



CONTENTS

	PAGE
Operation Sindoor - Hon'ble Prime Minister of India	I-4
Shri Narendra Modi's address to the Nation	
Message from Hon'ble Justice Rajesh Bindal, Judge, Supreme Court of India	I-8
Message from Hon'ble Justice Anita Sumanth, Judge, High Court of Madras	I-11
Message from Hon'ble Justice Piyush Agrawal, Judge, High Court of Judicature at Allahabad	I-12
Message from Hon'ble Justice Abhay Ahuja, Judge, High Court of Bombay	I-13
Message from Hon'ble Justice Dr. Neela Gokhale, Judge, High Court of Bombay	I-14
Message from Justice Ms. Aarti Sathe, Judge, High Court of Bombay	I-15
Message by Justice C. V. Bhadang (Former Judge, Bombay High Court), President Income Tax Appellate Tribunal	I-16
From the Desk of the Editor	I-17
Message from the National President	I-21
Message from the Chairman and Co-chairman	I-23
All India Federation of Tax Practitioners (AIFTP) - 50 Years of celebration (Golden Jubilee)	I-26
About the Authors	I-30
Direct Tax Publication Committee	I-34
Chapter-Headings	I-35

CHAPTER 1

CYBERCRIME IN CONTEXT

Q.1	What is cybercrime?	2
------------	---------------------	---

	PAGE
Q.2 What makes cybercrime differ from traditional crime?	2
Q.3 Is there a universally accepted definition of cybercrime?	2
Q.4 What are some of the ways cybercrimes are commonly classified?	3
Q.5 Can you give an example of a cybercrime targeting an individual?	3
Q.6 What kind of cybercrimes target organizations?	3
Q.7 How are cybercrimes categorized by the Indian government?	3
Q.8 Why is it important to classify cybercrimes?	3
Q.9 Does the classification of a cybercrime affect its prosecution?	4
Q.10 Are all cyber-related activities considered cybercrime?	4
Q.11 What is a cyber-dependent crime?	4
Q.12 What are the examples of cyber-dependent crimes?	4
Q.13 What is a cyber-enabled crime?	5
Q.14 What are some common examples of cyber-enabled crimes?	5
Q.15 What is the key difference between cyber-dependent and cyber-enabled crimes	5
Q.16 What is the significance of distinguishing between these two categories?	5
Q.17 Does the Indian Legal system differentiate between these two categories?	5
Q.18 Could online harassment be categorised as a cyber-dependent crime or a cyber-enabled crime?	6
Q.19 What about phishing attacks?	6
Q.20 Do law enforcement agencies handle the investigation of these two categories in different ways? Do law enforcement agencies approach the investigation of these two categories differently?	6

	PAGE
Q.21 When did cybercrime first emerge?	6
Q.22 What were some of the initial forms of cybercrime?	7
Q.23 In what ways did the rise of the internet influence cybercrime? How did the rise of the internet impact cybercrime?	7
Q.24 What is the “infrastructure shift” in relation to cybercrime?	7
Q.25 In what ways did the advent of e-commerce impact cybercrime?	7
Q.26 How has mobile technology helped in the rise of cybercrime?	8
Q.27 In what ways has the emergence of the Dark Web impacted cybercrime?	8
Q.28 What does “Internet of Things” (IoT) mean in the context cybercrime?	8
Q.29 How have cybercriminals adapted to the developments in cybersecurity?	8
Q.30 What is the trend of “Crime-as-a-Service”?	8
Q.31 How did the COVID-19 pandemic influence cybercrime?	9
Q.32 What specific types of cybercrime saw a rise during the pandemic?	9
Q.33 In what ways did the transition to remote work affect cybersecurity?	9
Q.34 How did fear and uncertainty influence cybercrime throughout the pandemic?	9
Q.35 Were any new methods of cybercrime noted during the pandemic?	9
Q.36 What actions did governments and organizations take in response to the increase in cybercrime during the pandemic?	10
Q.37 Has the rise in digital dependence after COVID-19 maintained the elevated levels of cybercrime?	10

	PAGE
Q.38 What enduring effect has COVID-19 had on cybersecurity strategies?	10
Q.39 Did the use of digital payment platforms lead to an increase in cybercrimes?	10
Q.40 What is the primary law governing cybercrime in India?	11
Q.41 When was the Information Technology Act enacted?	11
Q.42 What was the purpose of the IT Act, 2000?	11
Q.43 What are some key offenses covered under the IT Act, 2000?	11
Q.44 Has the IT Act been amended, and if so, when was the major amendment?	12
Q.45 What are the powers of the Adjudicating Officer under the IT Act?	12
Q.46 Does the IT Act apply to offenses committed outside India?	12
Q.47 What function does the Cyber Appellate Tribunal serve under the IT Act?	12
Q.48 Is intermediary liability covered by the IT Act 2000?	13
Q.49 What are the penalties for cyber terrorism under the IT Act?	13
Q.50 What is the Bharatiya Nyaya Sanhita, 2023?	13
Q.51 When did the Bharatiya Nyaya Sanhita (BNS), 2023 take effect? When did the Bharatiya Nyaya Sanhita (BNS), 2023 come into effect?	14
Q.52 In what ways does the Bharatiya Nyaya Sanhita (BNS) influence the management of cybercrimes?	14
Q.53 Has the BNS established distinct classifications for cybercrimes?	14
Q.54 Can you provide an example of how the BNS is relevant to actions related to cyber activities?	14
Q.55 How does the BNS interact with the Information Technology Act?	15

