CHAPTER 11

Other Offences under the Information Technology Act in India

A Brief Overview of Cybercrimes

These days Information Technology (IT) is becoming increasingly popular and imminent in the day-to-day life of individuals, companies and the society as a whole. This is because it has brought more efficiency, accuracy and speedier transactions particularly in business world. We find the popularity of data processing equipments and the use of computers in day-to-day transactions like online banking, tele-marketing, use of credit or debit cards and so on, which have made banking very swift, and accurate. Such advances in the IT and the potentialities in the business world have attracted many misusers, unscrupulous people and criminals to commit many cyber crimes relating to financial world. The cyber crime offenders befool people through the Internet using different techniques and schemes. And therefore, we find these days a new class of white collared criminals perpetuating fraud on the Internet.

With various kinds of financial crimes on the cyberspace ranging from security frauds by altering information into a computer system or manipulating the programmes for processing information and altering the output. Many frauds are being committed on the online auction trade. The Internet fraud commonly known as phishing where e-mails appear to be from legitimate online banking websites warn the recipients of a recent unauthorised purchase for their attention requiring urgent action. Such Internet fraud masters can create false identities about themselves and sell the information to equally dangerous third parties. Even Internet gambling is becoming popular. Digital forgery is done by creating document which the offender knows is not genuine and yet project the document as if it is genuine one, by affixing somebody else's signature on the document. The Internet is also being used for sale of illegal things or articles which are

prohibited in a country—like selling arms, drugs and other prohibited military armour. There are also violations of copyrights on the Internet.

We have pointed out some of the misuses of the Internet by various kinds of cyber criminals in the previous paragraph. This raises the need to provide reasonable control through legal means on the activities of the cyber offenders on the Internet. Most of the countries who frequently use cyberspace/Internet for business transactions and for interaction with society in general have enacted cyber laws to control cyber crimes. In India we have enacted the IT Act and have tried to curb, control and punish cyber crimes. We have discussed in Chapter X of this work some important cyber crimes on the Internet. In this Chapter we will discuss many other cyber crimes and the procedures to control and prosecute cyber crime offenders.

Offences by Intermediaries

Under Section 67C of IT (Amendment) Act, 2008—

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

The above Section requires the intermediary to preserve and retain information for such duration and format as the Central Government may prescribe. Any violation by the intermediary who intentionally or knowingly contravenes the provisions under this Section shall be punished for an imprisonment up to three years and also shall be liable to fine. The above mentioned offence requires *mens rea* on the part of the intermediary to commit an offence. The offence is also cognizable and bailable under Section 77B of the Act.

(a) Exemption from Liability of Intermediary in Certain Cases.

Under Chapter XII of the IT (Amendment) Act, 2008, Section 79 states—

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promises or authorises in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation: For the purpose of this section, the expression 'third party information' means any information dealt with by an intermediary in his capacity as an intermediary.

The above Section gives intermediaries generally an exemption from liability for any third party information, data or communication made available or hosted by him. However, under sub-section (3) of this Section, the intermediary who conspires, abets or aids or induces by threats or promises or authorises in the commission of unlawful act or any information or data controlled by the intermediary is being used to commit unlawful act shall be made liable for the offence if he fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Power of the Controller to Give Directions to Certifying Authorities

The Controller under the Act has the power—

(1) to may by order, direct a CA or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order by the Controller if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or both[1].

1. Section 68, IT (Amendment) Act, 2008.

(ii) 'traffic data' means any data identifying or purporting to identify any person, computers system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service or any other information.

The above Section provides for the power of the Central Government for the purposes of enhancing cyber security and for identification may authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. A person in-charge or the intermediary when called upon, shall provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource. Such monitoring requires proper procedure and safeguards for monitoring and collecting traffic data which shall be prescribed under the rules. Any person who contravenes the provisions of sub-section (2) shall be punished with imprisonment for a term up to three years and shall also be liable to fine. The above offence is cognizable, although it is bailable under Section 77B of the Act.

Offences Relating to Protected System

Section 70 as amended by the IT (Amendment) Act, 2008 provides—

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
Explanation: For the purposes of this section, 'Critical Information Infrastructure' means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

The above Section provides for the offence relating to protected system which directly or indirectly affects the Critical Information Infrastructure. The object of the offence is to prevent the incapacitation or destruction of computer resource which may have debilitating impact on national security, economy, public health

or safety. The appropriate Government may by order in writing, authorise the persons who are authorised to access protected system. The contravention of the provisions of this section is serious offence which may be punished with imprisonment up to ten years and shall also be liable to fine. The offence is cognizable and also non-bailable under Section 77B of the Act.

