THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

(Set up by an Act of Parliament)

Pune Branch of WIRC of ICAI

NEWSLETTER

SEPTEMBER

2023

ISSUE NO. 09

CHAIRMAN'S MESSAGE

CA Rajesh Agrawal

Chairman

Pune Branch of WIRC of ICAI

Dear Members & Students,

During this month considering the due dates of income tax, we have organized many other professional programs for the benefit of members and students.

This month like August, we have started with National Conference on Direct Taxes Organized by Direct Taxes Committee of ICAI Hosted by Pune Branch of WIRC of ICAI which was inaugurated by CA. Piyush S Chhajed, Vice-Chairman, Direct Taxes Committee, ICAI, CA. Chandrashekhar V Chitale, Conference Director & CCM, ICAI, CA. Rajesh Agrawal, Conference Co-ordinator & Chairman, Pune Branch of WIRC of ICAI , RCM, MCM & Other Dignitaries and also graced by Shri. Chandrakant Patil Saheb, Hon'ble Minister of State in Higher and Technical Education, Government of Maharashtra, India & Guardian Minister- Pune district. The topics covered including Tribunal simulation and the faculties came across India was well appreciated by the members. This national conference again received a big response with more than 425 registrations.

As 30th Sept. is also last date for membership payment and new compliance need to be done by the members before payment, we have started help desk for the benefit of members at large including branches from western region of Maharashtra.

September is usually the busiest month for members and students. Most of us are busy in Company Audits and Tax Audits as 30th September is the last date for submissions.

Considering the due dates members has well appreciated the 'Series on Tax & Statutory Audit (Virtual)'.

The branch also arranged 17 Career counseling sessions in schools and colleges for creating awareness within students.

We have organized Ganesh Festival, ELOCUTION CONTEST On the occasion of Teacher's Day, 2023, Teacher's Day Programme, Live Session -on the theme- "Learnings from My Principal - My Teacher," from ICAI. H.O. in the month of September.

Do not forget to share your ideas, views and thoughts on any and every matter related to the branch. Assuring you that we shall definitely take cognizance of each and every email, message and verbal communication.

"You are the greatest book that ever was or ever will be, the infinite depository of all that is. Until the inner teacher opens, all outside teaching is in vain." - Swami Vivekananda

NATIONAL CONFERENCE ON DIRECT TAXES
1st & 2nd SEPTEMBER

Cyber Crime *- An emerging Challenge to Indian Banking Industry*

Rahul Sharma
B.Com, FCA, MBA (Fin.), LI.b., CAIIB
Senior Manager – UCO Bank,

Increased use of e-products :- On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998 when founding stones of information and technology were laid in Indian banking sector nobody knew that later on this will be proved a turning stone & not a mile stone and will changed completely the face of banking industry . In changing scenario system of receipt/payment has changed remarkably – swiping of debit cards or credit cards, payments through wallets (using QR codes) and e payments through net & mobiles have become our habits.

As of now India is the fourth largest internet user country in the world. The reach of internet banking has also increased due to the increased internet usage.

Data for e banking services in India are as follows :-

Volume of e-banking (Numbers)

Particulars of E Service	31.03.2013	31.03.2014	31.03.2015	31.03.2016	31.03.2017	31.03.2018
Automated Teller Machines	116378	162543	182480	199954	207813	207920
Debit Cards	336866879	399652017	564707913	671187187	780795417	903656781
Credit Cards	19553677	19226475	21288891	24860730	30374102	37782876
NEFT (Millions)	394.13	661.01	927.55	1252.88	1622.1	1946.36
RTGS (Millions)	68.52	81.11	92.78	98.34	107.86	124.46
Mobile Banking (Millions)	53.30	94.71	171.92	389.49	976.85	1872.26

The Reserve Bank of India constituted a working group on Internet Banking. The group divided the internet banking products in India into 3 types based on the levels.

Ø. Information Only System: General purpose information like interest rates, branch location, bank products and their features, loan and deposit calculations are provided in the banks website. There exist facilities for downloading various types of application forms. The
communication is normally done through e-mail. There is no interaction between the customer and bank's application system. No identification of the customer is done. In this system, there is no possibility of any unauthorized person getting into production systems of the bank through internet.

