 43 of the Information Technology Act, 2000 defines Hacking as an illegal act by any person who without permission of the owner or any other person who is incharge of a computer, computer system or computer network destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means. The said act makes liable the offender to pay compensation to the aggrieved party. Further, if the aforesaid illegal activity is committed dishonestly or fraudulently (the expression "dishonestly or fraudulently" is defined under the Indian Penal Code) by the accused persons, the same makes him liable for the criminal prosecution under Section 66 Information Technology Act, 2000.

The Economic Offences Wing of the Delhi Police has registered a case u/s 66 IT Act r/w Section 420/468/471 IPC and the accused persons were held to be liable. The case is under investigation.

Neeraj Aarora
(Advocate)