The Offence of Misrepresentation

Under Section 71 as amended by the IT (Amendment) Act, 2008, it is provided that any person who makes any misrepresentation to or suppresses any material fact from the Controller or the CA for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees or with both.

Under the above Section for obtaining any license or Electronic Signature Certificate if any person makes any misrepresentation or suppresses any material fact, he shall be punished for imprisonment up to two years or with fine up to one lakh rupees or with both. The offence under this Section is non-cognizable offence and is also bailable offence under Section 77B of the Act.

Offence of Publishing Electronic Signature Certificate with False Particulars

Section 73 as amended by the IT (Amendment) Act, 2008, provides—

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that—
   (a) The Certifying Authority listed in the certificate has not issued it; or
   (b) The subscriber listed in the certificate has not accepted it; or
   (c) The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a electronic signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees, or with both.

In the above Section, if a person publishes an electronic signature certificate or otherwise makes it available to any other person with the knowledge that (i) the CA listed in the certificate has not issued it; or (ii) the subscriber listed in the certificate has not accepted it; or (iii) the certificate has been revoked or suspended unless such publication is for the purpose of verifying an electronic

of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.

Like under the IPC even an attempt of an offence under the IT Act is punishable. In case a provision for punishment for an attempt is provided for under the IT Act the offender shall be punished as provided for under the provision for an attempt of the offence. Otherwise when no provision has been made for an attempt of an offence under the IT Act, then the offender may be punished with one-half of the longest term of imprisonment provided for the offence. He may also be punished with fine as provided for under the concerned offence. The offender may also be given the punishment of one-half of the imprisonment as well as the fine provided for under the offence in the IT Act. An attempt is done by the offender when he does an act while attempting the offence and not for the remote act or omission.

Commission of Offences by Companies under the IT Act

Under Section 85 of the Information Technology Act, 2000—

(1) Where a person committing a contravention of any of the provisions of this Act or any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.
   Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section(1) where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly[5].

5. Section 85 IT (Amendment) Act, 2008.

Moreover, the accused can also file an application for plea bargaining in the Court in which such offence is pending for trial under Section 265B of criminal procedure, 1973. Moreover, the accused can also file an application for mutually satisfactory disposition of the offence under Section 265C of code of criminal procedure, 1973.

Cognizance of Offences and Bail under the IT Act

Under Section 77B of the IT (Amendment) Act, 2008, notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

The above Section provides that if the offence is punishable with imprisonment of three years and above under this Act, a police officer can take cognizance of the offence and arrest an accused without a warrant of the court. And any offence under the Act which is punishable with imprisonment up to three years is a bailable offence. Therefore, an accused for an offence under the Act punishable up to three years is entitled to get bail on the principles applicable to bailable offences.

Punishment for Abetment and Attempt to Commit Offences under the IT Act

Under Section 84B of the IT (Amendment) Act, 2008, any person who abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy or with the aid which constitutes the abetment.

The offence of abetment can be committed under the IT Act by instigation or in pursuance of the conspiracy and by aiding the offender in the commission of the offence. It is similar to an abetment as defined under Section 107 of the IPC. Like in IPC an offender is liable for the punishment provided for under the provisions of the IT Act for the abetment of any offence under the Act.

Under Section 84C of the IT (Amendment) Act, 2008, any person who attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment

Explanation: For the purposes of this section—

(i) company means any body corporate and includes a firm or other association of individuals; and

(ii) 'director', in relation to a firm, means a partner in the firm.

Under the above section if a person committing a contravention of the provisions of this Act, rule, direction or order is a company then every person who was in-charge of and was responsible to the company for the conduct of the business as well as the company itself shall be guilty of contravention and can be prosecuted for the offence and punished accordingly, unless it can be proved that a person, when the contravention took place, was without his knowledge and he exercised all due diligence to prevent the contravention. However, if contravention of the provision of the Act, rule, direction or order committed by a company it is proved that the contravention has taken place with the consent or connivance or due to negligence of any director, manager, secretary, or other officer then such person shall be deemed to be guilty of contravention and punished accordingly under the Act.