Ø Electronic Information Transfer System: The system provides customer- specific information in the form of account balances, transaction details, and statement of accounts. The information is still largely of the 'read only' format. Identification and authentication of the customer is through password. The information is fetched from the bank's application system either in batch mode or off-line. The application systems cannot directly access through the internet.

Ø Fully Electronic Transactional System: This system allows bi-directional capabilities. Transactions can be submitted by the customer for online update. This system requires high degree of security and control. In this environment, web server and application systems are linked over secure infrastructure. It comprises technology covering computerization, networking and security, inter-bank payment gateway and legal infrastructure.

Risk Assumption due to increased e transactions :- On one hand, technology has created advantage for banks and financial institutions but on the other hand, there have been risks involved in it as well. Apparently banks assume operational risks due to Technology advancements but implicitly it can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information.

As a whole we have assumed risk in almost all the areas of banking due to increased use of technology.

Cyber wrongdoings (crimes) and their types:- Broadly speaking following type of wrong doings (crimes) are associated with cyber world DDoS Attacks These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers.

The hacker then hacks into the system once the network is down. Botnets Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks. Identity Theft This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.

Cyberstalking This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety. Social Engineering Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information.

Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name. PUPs PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download. Phishing This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer.

Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access. Prohibited/Illegal Content This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network. Online Scams These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money.

Online scams include enticing offers that are “too good to be true” and when clicked on can cause malware to interfere and compromise information. Exploit Kits They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

ATM Cloning and Skimming : Cloning is also called skimming and requires copying information at a credit card terminal using an electronic device or software, then transferring the information from the stolen card to a new card or to rewrite an existing card with the information. Dark Web The dark web refers to encrypted online content that is not indexed by conventional search engines. Sometimes, the dark web is also called the dark net. The dark web is a part of the deep web, which just refers to websites that do not appear on search engines. It is a platform of illegal business on net, here information is traded – stolen card numbers, web based managing account, medical records and access to servers.

Indian Legal system and punish ability of Cyber Crimes :- Cyber Crime is not defined officially in IT Act or in any other legislation. Hence, the concept of cyber crime is just a "combination of crime and computer". Following provisions of information Technology act are relevant to us as banker. It has been tried to make them understandable through case laws :-

Section	Offence	Applicability in some	Penalty
43	Penalty and Compensation for damage to computer, computer system,	*Mphasis BPO Fraud: 2005* In December 2004, four call centre employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. These employees were not authorized to obtain the PINs. In association with others, the call centre employees opened new accounts at Indian banks using false identities. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to tr ansfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks. By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recovered was $230,000. *Verdict:Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved to commit transactions.* Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, BugsAll of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information. *Provisions Applicable: - Sections 43, 66, 66A of IT Act and Sec tion 426 of Indian Penal Code.*	Will be liable to pay damages to the affected person and also penalty up to Rs. 500000 and imprisonment up to 3 years
65	Tampering with computer source documents	*Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh*In this case, Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocomm. *Verdict:Court held that tampering with source code invokes Section 65 of the Information Technology*	Imprisonment up to three years, or/and with fine up to₹200,000
66	Hacking with computer system	*Kumar v/s Whiteley* In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed th e passwords to deny access to the authorized users.Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers.The CBI had registered a cyber crime case	Imprisonment up to three years, or/and with fine up to₹500,000

National Level Institutions dealing Cyber Crimes in India

A. National Investigation Act 2008 (NIA) : An Act to constitute an investigation agency at the national level to investigate and prosecute offences affecting the sovereignty, security and integrity of India, security of State, friendly relations with foreign States and offences under Acts enacted to implement international treaties, agreements, conventions and resolutions of the United Nations, its agencies and other international organisations and for matters connected therewith or incidental thereto.

This Institution is also related with Interstate and International offences. Related to terrorism and other offences. In 93 cases charge sheet was filed and out of that 13 were decided.