	PAGE
Q.56 Does the BNS contain provisions against misinformation or fake news?	15
Q.57 Does the BNS extend to offenses committed outside India?	15
Q.58 How does the BNS make prosecution of cybercrimes more efficient?	15
Q.59 What is the function of the BNS within cybercrime framework?	16
Q.60 In what way is the Protection of Children from Sexual Offences (POCSO) Act, 2012, connected to cybercrime?	16
Q.61 Is the Consumer Protection Act, 2019 applicable to online frauds?	16
Q.62 What does Digital Personal Data Protection (DPDP) Act, 2023 entail?	17
Q.63 In what way does the DPDP Act help in fighting cybercrime?	17
Q.64 What consequences does the DPDP Act have for companies managing personal data?	17
Q.65 Is the Indian Copyright Act, 1957, applicable to cybercrime? Can the Indian Copyright Act, 1957, be applied to cybercrime?	17
Q.66 How does the Indian Telegraph Act of 1885 play role in cybercrime investigation?	18
Q.67 Are there any particular regulations in India aimed at combating money laundering via digital methods?	18
Q.68 How do these multiple laws interact in a cybercrime case?	18
Q.69 What is the importance of “due diligence” under various Indian laws concerning cybercrime?	18
Q.70 What is CERT-In and what is its role?	19
Q.71 What is the Indian Cybercrime Coordination Centre (I4C)?	19
Q.72 What are the key functions of I4C?	19

	PAGE
Q.73 Who are “intermediaries” in the context of cybercrime, as per the IT Act?	19
Q.74 What are the responsibilities of intermediaries in combating cybercrime?	20
Q.75 What is a Cyber Cell in the context of Indian policing?	20
Q.76 In what ways do CERT-In, I4C, and Cyber Cells work together?	20
Q.77 What role does the National Cybercrime Reporting Portal (cybercrime.gov.in) play?	20
Q.78 Are there additional institutional bodies involved in combating cybercrime in India?	20
Q.79 How does the government ensure coordination among these diverse entities?	21
Q.80 What is the Budapest Convention on Cybercrime?	21
Q.81 When was the Budapest Convention adopted?	21
Q.82 What are the main objectives of the Budapest Convention?	21
Q.83 Is India a signatory to the Budapest Convention?	22
Q.84 Why has India not ratified the Budapest Convention?	22
Q.85 Although India is not a signatory, does it conform to any principles of the Convention?	22
Q.86 In what ways does India engage in international cooperation without being a signatory?	22
Q.87 What does the “24/7 network” represent in the context of the Convention?	22
Q.88 What alternative international instruments exist for cybercrime cooperation?	23
Q.89 What significance do UN Resolutions hold in the fight against cybercrime?	23
Q.90 Has the UN developed its own comprehensive treaty on cybercrime?	23

	PAGE
Q.91 What are some regional pacts related to cybercrime?	23
Q.92 Is India involved in any regional pacts related to cybercrime?	23
Q.93 What is the aim of these regional pacts?	24
Q.94 In what ways do UN efforts vary from the Budapest Convention?	24
Q.95 What is the importance of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes?	24
Q.96 In what way UN resolutions impact national cybercrime policies?	24
Q.97 Are there any challenges in achieving a global consensus on cybercrime through the UN?	24
Q.98 What is the role of Interpol in international cybercrime cooperation	25
Q.99 In what does India participate in bilateral cooperation on cybercrime?	25
Q.100 Which countries engage with India in notable bilateral collaboration regarding cybercrime?	25
Q.101 What are MLATs (Mutual Legal Assistance Treaties)?	25
Q.102 How does India participate in multilateral forums for cybercrime?	25
Q.103 What are the benefits of multilateral cooperation in combating cybercrime?	26
Q.104 Does India collaborate with international law enforcement agencies like Europol or FBI on cybercrime?	26
Q.105 What are the challenges India faces in international cooperation on cybercrime?	26
Q.106 How does India contribute to global cybersecurity capacity building efforts?	26

	PAGE
Q.107 What is the role of diplomatic channels in India's international cybercrime efforts?	26
Q.108 Has India hosted any international conferences or initiatives on cybercrime?	27
Q.109 What are jurisdictional issues in cybercrime?	27
Q.110 Why is anonymity a significant challenge in cybercrime investigations	27
Q.111 How does the borderless nature of the internet contribute to jurisdictional problems?	27
Q.112 What is the "digital divide" in terms of law enforcement's capabilities?	27
Q.113 How do legal differences between countries create challenges?	28
Q.114 What is "forum shopping" in the context of cybercrime?	28
Q.115 How do encrypted communications pose a challenge to law enforcement?	28
Q.116 Is it possible to completely eliminate anonymity online?	28
Q.117 What is the "cloud computing" challenge for jurisdiction?	28
Q.118 How does the principle of "territoriality" conflict with cybercrime's nature?	29
Q.119 Why is cybercrime often underreported?	29
Q.120 What are the consequences of underreporting?	29
Q.121 What makes cybercrime enforcement difficult?	29
Q.122 Is there a shortage of skilled cyber investigators in India?	29
Q.123 How do "evidential challenges" impact cybercrime prosecution?	30
Q.124 What is the role of public-private partnerships in overcoming enforcement difficulties?	30
Q.125 How does the rapid pace of technological change affect enforcement?	30

	PAGE
Q.126 What challenges do victims face in seeking justice for cybercrimes?	30
Q.127 How can international collaboration help address enforcement difficulties?	30
Q.128 What is the “attribution problem” in cybercrime?	31
Q.129 How do cybercriminals’ techniques constantly evolve?	31
Q.130 What is “Ransomware-as-a-Service” (RaaS)?	31
Q.131 What is “phishing” and how has it evolved?	31
Q.132 How are AI and Machine Learning being used by cybercriminals?	31
Q.133 What is the threat posed by “deepfakes” in cybercrime?	32
Q.134 How does the rise of cryptocurrencies impact cybercrime?	32
Q.135 What is the concept of “supply chain attacks”?	32
Q.136 How are “Internet of Things” (IoT) devices being exploited by criminals?	32
Q.137 What is “social engineering” and why is it so effective?	32
Q.138 How are “zero-day exploits” a challenge for cybersecurity?	32
Q.139 Why is public awareness crucial in combating cybercrime?	33
Q.140 What are common legal knowledge gaps among the general public regarding cybercrime?	33
Q.141 How does legal literacy empower individuals against cybercrime?	33
Q.142 What initiatives can bridge these legal knowledge gaps?	33
Q.143 How can schools and universities contribute to legal literacy on cybercrime?	34
Q.144 What is the importance of knowing about reporting mechanisms (<i>e.g.</i> , cybercrime.gov.in)?	34

