

- Accountants, on investigation team, 145
- Accountant-client privilege, 56
- Accounting changes, 35
- Accounting department, as information source, 157–158
- Accounts payable fraud, 132
- Accusatory model (interviewing), 196–198
- Acts, fraudulent, 4
- Act on the Protection of Personal Information (Japan), 223, 224
- Actus reus*, 182
- Admissibility:
  - of confessions, 63
  - of evidence, 46–48
- Admission-seeking questions, in interviews, 192–193
- Adversarial proceedings, 44, 46
- Adverse testimony privilege, 55
- Africa, *see* Middle East and North Africa; Sub-Saharan Africa
- Age, of interviewee, 180
- Agency of the Republic of Slovenia for Public Legal Records and Related Services (AJPES), 262
- Agents, external fraud by, 37
- Alibis, 198
- Allegations, 152–153
- Altered checks, 14–15
- Altered expenses, 19
- Anonymity, in whistle-blowing policies, 118–119
- Anonymous feedback mechanisms, 84
- Anti-Corruption Commission Act (Malaysia), 227
- Anti-Corruption Law (Brazil), 269
- Anti-fraud controls:
  - in Asia-Pacific region, 211, 213*e*
  - in Canada, 245, 247*e*
  - in Eastern Europe and Western/Central Asia, 251, 253*e*
  - in Latin America and the Caribbean, 265, 267*e*
  - in Middle East and North Africa, 287, 289*e*
  - in Southern Asia, 303, 305*e*
  - in Sub-Saharan Africa, 315, 317*e*
  - in United States, 329, 331*e*
  - in Western Europe, 337, 339*e*
- Anti-fraud policies:
  - in anti-fraud programs, 104–106
  - and fraud risk assessment, 99
- Anti-fraud programs, 101–139
  - anti-fraud policy in, 104–106
  - and employee policies, 124, 128
  - and employee support, 121–122
  - and hiring processes, 122–124
  - and internal controls, 109–111
  - and organizational culture, 101–104
  - and risk management, 108–109
  - fraud response, 136–138
  - personnel-focused controls, 116–128
  - process- and policy-focused controls, 128–131
  - responsibilities for, 111–116
  - scheme-specific control activities, 131–136
  - and training, 124–128
  - whistle-blower policy in, 106–107
  - whistle-blower program, 116–121
- Anti-fraud training, 124–128
- Anti-Money Laundering and Anti-Terrorist Financing Act (Netherlands), 357
- Anti-retaliation, in whistle-blower policies, 107, 120
- Anti-Unfair Competition Law (China), 220
- Approach section (case reports), 170
- Arms, crossing of, 204
- Asia, *see* Eastern Europe and Western/Central Asia; Southern Asia
- Asia-Pacific region, 211–244
  - anti-fraud controls in, 211, 213*e*
  - Australia, 213–218
  - China, 218–221
  - detection methods in, 211, 212*e*
  - Japan, 221–225
  - Malaysia, 225–227
  - New Zealand, 227–231
  - Philippines, 231–234
  - scheme types in, 211, 212*e*
  - Singapore, 234–237
  - South Korea, 237–241
  - Taiwan, 241–244