B. National Technical Research Organization (NTRO): The organization was founded in 2004. The main thrust is Development of Technology and Technological Development. This covers areas like aviation, remote sencing, cryptography and cyber security. The NTRO acts as the primary advisor on security issues to the Prime Minister and the Union Council of Ministers of India. It also provides technical intelligence to other Indian agencies. NTRO's activities include satellite and terrestrial monitoring.

C. National Critical Information Infrastructure Protection Centre : It is an organisation of the Government of India created under the Section 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16 January 2014. Based in New Delhi, India, it is designated as the National Nodal Agency in terms of Critical Information Infrastructure Protection. It is a unit of the National Technical Research Organisation (NTRO) and therefore comes under the Prime Minister's Office (PMO). NCIIP has identified i. Power & Energy, iiBanking, Financial Services & Insurance, iii. Telecom, iv Transport, v. Government and vi. Strategic & Public Enterprises as critical sectors. Aim of the organization is to protect critical information infrastructure in the country. It is decided by the policy that all government websites are to be hosted on infrastructure of National Informatics Center. National Cyber Security policy was formed on 02.07.2013.

D. Indian Cyber Crime Coordination Centre (I4C) : Home Ministry prepared a road map for tackling cyber crime. Press notification of December 2015 announced creation of I4C to fight against cyber crime. Creation was accepted in principle in May 2013 itself and finalized in September 2014 but nothing remarkable happened till recently in this respect.

E. National Association of Software and Services Companies (NASSCOM) : This is a not for profit trade association of Information Technology and BPO companies which was established in 1988. As today there are 1850 companies are registered. This association represent vital Information Technology and allied industries like BPO and KPO. NASSCOM is dedicated to expanding India's role in the global IT order by creating a conducive business environment, simplifying policies and procedures, promoting intellectual capital and strengthening the talent pool. Objective of this organization is setting strategic direction, Policy Advocacy and collaboration of best practices.

F. Data Security Council of India : is a premier industry body on data protection in India, setup by NASSCOM, committed to making cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments, their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. Tagline is “Promoting Data Protection”. This organization coordinate with government and industry. Organization was founded in August 2008. Initiatives of this organization includes Data Security, Data Privacy and Cyber Crime Awareness. In April 2015 it launched “Cyber Crime Material Level 2” – This enables police personnel to investigate online offence.

G. Indian Computing Emergancy Response Team (CERT In) : This institution comes with in Department of Electronics and Information Technology (DeITY) and founded in 2004. It has been declared as nodal agency in India under section 70B of the Information Technology Act 2000. It has legal authority to issue direction for blocking public access to information. It is Authorized to monitor and collect traffic data or information. Main Functions of organization are – a. Collection, Analysis and Dissemination of Information on cyber incidents, b. Forecast and alert of cyber security incidents, c. Emergency measures for cyber security, d. Coordination of cyber incidents, e. Issue Guidelines on Information security and f. Other prescribed functions. After IT amendment Act which made effective in 2009 Section 69 was challenged as an enactment against freedom of expression. Information Bureau notification dated 25.04.2011 clarified that “Occurrence of public emergency and interest of public safety is sin qua non for the application of the section.

National Level Institutions dealing Cyber Crimes in India

A. Central Bureau of Investigation (CBI) : This organization function under Department of Personnel, Ministry of Personnel, Pension and Public services under Government of India. It has been entrusted with the task of "Preservation of values in public life and ensure health of economy". This organization is a nodal police agency of Interpol. CBI succeeded Delhi Special Police Establishment (DSPE) with enlarged functions, vide resolution of ministry of Home affairs, GOI April, 1963. It has specialized structure to with cyber crime : a. Cyber crime research and development unit, b. Cyber crime Lab, c. Cyber crime Investigation cell and d. Network Monitoring Centre.

B. Investigation Bureau (IB): This is the oldest investigation agency which was founded in the end of 19th century. It comes under the ministry of Home Affairs, it was earlier used by British for gathering intelligence about external invasions and confidential information. Top posts under this organization are held by officers of Police, Revenue services and Army.

C. Research and Analysis Wing (RAW): It is a Foreign Intelligence Agency of India, it is not under any department but a separate outfit – work as a wing of cabinate secretariat. It was started in early 1960s after Chinese aggression in India.