	PAGE
Q.145 How does understanding data protection laws benefit individuals	34
Q.146 What is the role of the media in raising public awareness about cybercrime?	34
Q.147 How can simplified Q&A formats help in promoting legal literacy?	34
Q.148 What is the long-term impact of increased legal literacy on cybercrime rates?	35
Q.149 What is the role of lawyers in combating cybercrime?	35
Q.150 How do Chartered Accountants (CAs) contribute to cybercrime prevention?	35
Q.151 What are the responsibilities of Compliance Officers in cybersecurity?	35
Q.152 How do these professionals help businesses navigate the legal complexities of cybercrime?	35
Q.153 What is the importance of legal counsel for victims of cybercrime?	36
Q.154 How do Chartered Accountants assist in cases of cyber-enabled financial fraud?	36
Q.155 What is the significance of “privacy by design” and “security by design” from a legal perspective?	36
Q.156 How do lawyers and compliance officers ensure an organization’s adherence to the DPDP Act?	36
Q.157 What training or specialization is required for these professionals in cyber law?	36
Q.158 How can these professionals help in reducing the overall impact of cybercrime on society?	37

CHAPTER 2

DIGITAL FINANCIAL FRAUDS

Q.159 What is Phishing?	41
Q.160 How do Phishing attacks typically work?	42

	PAGE
Q.161 What are the common signs of a Phishing attempt?	42
Q.162 What is Vishing?	43
Q.163 How do Vishing scams usually work?	43
Q.164 What are the common signs of a Vishing attempt?	44
Q.165 What are QR Code Frauds?	44
Q.166 How do QR Code scams typically operate?	44
Q.167 What are the key red flags for QR Code Frauds?	45
Q.168 Can scanning a malicious QR code harm my smartphone?	46
Q.169 What is “Social Engineering” in the context of these frauds?	46
Q.170 Are there any specific scams in India that use these methods?	47
Q.171 Why are these types of frauds so common?	47
Q.172 What is a Remote Access Scam?	48
Q.173 How do Remote Access Scams typically work?	48
Q.174 What are the warning signs of a Remote Access Scam?	48
Q.175 What is OTP Hijacking?	49
Q.176 How do OTP Hijacking scams typically work?	49
Q.177 What is “SIM Swap Fraud” and how does it relate to OTP hijacking?	50
Q.178 What are the signs that my OTP might be hijacked or my SIM swapped?	50
Q.179 Are SMS OTPs becoming less secure?	51
Q.180 What is an “OTP Bot”?	51
Q.181 How can malware lead to OTP hijacking?	52
Q.182 Why is it so important to be careful with unsolicited requests for information?	52
Q.183 What role does “human weakness” play in OTP hijacking?	53

	PAGE
Q.184 What is Section 66C of the IT Act?	55
Q.185 What is the punishment for identity theft under section 66C?	56
Q.186 Can you give examples of identity theft relevant to financial fraud?	56
Q.187 What is Section 66D of the IT Act?	56
Q.188 What is the punishment for cheating by personation under section 66D?	56
Q.189 Can you give examples of cheating by personation relevant to financial fraud?	57
Q.190 What is the difference between identity theft (Section 66C) and cheating by personation (Section 66D)?	57
Q.191 Do these sections only apply to individuals, or can they apply to organized groups?	58
Q.192 Are there other sections of the IT Act relevant to cyber financial fraud?	58
Q.193 Is it important to report these crimes under the IT Act?	58
Q.194 What is “Cheating” under section 318 of the BNS?	59
Q.195 How does Section 318 BNS apply to digital financial frauds?	59
Q.196 What is the punishment for cheating under section 318 BNS?	60
Q.197 What is “Forgery” under section 336 of the BNS?	60
Q.198 What does “digital forgery” mean under BNS?	61
Q.199 How does Section 336 BNS apply to digital financial frauds?	61
Q.200 What is the punishment for forgery under section 336 BNS?	62
Q.201 What elements must be proven to establish forgery under BNS?	62
Q.202 Why is the BNS considered an important update for combating digital fraud?	62

	PAGE
Q.203 Can these sections be used in conjunction with the IT Act?	63
Q.204 What are the RBI guidelines on customer protection in unauthorized electronic transactions?	64
Q.205 What is “zero liability” for customers in case of unauthorized transactions?	65
Q.206 What if I report the fraud after three days but within seven working days?	65
Q.207 What happens if I report the fraud after seven working days?	65
Q.208 How quickly must banks resolve fraud complaints?	66
Q.209 What is “shadow reversal” and why is it important?	66
Q.210 What are the RBI’s new draft guidelines (2025) for digital banking and fraud protection?	66
Q.211 What is the Financial Fraud Risk Indicator (FRI) and how does it help?	67
Q.212 What is the Mobile Number Revocation List (MNRL) and its purpose?	67
Q.213 How does RBI promote customer awareness about fraud?	68
Q.214 What is the bank’s responsibility if I am a victim of fraud?	68
Q.215 Can banks force me to use digital banking?	68
Q.216 Why is timely reporting of fraud to the bank so important?	69
Q.217 Why are court cases important in understanding digital financial fraud?	70
Q.218 What is the “Digital Arrest” scam, and what was a recent landmark judgment related to it?	70
Q.219 Under which laws were the convicts in the “Digital Arrest” case punished?	71