In *Avnish Bajaj* v. *the State*[6], it was held by the High Court of Delhi that unlike some other statute containing penal provisions, the IPC does not incorporate the concept of criminal liability of a Director or an employee where the principal accused is a company. In other words, there is no provision similar to Section 141 of the Negotiable Instruments Act, 1881 or Section 140 of the Customs Act, 1962 or Section 85 of the IT Act. These are provisions that provide for a deemed criminal liability of a person who, at the time of commission of the offence by the company, was in charge of the affairs of the company or responsible to it for the conduct of its business. The proviso to such provision makes it possible for such person to escape liability by proving at the stage of trial that the offence was committed by the company without his or her knowledge. Therefore, once the deemed criminal liability gets attracted under the substantive provisions, the burden shifts to the accused under the proviso to rebut such presumption. And the court held that in this case it appears that without the company being made an accused its directors can be proceeded against under Section 67 read with Section 85 of the IT Act.

The Power of Police Officer and other Officers to Enter and Search

Under Section 80 of the IT (Amendment) Act, 2008, it is provided that—

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector, or any other

6. MANU/DE/0851/2008: 150(2008) DLT 769.

of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.

Like under the IPC even an attempt of an offence under the IT Act is punishable. In case a provision for punishment for an attempt is provided for under the IT Act the offender shall be punished as provided for under the provision for an attempt of the offence. Otherwise when no provision has been made for an attempt of an offence under the IT Act, then the offender may be punished with one-half of the longest term of imprisonment provided for the offence. He may also be punished with fine as provided for under the concerned offence. The offender may also be given the punishment of one-half of the imprisonment as well as the fine provided for under the offence in the IT Act. An attempt is done by the offender when he does an act while attempting the offence and not for the remote act or omission.

Commission of Offences by Companies under the IT Act

Under Section 85 of the Information Technology Act, 2000—

(1) Where a person committing a contravention of any of the provisions of this Act or any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section(1) where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly[5].

5. Section 85 IT (Amendment) Act, 2008.

Explanation: For the purposes of this section—

(i) company means any body corporate and includes a firm or other association of individuals; and

(ii) 'director', in relation to a firm, means a partner in the firm.

Under the above section if a person committing a contravention of the provisions of this Act, rule, direction or order is a company then every person who was in-charge of and was responsible to the company for the conduct of the business as well as the company itself shall be guilty of contravention and can be prosecuted for the offence and punished accordingly, unless it can be proved that a person, when the contravention took place, was without his knowledge and he exercised all due diligence to prevent the contravention. However, if contravention of the provision of the Act, rule, direction or order committed by a company it is proved that the contravention has taken place with the consent or connivance or due to negligence of any director, manager, secretary, or other officer then such person shall be deemed to be guilty of contravention and punished accordingly under the Act.

In *Avnish Bajaj* v. *the State*[6], it was held by the High Court of Delhi that unlike some other statute containing penal provisions, the IPC does not incorporate the concept of criminal liability of a Director or an employee where the principal accused is a company. In other words, there is no provision similar to Section 141 of the Negotiable Instruments Act, 1881 or Section 140 of the Customs Act, 1962 or Section 85 of the IT Act. These are provisions that provide for a deemed criminal liability of a person who, at the time of commission of the offence by the company, was in charge of the affairs of the company or responsible to it for the conduct of its business. The proviso to such provision makes it possible for such person to escape liability by proving at the stage of trial that the offence was committed by the company without his or her knowledge. Therefore, once the deemed criminal liability gets attracted under the substantive provisions, the burden shifts to the accused under the proviso to rebut such presumption. And the court held that in this case it appears that without the company being made an accused its directors can be proceeded against under Section 67 read with Section 85 of the IT Act.

