

Contents

Table of cases	xvii
Table of legislation	xix
Abbreviations	xxiii
List of contributors	xxvii
Glossary	xxxi
<hr/>	
1 Fraud: scale, impact and response	1
1.1 Introduction	2
1.2 Defining fraud	2
1.3 Scale and impact	4
1.4 Local, regional and national structures and responsibilities	7
1.5 Offender and victim profiles	14
1.6 Fraud indicators (red flags)	16
1.7 Reporting fraud	19
1.8 Fraud enablers	22
1.9 Other methods used to facilitate fraud	25
1.10 The Fraud Investigation Model (FIM)	27
<hr/>	
2 Legislation	35
2.1 Introduction	36
2.2 The Fraud Act 2006	36
2.3 Conspiracy to defraud	43
2.4 The Bribery Act 2010	44
2.5 The Proceeds of Crime Act 2002 (money laundering offences)	53
2.6 The Theft Act 1968 (false accounting, section 17)	58
2.7 The Computer Misuse Act (CMA) 1990	59
2.8 The Financial Services and Markets Act (FSMA) 2000	61
2.9 The Insolvency Act 1986	62
2.10 Identity crime-related legislation	65
<hr/>	
3 Types of fraud	66
3.1 Introduction	67
3.2 Volume frauds	67
3.3 Other frauds	85
3.4 Identity-related frauds	99

4	Digitally enabled (cyber) crime	103
4.1	Introduction	104
4.2	Cyber terminology—jargon buster	106
4.3	Types of cyber-dependent crimes	108
4.4	The initial investigation of fraud-related cyber crime	115
4.5	Roles of different agencies	121
4.6	Cyber crime prevention and protection	122
5	Prevention and disruption	125
5.1	Introduction	126
5.2	Elements of fraud prevention	128
5.3	Methods and types of prevention available	131
5.4	Measuring the impact of prevention	133
5.5	Centres of best practice	134
5.6	Organisational fraud health checks	136
5.7	Disruption	138
5.8	Website take down	140
5.9	Telephone disruption	144
6	Investigation and case management	147
6.1	Introduction	148
6.2	National Fraud Intelligence Bureau referrals process	150
6.3	Case acceptance criteria	153
6.4	Criminal v Civil routes	155
6.5	Developing a case theory	156
6.6	Resource management	158
6.7	Making and recording a decision	159
6.8	Case management	161
6.9	Partnership and cross-sector working	164
6.10	Investigation plans	167
6.11	Victim management	169
6.12	Witness management	176
6.13	Covert investigations	177
6.14	Gathering relevant material	182
6.15	Forensic investigative opportunities	199
6.16	International investigations	205
6.17	Use of subject matter experts (SMEs)	207
6.18	Identifying and managing the suspect	210
6.19	Developing a media strategy	219
7	Fraud and financial investigations	223
7.1	Introduction	224
7.2	The role of the financial investigator (FI)	225

7.3	Legislation	227
7.4	Protocols	232
7.5	Restraint and confiscation	232
<hr/>		
8	Fraud and disclosure	235
8.1	Introduction	236
8.2	Disclosure and the principles	237
8.3	Disclosure roles	238
8.4	Manual guidance (MG) forms	239
8.5	Disclosure officer's policy file and CPS disclosure management document	244
8.6	Digital disclosure strategy	245
8.7	Third-party material	250
8.8	Legal professional privilege (LPP) material	250
8.9	Use of the HOLMES and other case management systems	251
8.10	Summary	252
<hr/>		
9	Investigating sector-specific fraud	253
9.1	Introduction	254
9.2	Police Intellectual Property Crime Unit (PIPCU)	254
9.3	The Insurance Fraud Enforcement Department (IFED)	259
9.4	Dedicated Card and Payment Crime Unit (DCPCU)	267
<hr/>		
10	Reviews and operational learning	276
10.1	Introduction	277
10.2	Fraud case reviews	277
10.3	Structured debriefs	284
Appendices		
1	CPS template for memorandum of understanding	295
2	Fraud investigation planning—aide-memoire	296
3	Frequently asked questions regarding the reporting, assessment and investigation process of fraud or cyber crime	302
4	Available support services	305
5	Example victim management strategy	307
6	Developing an overarching fraud interview strategy	314
7	Key questions for undertaking a review of a fraud investigation	315
	Bibliography	319
	Index	325