	PAGE
Q.220 What was the outcome of the Kerala High Court case involving Bank of Baroda and forged cheques?	71
Q.221 What was the key legal principle established by the Kerala High Court in the Bank of Baroda case?	72
Q.222 What did the Allahabad High Court rule regarding the burden of proof in unauthorized online transactions?	72
Q.223 Did the Allahabad High Court always rule in favour of the customer in such cases?	73
Q.224 What is the significance of courts labeling cybercrimes as “economic terrorism”?	73
Q.225 How do these judgments impact victims of digital financial fraud?	73
Q.226 Do these cases suggest a trend in how Indian courts are handling cybercrime?	74
Q.227 What is the National Cyber Crime Reporting Portal (NCRP)?	75
Q.228 How do I file a complaint on the NCRP?	75
Q.229 What is the National Cyber Crime Reporting Helpline number?	76
Q.230 What should I do immediately if I realize I’ve been a victim of financial fraud?	76
Q.231 What is CERT-In’s role in cyber financial fraud?	76
Q.232 How can CERT-In help me if I am a victim?	77
Q.233 What are “Bank Helpdesks” and how do I use them?	77
Q.234 Why is providing evidence important when reporting a fraud?	78
Q.235 What is the Citizen Financial Cyber Fraud Reporting and Management System (CFC-FRMS)?	78
Q.236 Can I report a fraudulent website or app?	78

	PAGE
Q.237 What is the role of local police in cyber financial fraud cases?	79
Q.238 Is there a time limit for reporting fraud to my bank?	79
Q.239 What are the fundamental “Safe Banking” practices recommended by RBI and banks?	80
Q.240 How can I protect myself from Phishing and Vishing attempts?	80
Q.241 What specific precautions should I take for UPI and QR code payments?	81
Q.242 How can I prevent Remote Access and OTP Hijacking scams?	81
Q.243 What is “Juice Jacking” and how can I avoid it?	81
Q.244 What are the RBI’s efforts in raising public awareness about financial frauds?	81
Q.245 What is the “Sanchar Saathi” portal and how does it help?	82
Q.246 How do dedicated phone number series help prevent fraud?	82
Q.247 Why is it important to use strong, unique passwords for different accounts?	82
Q.248 What is “Card Skimming” and how can I protect my debit/credit cards?	83
Q.249 Why should I be cautious about public Wi-Fi networks?	83
Q.250 What role does “Digital Intelligence Platform (DIP)” play in preventing fraud?	83
Q.251 What is “MuleHunter.AI” and how does RBI plan to use it?	83
Q.252 Why are regular software updates important for security?	84
Q.253 What is the overall goal of these prevention efforts?	84

CHAPTER 3

IDENTITY-BASED CYBER OFFENCES

Q.254	What is SIM swap fraud?	87
Q.255	How do fraudsters trick telecom providers into performing a SIM swap?	87
Q.256	What are the common signs that my SIM card might have been swapped?	88
Q.257	What immediate dangers does SIM swapping pose to me?	88
Q.258	How does Mobile Number Portability (MNP) relate to this fraud?	89
Q.259	What techniques do fraudsters use to gather information for SIM swaps?	89
Q.260	Can SIM swap fraud lead to unauthorized bank transactions?	89
Q.261	Are there any specific measures taken by Indian regulators to prevent SIM swap fraud?	90
Q.262	Why is relying solely on SMS-based Two-Factor Authentication (2FA) risky against SIM swap fraud?	90
Q.263	What role does the human element play in SIM swap fraud?	90
Q.264	What is a “port-out scam”?	91
Q.265	What should I do if I suspect my phone service has suddenly stopped working without explanation?	91
Q.266	What are deepfakes and how are they used in cybercrime?	91
Q.267	Can you provide examples of deepfake incidents in India?	92
Q.268	What is “spoofing,” particularly email spoofing?	92
Q.269	How do cybercriminals carry out email spoofing attacks?	92

	PAGE
Q.270 What is the difference between email spoofing and phishing?	93
Q.271 What is identity theft in simple terms?	93
Q.272 What are the different types of identity theft?	93
Q.273 How do criminals typically obtain personal information for identity theft?	94
Q.274 What is the “PAN 2.0 scam” and why is it dangerous?	94
Q.275 Why are deepfakes considered a significant leap in cybercrime compared to traditional spoofing?	95
Q.276 What is the “media trust crisis” caused by deepfakes?	95
Q.277 Why is personal identity information considered the “ultimate currency” in cybercrime?	95
Q.278 What is “phishing” in the context of identity theft?	96
Q.279 How can individuals protect themselves from phishing scams like the “PAN 2.0 scam”?	96
Q.280 What does Section 66C of the Information Technology (IT) Act, 2000, address?	97
Q.281 What is the punishment for identity theft under IT Act Section 66C?	97
Q.282 What does Section 72 of the IT Act, 2000, cover?	97
Q.283 What are the penalties for breaching confidentiality and privacy under IT Act Section 72?	98
Q.284 How do Sections 66C and 72 relate to identity-based cyber offenses?	98
Q.285 What is the primary purpose of the Information Technology Act, 2000, in relation to digital identity?	98
Q.286 Does the IT Act cover both physical and digital forms of identity theft?	99