D. Directorate of Enforcement : This is Financial Investigation Agency under Department of Revenue, ministry of Finance. This organization has been given specific task of implementation of Foreign Exchange Management Act (FEMA) 1999 and Prevention of Money Laundering Act (PMLA)

E. National Association of Software and Services Companies (NASSCOM) : This is a not for profit trade association of Information Technology and BPO companies which was established in 1988. As today there are 1850 companies are registered. This association represent vital Information Technology and allied industries like BPO and KPO. NASSCOM is dedicated to expanding India's role in the global IT order by creating a conducive business environment, simplifying policies and procedures, promoting intellectual capital and strengthening the talent pool. Objective of this organization is setting strategic direction, Policy Advocacy and collaboration of best practices.

F. Data Security Council of India : is a premier industry body on data protection in India, setup by NASSCOM, committed to making cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments, their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. Tagline is "Promoting Data Protection". This organization coordinate with government and industry. Organization was founded in August 2008. Initiatives of this organization includes Data Security, Data Privacy and Cyber Crime Awareness. In April 2015 it launched "Cyber Crime Material Level 2" – This enables police personnel to investigate online offence.

G. Indian Computing Emergancy Response Team (CERT In) : This institution comes with in Department of Electronics and Information Technology (DeITY) and founded in 2004. It has been declared as nodal agency in India under section 70B of the Information Technology Act 2000. It has legal authority to issue direction for blocking public access to information. It is Authorized to monitor and collect traffic data or information. Main Functions of organization are – a. Collection, Analysis and Dissemination of Information on cyber incidents, b. Forecast and alert of cyber security incidents, c. Emergency measures for cyber security, d. Coordination of cyber incidents, e. Issue Guidelines on Information security and f. Other prescribed functions. After IT amendment Act which made effective in 2009 Section 69 was challenged as an enactment against freedom of expression. Information Bureau notification dated 25.04.2011 clarified that "Occurrence of public emergency and interest of public safety is sin qua non for the application of the section.

H. Central Bureau of Investigation (CBI) : This organization function under Department of Personnel, Ministry of Personnel, Pension and Public services under Government of India. It has been entrusted with the task of "Preservation of values in public life and ensure health of economy". This organization is a nodal police agency of Interpol. CBI succeeded Delhi Special Police Establishment (DSPE) with enlarged functions, vide resolution of ministry of Home affairs, GOI April, 1963. It has specialized structure to with cyber crime : a. Cyber crime research and development unit, b. Cyber crime Lab, c. Cyber crime Investigation cell and d. Network Monitoring Centre.

I. Investigation Bureau (IB): This is the oldest investigation agency which was founded in the end of 19th century. It comes under the ministry of Home Affairs, it was earlier used by British for gathering intelligence about external invasions and confidential information. Top posts under this organization are held by officers of Police, Revenue services and Army.

F. Research and Analysis Wing (RAW): It is a Foreign Intelligence Agency of India, it is not under any department but a separate outfit – work as a wing of cabinate secretariat. It was started in early 1960s after Chinese aggression in India.

G. Directorate of Enforcement : This is Financial Investigation Agency under Department of Revenue, ministry of Finance. This organization has been given specific task of implementation of Foreign Exchange Management Act (FEMA) 1999 and Prevention of Money Laundering Act (PMLA)

Data Security : Some Issues

Data has certain value due to which it needs to be protected. This value is there due to - a. Confidentiality Value : Some Data/Information are so confidential that their leakage may cause threat even to the sovereignty of a nation, b. Financial Value : Some Data/Information may have monitory value like CVV number, ATM card PIN, Credit Card number and details as to Date of Birth etc., c. Copy Right Value : Some Data/Information may be so valuable that their copy may also have worth e.g. Music CD, Movie DVD etc.

Security Should be at right time and place : At the point of Storage of data sufficient security has to place – sufficiency of security measures depends on volume and nature of data stored & Vulnerability associated with data. Security should also be deployed in Transit of Data/Information – Such security is very important because data is most vulnerable in transit. Most frauds related with cyber world are committed when data remained in transit. Security at the time of retrieval is also very important – since data may be accessed by some one who may not supposed to do the same.