The Power of Police Officer and other Officers to Enter and Search

Under Section 80 of the IT (Amendment) Act, 2008, it is provided that—

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector, or any other

6. MANU/DE/0851/2008: 150(2008) DLT 769.

APPENDIX II

The Information Technology (Certifying Authorities) Rules, 2000

[Extracts]

In exercise of the powers conferred by Section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the application and other guidelines for certifying Authorities, namely—

1. Short Title and Commencement

(1) These Rules may be called Information Technology (Certifying Authorities) Rules, 2000.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions

In these Rules, unless the context otherwise requires,—

(a) 'Act' means the Information Technology Act, 2000 (21 of 2000);

(b) 'applicant' means Certifying Authority applicant;

(c) 'auditor' means any internationally accredited computer security professional or agency appointed by the Certifying Authority and recognized by the Controller for conducting technical audit of operation of Certifying Authority;

(d) 'Controller' means Controller of Certifying Authorities appointed under sub-section (1) of Section 17 of the Act;

(e) 'Digital Signature Certificate' means Digital Signature Certificate issued under sub-section (4) of Section 35 of the Act;

(f) 'information asset' means all information resources utilized in the course of any organization's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks);

(g) 'license' means a license granted to Certifying Authorities for the issue of Digital Signature Certificates under these rules;

(h) 'licensed Certifying Authority' means Certifying Authority who has been granted a license to issue Digital Signature Certificates;

(i) 'person' shall include an individual; or a company or association or body of individuals; whether incorporated or not; or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments;

(j) 'Schedule' means a schedule annexed to these rules;

(k) 'subscriber identity verification method' means the method used to verify and authenticate the identity of a subscriber;

(l) 'trusted person' means any person who has,—

(i) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Rules in respect of a Certifying Authority; or

(ii) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of a Certifying Authority's computing facilities.

(m) words and expressions used herein and not defined but defined in Schedule-IV shall have the meaning respectively assigned to them in that schedule.

3. The Manner in which Information be Authenticated by Means of Digital Signature

A Digital Signature shall,—

(a) be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again;

(b) use what is known as 'Public Key Cryptography', which employs an algorithm using two different but mathematical related 'keys'—one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form, the process termed as hash function shall be used in both creating and verifying a Digital Signature.

Explanation: Computer equipment and software utilizing two such keys are often termed as 'asymmetric cryptography'.

4. Creation of Digital Signature

To sign an electronic record or any other item of information, the signer shall first apply the hash function in the signer's software; the hash function shall

compute a hash result of standard length which is unique (for all practical purposes) to the electronic record; the signer's software transforming the hash result into a Digital Signature using signer's private key; the resulting Digital Signature shall be unique to both electronic record and private key used to create it; and the Digital Signature shall be attached to its electronic record and stored or transmitted with its electronic record.

5. Verification of Digital Signature

The verification of a Digital Signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a Digital Signature and by using the public key and the new hash result, the verifier shall check,—

(i) if the Digital Signature was created using the corresponding private key; and

(ii) if the newly computed hash result matches the original result which was transformed into Digital Signature during the signing process. The verification software will confirm the Digital Signature as verified if—

(a) the signer's private key was used to digitally sign the electronic record, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a Digital Signature created with the signer's private key; and

(b) the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.

6. Standards

The Information Technology architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different activities associated with the Certifying Authority's functions are as under,—

The product	The standard
Public Key Infrastructure	PKIK
Digital Signature Certificates and Digital Signature revocation list Directory (DAP and LDAP)	X.509. version 3 certificates as specified in ITU RFC 1422 X500 for publication of certificates and Certificates Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key algorithm	DSA and RSA
Digital Hash Function	[SHA-1 and SHA-2]

(Contd.)...

The product	The standard
RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)
	PKCS#5 Password Based Encryption Standard
	PKCS#7 Cryptographic Message Syntax standard
	PKCS#8 Private Key Information Syntax standard
	PKCS#9 Selected Attribute Types
	PKCS#10 RSA Certification Request
	PKCS#12 Portable format for Storing/ transporting a user's private keys and certificates
Distinguished name	X. 520
Digital Encryption and Digital Signature	PKC5#7
Digital Signature Request Format	PKCS#10

7. Digital Signature Certificate Standard

All Digital Signature Certificates issued by the Certifying Authorities shall conform *to ITU X.509 version 3 standard* as per Rule 6 and shall *inter alia* contain the following data, namely,—

(a) Serial Number (assigning of serial number to the Digital Signature Certificate by Certifying Authority to distinguish it from other certificate);

(b) Signature Algorithm Identifier (which identifies the algorithm used by Certifying Authority to sign the Digital Signature Certificate);

(c) Issuer Name (name of the Certifying Authority who issued the Digital Signature Certificate);

(d) Validity period of the Digital Signature Certificate;

(e) Name of the subscriber (whose public key the Certificate identifies); and

(f) Public Key Information of the subscriber.