	PAGE
Q.287 What does “fraudulently or dishonestly” mean in the context of Section 66C?	99
Q.288 Can a single cyber incident lead to charges under both Section 66C and Section 72 of the IT Act?	99
Q.289 What kind of information is protected under Section 72 of the IT Act?	99
Q.290 What is the Bharatiya Nyaya Sanhita (BNS), 2023, and how does it relate to cybercrime?	100
Q.291 How does BNS Section 336 define “forgery”?	100
Q.292 What are the different levels of punishment for forgery under BNS Section 336?	100
Q.293 What does “cheating by personation” mean under BNS Section 319?	101
Q.294 What is the punishment for cheating by personation under BNS?	101
Q.295 How does BNS address digital forms of forgery and personation?	101
Q.296 What was the Indian Penal Code (IPC) and why was it replaced by the BNS?	102
Q.297 What elements must be proven to establish an offense under BNS Section 336 (Forgery)?	102
Q.298 Is forgery under BNS Section 336(2) a bailable offense?	102
Q.299 Is forgery with intent to cheat under BNS Section 336(3) a bailable offense?	103
Q.300 Does “cheating by personation” under BNS Section 319 apply only to real people?	103
Q.301 How does the BNS’s definition of “Document” impact digital crimes?	103
Q.302 What is the role of the Telecom Regulatory Authority of India (TRAI) in preventing telecom fraud?	104
Q.303 What key guidelines has TRAI issued to prevent SIM porting fraud?	104

	PAGE
Q.304 What is the Digital Consent Acquisition (DCA) pilot launched by TRAI?	105
Q.305 How does the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, protect individual identity information?	105
Q.306 What are the penalties for unauthorized use or disclosure of Aadhaar data under the Aadhaar Act?	105
Q.307 What is the Central Identities Data Repository (CIDR) mentioned in the Aadhaar Act?	106
Q.308 What is the primary objective of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016?	106
Q.309 Does UIDAI collect sensitive personal information like religion or caste?	106
Q.310 How does UIDAI respond to requests for identity verification?	107
Q.311 What is the penalty for tampering with data in the Central Identities Data Repository (CIDR) under the Aadhaar Act?	107
Q.312 What is the 'Chakshu' platform introduced by the Department of Telecommunications (DoT)?	107
Q.313 How does TRAI's Digital Consent Acquisition (DCA) pilot enhance consumer autonomy?	107
Q.314 Can you provide examples of real-world Aadhaar-linked financial fraud cases in India?	108
Q.315 How do phishing scams exploit Aadhaar and PAN details?	108
Q.316 What was the "PAN 2.0 scam"?	109
Q.317 How did the Mumbai ATM skimming scam operate?	109
Q.318 What legal recourse did victims of Aadhaar misuse find in cases like the Bombay High Court ruling?	109

	PAGE
Q.319 Can Aadhaar misuse lead to victims being implicated in major financial crimes?	110
Q.320 How does identity theft linked to Aadhaar often cascade into other frauds?	110
Q.321 What are the broader consequences of Aadhaar misuse beyond direct financial loss?	111
Q.322 Why is prompt action critical for victims of Aadhaar-linked fraud?	111
Q.323 What is the significance of the Bombay High Court's ruling regarding Aadhaar fraud?	111
Q.324 What is the role of phishing in Aadhaar-linked financial breaches?	111
Q.325 What immediate steps should I take if I suspect my SIM card has been swapped?	112
Q.326 How can I block a lost or stolen mobile phone in India?	112
Q.327 What are the official channels for reporting Aadhaar-related fraud to UIDAI?	113
Q.328 How does UIDAI assist individuals who have been victims of Aadhaar fraud?	113
Q.329 What is the 'Chakshu' platform?	114
Q.330 Why is it important to act quickly if you suspect SIM swap fraud?	114
Q.331 What is the National Cyber Crime Reporting Portal?	114
Q.332 Can a blocked phone's IMEI be unblocked if the phone is recovered?	115
Q.333 What is the UIDAI toll-free helpline number and its availability?	115
Q.334 What kind of documentation should a victim of SIM swap fraud retain?	115
Q.335 How does the CEIR portal help in combating mobile phone theft and fraud?	115
Q.336 What is the significance of the government establishing centralized platforms for reporting cybercrimes?	116

	PAGE
Q.337 What are biometric locks and how do they enhance digital security?	116
Q.338 How do biometric authentication systems work to prevent identity theft?	117
Q.339 Are biometric authentication systems being used for digital transactions in India?	117
Q.340 What is an Aadhaar Virtual ID (VID)?	117
Q.341 How do I generate an Aadhaar Virtual ID?	118
Q.342 What are the benefits of using an Aadhaar Virtual ID?	118
Q.343 Is a Virtual ID permanent?	119
Q.344 What is “liveness detection” in biometric systems?	119
Q.345 How does biometric authentication align with RBI’s Two-Factor Authentication (2FA) guidelines?	119
Q.346 Can Aadhaar Virtual IDs be used for linking Aadhaar with other services like PAN or bank accounts?	120
Q.347 What are some examples of biometric locks available in India?	120
Q.348 How does using a Virtual ID enhance privacy during e-KYC verification?	120
Q.349 What are consent-based authentication systems?	121
Q.350 How does India’s Digital Personal Data Protection (DPDP) Act, 2023, relate to consent-based data sharing?	121
Q.351 What are “Consent Managers” under the DPDP Act?	121
Q.352 How do consent-based systems enhance data privacy and control for individuals?	122
Q.353 Can consent for data sharing be withdrawn?	122
Q.354 What is the significance of the Digital Consent Acquisition (DCA) pilot in India?	122

	PAGE
Q.355 What are the core principles of a data protection framework in India, as outlined in the White Paper on Data Protection?	123
Q.356 What does “informed consent” mean under India’s data protection framework?	123
Q.357 What is the role of “data fiduciaries” under the DPDP Act?	123
Q.358 How does the DPDP Act ensure transparency in data processing?	124
Q.359 What is the significance of the DPDP Act aligning with the electronic consent artefact design in the AA (Account Aggregator) ecosystem?	124
Q.360 How do Consent Managers provide a “single point of contact” for data principals?	124