Pillars of Cyber Security :- Some Cyber experts concludes that Cyber security has 4 pillars (First Four enumerated below), while some others are of the opinion that there are more than 4 pillars of data security. Some other cyber professional discuss only first 3 which are called CIA in short.

1. Confidentiality :- Quality of confidentiality has to be maintained. Security system which address confidentiality of data is a good security system. If a security system cannot maintain confidentiality of information it is futile.

2. Integrity : Integrity of data means data should remain in same form and should not be allowed to be tempered and manipulation. This concept should be respected the most when data is in transit.

3. Availability : This concept says that data should be made available at all times as envisaged from system. Non availability of data at the time of need of it makes entire system vulnerable. DOS – Denial of System and DDOS – Distributed Denial of System are among most common bugs in our computer systems.

4. Non Repudiation : this pillar says that all stake holders of data should be made responsible and should not be permitted to deny their responsibility. A. Creator owns the responsibility of data entry, B. Sender owns the responsibility of sending data, C. Receiver owns the responsibility of receiving data and finally D. Network provider owns the responsibility of carrying data. No one of them should be allowed to step back and every one of them should be made responsible for their job.

5. Authorization : Process of confirming whether the user has authority to access and issue commands which he is accessing and issuing.

6. Authentication : This is a process which confirms that he is the actual person or entity who has accessed the system. One factor Authentication this authentication is exercised through possession of device or card. e.g. Id cards or debit cards etc. Two Factor Authentication: In addition of card or device if a person is required to enter PIN or password then it will be called two factor authentication.

Reliability : Dependability is a subset of integrity. If one can rely upon in times of crisis or disaster data will be called reliable.

Simple Mail Transfer Protocol (SMTP) : Emails are not authentic communication unless specific technology are deployed. A. Digital signature : Authentic electronic communication results because of digital signatures. These are digital code called a hash value generated and authenticated by a process (Public key encryption). B. Electronic Signature : Authenticates that person claiming to send has actually sent it and person receiving authenticates and confirm receiving it by user id and password. It is as security measure on both the ends.

Rahul Sharma
B.Com, FCA, MBA (Fin.), LI.b., CAIIB
Senior Manager – UCO Bank,
152/41, Shipra Path, Opp. Patel Marg,
Mansarovar, Jaipur - 302 020
Phone - 9460759564

"CCD" - *Do we need to obtain Valuation report for Issuance of Compulsory Convertible Debenture ("CCD") to investors?*

CA Lalit Valecha
Partner,
Ahuja Valecha and Associates LLP

We are in midst of funding winter where we have seen a significant drop in startup valuations since Q4 of calendar year 2022 and also in 2023 as compared to the glitzy valuations that existing in 2021 and early part of 2022, further the round size have also reduced. However the Startups needs fund and investment to stay afloat and increase runway, it is observed that many startups in the early stage and also during bridge rounds are raising funds in form of Compulsory Convertible Debenture ("CCD") with commercial terms favourable to both the investor and startups by agreeing on a construct of conversion of CCD into shares in future based on the lower of the a) valuation in the next Qualified Financing Round ("QFR") or b) a post money valuation cap, or a discount on the valuation in the QFR , this helps startups close the commercial negotiation faster without worrying to raise a round at a fixed valuation. Considering this background the question that arises is that whether the Startup/ Company needs to obtain a valuation report for issuance of CCD, for this we can take into consideration a simple case study as below.

Background:

The entity is an unlisted private limited Company incorporated under the provisions of Companies Act, 2013. The Company proposes to issue Compulsory Convertible Debenture ("CCD") of face value of ? 10,000/- per CCD to certain investors pursuant to a Compulsory Convertible Debenture Agreement executed between the Company, its founder and investors and in terms of provisions of Section 42, Section 62(1)(c) and Section 71 of the Companies Act, 2013 (the "Act") read with Rule 13 of the Companies (Share Capital and Debentures) Rules, 2014 and Rule 14 of the Companies (Prospectus & Allotment of Securities) Rules, 2014, as amended.