8. Licensing of Certifying Authorities

(1) The following persons may apply for grant of a license to issue Digital Signature Certificates, namely,—

(a) an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession;

(b) a company having,—

(i) paid up capital of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees.

Provided that no company in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of its capital, shall be eligible for grant of license.

Provided further that in a case where the company has been registered under the Companies Act, 1956 (1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of license under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least 51 per cent of paid equity capital, being the Hindu Undivided Family, firm or company.

Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company.

Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity shares held in such company,—

(i) unless such a company acquires or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Controller;

(c) a firm having,—

(i) capital subscribed by all partners of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees.

Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of license.

Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of license under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of all of its partners.

Provided also that the partners referred to in the second proviso shall not include Non-resident Indian and foreign national.

Provided also that the partners of a firm referred to in the second proviso whose net worth has been determined on the basis of such partners, shall not sell or transfer its capital held in such firm,—

(i) unless such firm has acquired or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Controller;

(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation: For the purpose of this rule,—

(i) 'company' shall have the meaning assigned to it in clause 17 of Section 2 of the Income-tax Act, 1961 (43 of 1961);

(ii) 'firm', 'partner' and 'partnership' shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression 'partner' shall also include any person who, being a minor has been admitted to the benefits of partnership;

(iii) 'foreign company' shall have the meaning assigned to it in clause (23A) of Section 2 of the Income-tax Act, 1961 (43 of 1961);

(iv) 'net worth' shall have the meaning assigned to it in clause (ga) of sub-section (1) of Section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986);

(v) 'Non-resident' shall have the meaning assigned to it as in clause 26 of Section 2 of the Income-tax Act, 1961 (43 of 1961).

(2) The applicant being an individual, or a company, or a firm under sub-rule (1), shall [furnish a performance bond in the form of a banker's guarantee] from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of not less than [fifty lakhs] of rupees and the [performance bond in the form of banker's guarantee] shall remain valid for a period of six years from the date of its submission.

Provided that the company and firm referred to in the second proviso to clause (b) and the second proviso to clause (c) of sub-rule (1) shall [furnish a performance bond in the form of a banker's guarantee] for [one crore] of rupees:

Provided further that nothing in the first proviso shall apply to the company or firm after it has acquired or has its net worth of fifty crores of rupees.

(3) Without prejudice to any penalty which may be imposed or prosecution may be initiated for any offence under the Act or any other law for the time being in force, the [performance bond in the form banker's guarantee] may be invoked,—

(a) when the Controller has suspended the license under sub-section (2) of section 25 of the Act; or

(b) for payment of an offer of compensation made by the Controller; or

(c) for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority, its officers or employees; or

(d) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, if the Certifying Authority's license or operations is discontinued; or

(e) any other default made by the Certifying Authority in complying with the provisions of the Act or rules made thereunder.

Explanation: 'transfer of operation' shall have the meaning assigned to it in clause (47) of Section 2 of the Income-tax Act, 1961 (43 of 1961).

9. Location of the Facilities

The infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate as well as maintenance of Directories containing information about the status, and validity of Digital Signature Certificate shall be installed at any location in India.

10. Submission of Application

Every application for a licensed Certifying Authority shall be made to the Controller,—

(i) in the form given at Schedule-I; and

(ii) in such manner as the Controller may, from time to time, determine, supported by such documents and information as the Controller may require and it shall *inter alia* include,—

(a) a Certification Practice Statement (CPS);

(b) a statement including the procedures with respect to identification of the applicant;

(c) a statement for the purpose and scope of anticipated Digital Signature Certificate technology, management, or operations to be outsourced;

(d) certified copies of the business registration documents of Certifying Authority that intends to be licensed;

(e) a description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;

(f) an undertaking by the applicant that to its best knowledge and belief it can and will comply with the requirements of its Certification Practice Statement;

(g) an undertaking that the Certifying Authority's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of Digital Signature Certificate are audited by the auditors and approved by the Controller in accordance with rule 20;

(h) an undertaking to submit a performance bond or banker's guarantee in accordance with sub-rule (2) of Rule 8 within one month of Controller indicating his approval for the grant of license to operate as a Certifying Authority;

(i) any other information required by the Controller.