CHAPTER 4

E-COMMERCE AND PLATFORM FRAUD

Q.361 How did technological boom paved way for creation of Internet?	126
Q.362 What is e-commerce?	128
Q.363 What is Platform-based e-commerce and its types?	130
Q.364 What are various types of e-commerce platform fraud?	132
Q.365 Are there legal framework(s) provided by the Indian Statutes to address e-commerce platform fraud?	137
Q.366 What specific remedies are provided in the Information Technology Act and its subsequent amendments?	138
Q.367 Is Consumer Protection Act, 1986, adequate to cater to e-commerce platform frauds?	141
Q.368 Does the new data protection statute mandate any e-commerce compliance?	144

	PAGE
Q.369 Is e-commerce taxed?	144
Q.370 Conclusion and suggestions	145

CHAPTER 5

INCOME TAX RELATED CYBER CRIMES AND LOSSES

Q.371 Discuss the impact of digitalization, as to the tax compliance?	150
Q.372 What are the challenges of digitalization in the tax system?	151
Q.373 Whether the digital challenges in tax compliance can be overcome by the taxpayer and authorities as well?	151
Q.374 In the present context, when we are standing at the cross roads of law, business and technology, discuss the significance of the cyber loss, if occurred, how to be dealt as per the provisions of Income Tax Act?	152
Q.375 What are the concerns that may be encountered in the event of lack of uncertainty or predictability of the disputes in respect of the claim of cyber losses; under the provisions of Income-Tax Act 1961?	154
Q.376 The principles of natural justice, being the soul of administration of justice, need to be adhered to for considering the allowability of Cyber loss – Discuss	155
Q.377 In the context of allowability of cyber loss occurred, in the event the substantial justice and technical consideration are pitted against each other, the cause of substantial justice deserves to be preferred – Discuss.	157
Q.378 Whether the cyber loss incurred can be treated as trading loss in commercial sense?	158
Q.379 Assessee an Individual had invested in shares. The shares held in a corporate entity have been sold and resulted in long-term capital	159

	PAGE
gain. The proceeds were kept in his bank account. Due to cybercrime, he lost all the money in the bank. The recovery appeared to be remote. Can the loss occurred due to cybercrime be claimed as capital loss, considering that there was long-term capital gains, which is liable to be taxed? Further the amount in the bank being lost due to cyber fraud can the same be claimed as a capital loss, and if so against the resulted long-term capital gains, on the sale of shares?	
Q.380 Once cyber loss has been established to be the loss on embezzlement, the year in which the deduction is to be claimed has its own eventualities – Discuss	162
Q.381 Explain the concept of allowability to business loss as per the provisions of Income Tax Act 1961?	164
Q.382 Explain the concept of Digital Evidence and its applicability to the provisions of Income Tax Act 1961	165
Q.383 State as to how the Digital Evidence in the content of electronic records is to be considered in the applicability of cases covered under Search Action u/s 132 of the Income Tax Act 1961	167
Q.384 State the contents of digital evidence investigation manual of Central Board of Direct Taxes	169
Q.385 In the context that pen drive and other electronic records are found and seized during Search Action discuss the evidentiary value of the same	174
Q.386 Whether revenue is entitled to demand unrestricted access to acquire electronic records present in laptops pertaining to third parties unconnected with person searched?	175

	PAGE
Q.387 Is it justifiable to claim the deduction of bad debt, as business loss? If claimed so is the deduction allowable as business loss?	176
Q.388 State the nature of cyber crimes in relation to Income Tax Act 1961	177
Q.389 Is there any scope for prevention or availability of any solutions for the averruncate or ward off or uproot, such cyber crimes?	178
Q.390 Is there any legal protection, and what is the scope for punishment under law?	179
Q.391 In the present process of digital revolution, era of digital economy, considering the explosion of data state the risks, and is there any protection?	180
Q.392 In the context of the claim for deduction of cyber losses, as per the provisions of Income Tax Act 1961, state the arguments that should meet the test of law	181
Q.393 Whether banks or lenders can claim deduction of cyber fraud losses as business loss either under section 28 or under section 37(1) of the Income Tax Act 1961. (Sections 26 and 31 of Income Tax Act 2025(2))	182
Q.394 Whether the whatsapp chats, on standalone basis, can be considered as valid evidence to support the addition by Assessing Officer?	183
Q.395 The electronic records by way of secondary evidence are not admissible in evidence unless the requirements of sections 61 & 63 of "THE BHARATIYA SAKSHYA ADHINIYAM 2023" (Formerly section 65B of Indian Evidence Act (1872)) are satisfied – Discuss	184
Q.396 What shall be the evidentiary value of the data on a pen drive seized from the cashier, where no evidence produced regarding the computer from which the pen drive was copied?	187

	PAGE
Q.397 Whether the document containing the details noticed in the smart phone of an assessee or employee during Search Action can be of evidentiary value, without corroborating such document with some other credible evidence?	189
Q.398 In the context of untested/unverified document, the print out taken from the computer back up of a third party, during Search Action is it justifiable to demonstrate, that payment has been received as mentioned in the said document without any other corroborative evidence	190
Q.399 Cyber security remains as an essential element for strategic business value – Discuss.	192
Q.400 In the context of money lost in crypto scam	193
Q.401 In the context of allowability of cyber loss, in the year in which the loss occurred, in the event the loss has been subsequently recovered and thereby credited in the books of account, discuss the taxability as per the provisions of Income Tax Act 1961	195
Q.402 The consequences of “financial embezzlement”, when require consideration, and to be dealt with, the powers should be exercised judiciously under the Income Tax Act 1961 – Discuss.	196

CHAPTER 6

GOODS AND SERVICES TAX RELATED CYBERCRIMES IN INDIA

Q.403 What are tax-related cybercrimes?	203
Q.404 What constitutes a cybercrime in the context of the Income-tax Act?	203
Q.405 What constitutes a cybercrime in the context of GST?	204
Q.406 What are the broader implications of GST cybercrimes?	205
Q.407 How are such frauds detected by the authorities?	206