Question:

Whether a valuation report is required to obtained from a Registered Valuer in terms of applicable provisions of Section 42 and Section 62(1)(c) of the Act at the time of issuance of CCDs or at the time of conversion of CCDs into Equity Shares?

Opinion

The issue and offer of CCD is governed by the provisions of Section 71 read with Section 42 and 62(1)(c) of the Act and Rule 13 of the Companies (Share Capital and Debentures) Rules, 2014 and Rule 14 of the Companies (Prospectus & Allotment of Securities) Rules, 2014. The provisions of Section 61(1)(c) read with Rule 13(2)(g) Companies (Share Capital and Debentures) Rules, 2014 provides that price of the shares or other securities to be issued on a preferential basis, either for cash or for consideration other than cash, shall be determined on the basis of valuation report of a registered valuer.

However, Rule 13(2)(h) of the Companies (Share Capital and Debentures) Rules, 2014 provides that where convertible securities are offered on a preferential basis with an option to apply for and get equity shares allotted, the price of the resultant shares pursuant to conversion shall be determined –

(i) either upfront at the time when the offer of convertible securities is made, on the basis of valuation report of the registered valuer given at the stage of such offer, or

(ii) at the time, which shall not be earlier than thirty days to the date when the holder of convertible security becomes entitled to apply for shares, on the basis of valuation report of the registered valuer given not earlier than sixty days of the date when the holder of convertible security becomes entitled to apply for shares:

1) the price worked out in accordance with the relevant SEBI guidelines in case of a listed Indian company or in case of a company going through a delisting process as per the SEBI (Delisting of Equity Shares) Regulations, 2009; or

2) the valuation of capital instruments done as per any internationally accepted pricing methodology for valuation on an arm's length basis duly certified by a Chartered Accountant or a SEBI registered Merchant Banker or a practicing Cost Accountant, in case of an unlisted Indian Company.

Basis the above even though the Company is not required to obtain a valuation report from Registered Valuer on issuance of CCD under the provision of Company Act 2013 the Company will be required to obtain valuation report from Chartered Accountant or a SEBI registered Merchant Banker or a or a practicing Cost Accountant. Also as per FDI pricing guidelines, the price or conversion formula of the instrument should be determined upfront at the time of issue of the instrument. The price at the time of conversion should not in any case be lower than the fair value worked out, at the time of issuance of such instruments, in accordance with these rules. Due to the above rules the Company may have to comply with the valuation regulation under FEMA if there are non-resident investors. Further the provision of Section 56(2) (viib) of the Income Tax Act 1961 read with rule 11UA of The income-tax Rules, 1962 ("IT Act") shall apply only in case of issuance of shares as such the Company is not required to obtain a valuation report for issuance of CCD under the IT Act.

Disclaimer

The content of the note / memo and any views expressed therein are entirely based on a specific case study enumerated above. Any inaccuracy could have a material impact on our views or conclusions and should therefore be intimated to us immediately.

The conclusions reached and views expressed are matters of opinion based on tax laws and other regulations prevailing as of the date of this note / memo and our past experience with the tax, regulatory or other authorities as may be applicable. However, there can be no assurance that the tax authorities or regulators may not take a position contrary to our views. Tax laws and other regulations are subject to changes from time to time and as such any changes may affect the advice contained in our note / memo.

CA Lalit Valecha
Partner,
Ahuja Valecha and Associates LLP

Pune Branch of WIRC of ICAI

Plot No. 08, Parshwanath Nagar, CST No. 333,
Sr. No. 573, Munjeri, Opp. Kale Hospital,
Near Mahavir Electronics, Bibwewadi, Pune 411037
Tel : (020) 24212251 / 52 Email : admin@puneicai.org

Advertisement Tariff

for Pune Branch Newsletter WEF November 2015

Back Page (19 X 15) Color	16,500/-
Inner Page of Front / Back Page (A4) Color	16,000/-
Full Page (A4) Color	15,000/-
Half Page	8,000/-
Quarter Page	4,500/-

Discount : 3 to 6 Insertions : 10 %
7 to 12 Insertions : 15 %
Additional GST : 18 %

www.puneicai.org

www.puneicai.org