11. Fee

(1) The application for the grant of a license shall be accompanied by a non-refundable fee of twenty-five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(2) The application submitted to the Controller for renewal of Certifying Authority's license shall be accompanied by a non-refundable fee of five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(3) Fee or any part thereof shall not be refunded if the license is suspended or revoked during its validity period.

12. Cross Certification

(1) The licensed Certifying Authority shall have arrangement for cross certification with other licensed Certifying Authorities within India which shall be submitted to the Controller before the commencement of their operations as per Rule 20.

Provided that any dispute arising as a result of any such arrangement between the Certifying Authorities; or between Certifying Authorities or Certifying Authority and the Subscriber, shall be referred to the Controller for arbitration or resolution.

(2) The arrangement for Cross Certification by the licensed Certifying Authority with a Foreign Certifying Authority along with the application, shall be submitted to the Controller in such form and in such manner as may be provided in the regulations made by the Controller; and the licensed Certifying Authority shall not commence cross certification operations unless it has obtained the written or digital signature approval from the Controller.

13. Validity of License

(1) A license shall be valid for a period of five years from the date of its issue.

(2) The license shall not be transferable.

14. Suspension of License

(1) The Controller may by order suspend the license in accordance with the provisions contained in sub-section (2) of Section 25 of the Act.

(2) The license granted to the persons referred to in clauses (a) to (c) of sub-rule (1) of Rule 8 shall stand suspended when the performance bond in the form of banker's guarantee furnished] by such persons is invoked under sub-rule (2) of that rule.

15. Renewal of License

(1) The provisions of Rule 8 to Rule 13, shall apply in the case of an application for renewal of a license as it applies to a fresh application for licensed Certifying Authority.

(2) A Certifying Authority shall submit an application for the renewal of its license not less than forty-five days before the date of expiry of the period of validity of license.

(3) The application for renewal of license may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.

16. Issuance of License

(1) The Controller may, within four weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors, as he may deem fit, grant or renew the license or reject the application.

Provided that in exceptional circumstances and for reasons to be recorded in writing, the period of four weeks may be extended to such period, not exceeding eight weeks in all as the Controller may deem fit.

(2) If the application for licensed Certifying Authority is approved, the applicant shall,—

(a) submit a performance bond or furnish a banker's guarantee within one month from the date of such approval to the Controller in accordance with sub-rule (2) of Rule 8; and

(b) [give an undertaking to the Controller] binding himself to comply with the terms and conditions of the license and the provisions of the Act and the rules made thereunder.

17. Refusal of License

The Controller may refuse to grant or renew a license if,—

(i) the applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or

(ii) the applicant is in the course of being wound up or liquidated; or

(iii) a receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or

(iv) the applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or

(v) the Controller has invoked performance bond or banker's guarantee; or

(vi) a Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or

(vii) a Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with Rule 31; or

(viii) the audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation; or

(ix) a Certifying Authority fails to comply with the directions of the Controller.

18. Governing Laws

The Certification Practice Statement of the Certifying Authority shall comply with, and be governed by, the laws of the country.

19. Security Guidelines for Certifying Authorities

(1) The Certifying Authorities shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labelling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

(2) Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are given in Schedule-II and Schedule-III respectively.

(3) The Certifying Authority shall formulate its Information Technology and Security Policy for operation complying with these guidelines and submit it to the Controller before commencement of operation.

Provided that any change made by the Certifying Authority in the Information Technology and Security Policy shall be submitted by it within two weeks to the Controller.

20. Commencement of Operation by Licensed Certifying Authorities

The licensed Certifying Authority shall commence its commercial operation of generation and issue of Digital Signature only after,—

(a) it has confirmed to the Controller the adoption of Certification Practice Statement;

(b) it has generated its key pair, namely, private and corresponding public key, and submitted the public key to the Controller;

(c) the installed facilities and infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate have been audited by the accredited auditor in accordance with the provisions of rule 31; and

(d) it has submitted the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller.

21. Requirements Prior to Cessation as Certifying Authority

Before ceasing to act as a Certifying Authority, a Certifying Authority shall,—

(a) give notice to the Controller of its intention to cease acting as a Certifying Authority.

Provided that the notice shall be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of license;

(b) advertise sixty days before the expiry of license or ceasing to act as Certifying Authority, as the case may be, the intention in such daily