	PAGE
Q.408 How do the Income-tax Department (CBDT) and the GST Department (CBIC) coordinate in cases of cyber-enabled tax frauds?	208
Q.409 What immediate actions are taken by tax authorities once such frauds are detected?	210
Q.410 What responsibilities do tax authorities and professionals have as Data Fiduciaries under the Digital Personal Data Protection Act, 2023?	212
Q.411 How do fake invoice scams work?	214
Q.412 How are fake invoice frauds linked to money laundering under the Prevention of Money Laundering Act, 2002 (PMLA)?	216
Q.413 How do authorities detect large fake-invoice schemes (technical side)?	217
Q.414 What are the specific criminal offences and corresponding punishments, including the monetary thresholds for imprisonment, prescribed under section 132 of the CGST Act, 2017?	218
Q.415 What are the essential legal and procedural criteria that determine when GST authorities must initiate criminal prosecution under Section 132 (Punishment for Offences) instead of merely levying a civil penalty/demand under section 122 (Penalty for Certain Offences) of the CGST Act?	220
Q.416 Can a person be arrested under GST laws and/or the Income-tax Act, and what legal remedies are available to challenge or prevent such arrest?	221
Q.417 What is Circular No. 171/03/2022-GST (CBIC) and why does it matter?	223
Q.418 In practical terms, how should GST officers and taxpayers act differently after Circular 171/03/2022-GST dated July 6, 2022?	225

	PAGE
Q.419 What is the Directorate General of Systems & Data Management (DG Systems & DM) and what role does it play in cyber security and prevention within the Central Board of Indirect Taxes and Customs (CBIC)?	227
Q.420 What are some real instances of cybercrime and fraud under GST?	229
Q.421 If a purchaser received invoices from a supplier later found to be fake, will the purchaser automatically face prosecution?	232
Q.422 What procedural safeguards/actions should a taxpayer take on receiving an SCN alleging fake invoices?	233
Q.423 Can victims of identity theft (GST registrations created using stolen PAN/Aadhaar) get relief?	233
Q.424 What should one do if they become a victim of GST-related cybercrime?	233
Q.425 How can taxpayers safeguard themselves?	234
Q.426 What is the government's approach to prevent such frauds?	234
Q.427 What is the way forward?	234

CHAPTER 7

NAVIGATING THE MINEFIELD OF MODERN EMPLOYMENT FRAUD

Q.428 Which are the most prevalent job frauds now?	258
Q.429 What are the largest red flags of a job scam?	259
Q.430 What can I do to identify an AI based deep fake in a video interview?	259
Q.431 What should I do to distinguish between a veritable and a bogus offer letter?	260
Q.432 What are the primary legislations in India that combat job scams?	260
Q.433 I've been scammed! What are the three things I need to do first?	261

	PAGE
Q.434 What happens to filing of formal police complaint in India?	261
Q.435 I have fallen into a trap of a fake foreign job opportunity and have gotten stuck in a foreign land. Who can help?	261
Q.436 What do I do to make sure that he is a legitimate company?	262
Q.437 How can firms prevent their brand being involved in frauds?	262

CHAPTER 8

MONEY LAUNDERING & CYBERCRIME UNDER PMLA

Q.438 How is Money Laundering committed through Cyber Crimes?	273
Q.439 What are the mechanisms put in place by the Government in order to detect money laundering through Virtual Digital Assets?	274
Q.440 What are the most common terms under at the nexus of money laundering and cyber-crime in the Indian context?	275
Q.441 What are the legal provisions under the Prevention of Money Laundering Act, 2002, for in relation to cybercrimes?	281
Q.442 What is the process of attachment under PMLA?	287
Q.443 What is the provision for Bail under PMLA?	291
Q.444 Who are reporting entities under PMLA? What are the statutory obligations of a reporting entity?	291
Q.445 What are the obligations of Chartered Accountants under PMLA, 2002 since they are aware about certain business activities of the their clients?	296
Q.446 What are suspicious transactions? What are the obligations of a reporting entity in terms of suspicious transactions?	298

	PAGE
Q.447 Does the PMLA provide for multi-agency coordination?	299
Q.448 What are a few examples of recent cases that had elements of being useful to understand the nexus between money laundering and cybercrime?	300

CHAPTER 9

RESPONSE PATHWAYS AND REDRESSAL TOOLKIT

Q.449 What are the various types of cybercrimes?	303
Q.450 What are the various elements of a crime in the case of a cyber offence	304
Q.451 What are various steps in cybercrime investigations?	305
Q.452 What are the standards of evidence and the internet in various jurisdictions?	305
Q.453 What are various types of Cyber/Computer-generated Evidence?	306
Q.454 Does Bharatiya Sakshya Adhiniyam (BSA), 2023 include provisions to encompass electronic evidence to thwart cybercrimes?	310
Q.455 Conclusion and suggestions	313

CHAPTER 10

DUBAI, UAE Q&A GUIDE ON FINANCIAL CRIME AND DATA PROTECTION UNDER UAE LAW

Q.456 What is the main purpose of Federal Decree-Law No. (34) of 2021?	315
Q.457 What is Information Technology (IT)?	316
Q.458 What is Electronic Information?	316
Q.459 How does the law define “Data” and its categories?	316
Q.460 What is a cyberattack?	317
Q.461 What is Encryption?	317
Q.462 What does “Electronic” mean in this law?	317

	PAGE
Q.463 What is digital evidence?	317
Q.464 What is Hacking?	317
Q.465 What is leakage?	318
Q.466 How does the law define “illegal content”?	318
Q.467 How does the law deal with fraud using credit cards or e-payment tools?	318
Q.468 How are personal data breaches punished?	318
Q.469 Is spreading rumors or false news online a criminal offence?	318
Q.470 How does UAE deals with creating fake websites or online accounts?	319
Q.471 What enforcement powers do authorities have against illegal content?	319
Q.472 Are there offences related to privacy violations and secret disclosure?	319
Q.473 What special provisions exist for crimes against UAE national security?	319
Q.474 Can cybercrime cases be settled amicably?	320
Q.475 Do UAE Courts have jurisdiction over a website or over a cybercrime committed by a person outside the UAE?	320
Q.476 What types of financial crimes does the law cover?	321
Q.477 How does the law treat digital/virtual currencies?	321
Q.478 What is e-payment instrument fraud?	321
Q.479 How does the law treat gambling promotion?	321
Q.480 How does the law define cyber extortion or blackmail?	321
Q.481 How does the law treat internet fraud?	322
Q.482 What are Illicit Financial Flows (IFFs) and how are they linked to money laundering?	322
Q.483 How is unauthorized fundraising regulated?	322
Q.484 Can legal entities be liable for financial crimes?	322

	PAGE
Q.485 What additional measures can courts impose besides fines and imprisonment?	323
Q.486 How much time frame is taken in UAE to file a criminal complaint with the court ?	323
Q.487 What measures can the court impose besides imprisonment and fines?	324
Q.488 What are the core compliance risks under this law for financial institutions?	325
Q.489 What due diligence is required for detecting illicit financial flows?	325
Q.490 How should banks and PSPs mitigate e-payment instrument fraud risk?	325
Q.491 How to ensure compliance when dealing with virtual or digital currencies?	325
Q.492 What compliance measures prevent unauthorized fundraising?	325
Q.493 How should compliance teams respond to cyber extortion cases involving customers?	326
Q.494 What are the corporate liability obligations (Art. 58)?	326
Q.495 What reporting duties apply for illegal online content linked to financial crime?	326
Q.496 What are necessary documents required for the purpose of the compliance for regulatory?	326
Q.497 What is the principal objective of the PDPL in the context of financial transactions?	326
Q.498 What is Personal Data under the PDPL?	327
Q.499 What constitutes Personal Data for financial sector purposes?	328
Q.500 Does the PDPL apply to all financial institutions?	328
Q.501 When may financial personal data be processed without consent?	328
Q.502 What is a Financial Data Controller?	329

	PAGE
Q.503 What are the core obligations of financial data controllers?	329
Q.504 What is a Processor in the financial context?	330
Q.505 What obligations do Processors have in financial services?	330
Q.506 How is cross-border transfer of financial personal data regulated?	331
Q.507 What breach notification duties apply to the financial sector?	331
Q.508 What rights do Data Subjects have over their financial personal data?	332
Q.509 What are the penalties for non-compliance in the financial sector?	333
Q.510 What are the steps for reporting financial crime in UAE?	334
Q.511 What are the common types of consumer Fraud and scams in UAE ?	334
Q.512 How To Report Fraud & Scams in UAE?	335
Q.513 What are key punishment including penalties for committing cybercrimes related to finance in UAE?	336
Q.514 How to initiate Financial Crime before the courts in United Arab Emirates ?	336
Q.515 What is the legal basis for collecting and processing client data under Anti Money Laundering Law (AML laws)?	338
Q.516 What types of personal data can be collected for AML compliance?	338
Q.517 Can sensitive or special category data be processed for AML purposes?	339
Q.518 Is client consent required for AML-related processing?	339
Q.519 Can personal data be shared with regulators or Financial Intelligence Units (FIUs)?	339

	PAGE
Q.520 How long can AML data be retained in accordance to the ADGM Data Protection Regulation?	340
Q.521 What safeguards must be applied when handling AML data?	340
Q.522 How should data breaches involving AML information be handled?	340
Q.523 Are automated AML screening systems compliant?	341
Q.524 What are the penalties for non-compliance?	341
Q.525 How do UAE data privacy laws interact with AML/CTF compliance for virtual assets?	342
Q.526 Which kinds of personal data are at risk for a VASPs entities?	342
Q.527 Whether VASPs entities in the UAE are permitted to share client data with regulators or any international regulatory authority?	342
Q.528 How does the UAE ensure the security of personal data collected for financial crime compliance?	343
Q.529 What are the retention and deletion obligations and compliance for data collected relating to financial crime?	343
Q.530 What are the penalties for mishandling personal data in the virtual asset sector?	343
Q.531 How can VASPs prevent financial crime related to the data privacy obligations?	343
Q.532 What is the legal basis for processing personal data for AML purposes under DIFC Law?	344
Q.533 Is client consent required for processing data for AML compliance?	344
Q.534 What categories of personal data may be processed for AML purposes?	344
Q.535 How long should financial institutions retain personal data collected for AML purposes?	345

	PAGE
Q.536 Can personal data collected be used for other activities such as marketing?	345
Q.537 How can financial institutions transfer AML-related data outside the DIFC?	345
Q.538 What are the obligations in case of breach involving AML information?	346
Q.539 What internal measures should financial institutions adopt to ensure compliance with both AML and data protection obligations?	346
Q.540 What penalties apply for non-compliance with DIFC data protection related to AML?	346
Q.541 How do the DIFC Data Protection principles align with AML compliance requirements?	347

CHAPTER 11

CYBER FRAUD VICTIM CHECKLIST: IMMEDIATE ACTIONS

Specimen Letter	353
Important Case Laws	359
Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions	362
Master Circular on Credit Card, Debit Card and Rupee Denominated Card	369
Customer Service - Reversal of Erroneous Debits Arising on Fraudulent or other Transactions	372
Frauds in Banks	374
Frauds in Banks - Monitoring of Deposit Accounts	375
List of Cases	377
Subject Index	383