## INDEX

- Assessment questions, in interviews, 192
- Assets, overstated, 30–32
- Asset misappropriation, 8, 10–26, 134
  - cash on hand, theft of, 10
  - cash receipts, theft of, 11–13
  - defined, 8, 10
  - disbursements, fraudulent, 13–21
  - in Fraud Tree, 9e
  - intangible assets, 25–26
  - internal controls to address risk of, 131–134
  - physical assets, 22–25
- Association of Certified Fraud Examiners (ACFE), 7, 209, 211, 217, 251, 265, 287, 303, 315, 329, 337
  - Fraud Risk Management Guide*, 85, 109
  - Report to the Nations on Occupational Fraud and Abuse*, 7, 10, 13, 116, 117, 126, 130, 211, 217, 251, 265, 287, 303, 315, 329, 337
- Attorney-client privilege, 53, 145
- Audience, for anti-fraud training, 125
- Audit committee, responsibilities of, in anti-fraud program, 113
- Auditors:
  - on investigation team, 145
  - responsibilities of, in anti-fraud program, 114–115
  - responsibility for fraud risk assessment, 79
- Audit policy, proactive, 130
- Australia, 46, 213–218
  - anti-fraud programs in, 217
  - Australia Corporations Act (2001), 216
  - Australian Business Register (ABR), 215
  - Australian Criminal Court Records, 214
  - Australian Federal Police, 214
  - Australian Financial Security Authority, 214
  - Australian Government Investigations Standards, 217
  - Australian Post, 214
  - Australian Privacy Act (1988), 215
  - Australian Prudential Regulation Authority (APRA), 216
  - Australian Securities and Investments Commission (ASIC), 214, 216
  - Australian Stock Exchange (ASX), 216
  - Australian Taxation Office (ATO), 216
  - Australian Transaction Reports and Analysis Centre (AUSTRAC), 216
  - employee privacy rights in, 61
  - legal/regulatory environment in, 215–216
  - sources of information in, 214–215
    - special considerations with fraud investigations in, 217–218
- Authentic evidence, 47–48
- Authorization, for investigations, 106
- Authorized maker schemes, 15
- Automated clearinghouse (ACH) payments, 15
- Automated legal information system (ASPI) (Czech Republic), 257
- Awareness, of fraud, 77
- Background checks, 123
- Background section (case reports), 170
- Beck-Online, 257
- Business email compromise (BEC) scams, 40–41
- Benchmark admissions, 200
- Benchmarking, 86
- Bench trials, 63
- Bias, avoiding, 167
- Bidding, 35–37
- Bid manipulation schemes, 36–37
- Bid rotation (bid pooling), 36
- Bid splitting, 37
- Bid suppression, 36
- Bid tailoring, 36
- Billing schemes, 16–17
- Board of directors, responsibilities of, in anti-fraud program, 112
- Body language, 190, 203–204
- Brazil, 267–270
  - anti-fraud programs in, 269–270
  - legal/regulatory environment in, 268–269
  - sources of information in, 267–268
  - special considerations with fraud investigations in, 270
- Bribery, 27
  - Australia, 216
  - Canada, 249
  - China, 220
  - by contractors/vendors, 35
  - internal controls to address risk of, 134–135
  - Japan, 223
  - Malaysia, 226
  - New Zealand, 229
  - Philippines, 232–233
  - Singapore, 236
  - South Korea, 239
  - Taiwan, 243
- Brokers, external fraud by, 37

## Index

- Bulgaria, 253–255
  - anti-fraud programs in, 255
  - legal/regulatory environment in, 254–255
  - sources of information in, 254
  - special considerations with fraud investigations in, 255
- Bulgarian National Bank, 254
- BULSTAT Register, 254
- Business, nature of, and fraud risk, 75
- Business identity theft, 37–41
  - company impersonation, 38
- Business processes, 25
  
- Calibrating, 192
- Canada, 245–250
  - anti-fraud controls in, 245, 247*e*
  - data privacy in, 73
  - detection methods in, 245, 246*e*
  - scheme types in, 245, 246*e*
- Canada Evidence Act, 45
- Canadian Charter of Rights and Freedoms, 64
- Caribbean, *see* Latin America and the Caribbean
- Cascading training, 127
- Case plan, finalization of, 154–155
- Case reports, 166–171
  - characteristics of well-written, 167
  - format of, 169–171
  - impartiality of, 168–169
  - legal considerations with, 168
  - organization of information in, 169
  - purpose of, 166–167
- Cash, theft of incoming, 131–132
- Cash disbursement fraud, 132
- Cash larceny, 12–13
- Cash on hand, theft of, 10
- Cash receipts, theft of, 11–13
- Cash register disbursement schemes, 18
- Central Asia, *see* Eastern Europe and Western/Central Asia
- Central Business Register (Denmark), 340
- Central Intelligence Agency (CIA), 176
- Central Register of Convicted Persons (Spain), 363
- Central Registry of Enterprises (Poland), 259
- CEO fraud, *see* Business email compromise (BEC) scams
- Certified Fraud Examiner (CFE) Code of Professional Standards, 168
- Certified Fraud Examiners (CFEs):
  - on investigation team, 145
  - survey on costs of fraud, 7–8
- Chain of custody, 51–52
- Character evidence, 48–49
- Character testimony, as sign of deception, 202
- Charter of Fundamental Rights of the European Union, 67
- Check and payment tampering, 13–16, 37
- Chile, 270–277
  - anti-fraud programs in, 276
  - legal/regulatory environment in, 273–276
  - sources of information in, 270–273
  - special considerations with fraud investigations in, 276–277
  - trials in, 63
- China, 218–221
  - anti-fraud programs in, 220–221
  - business visa for, 178
  - China SOX, 221
  - legal/regulatory environment in, 219–220
  - sources of information in, 218–219
  - special considerations with fraud investigations in, 221
- Chronology of events, 163
- Circumstantial evidence, 46
- Circumvention, of internal controls, 111
- Civil invasion of privacy, 67–69
- Civil Law Convention on Corruption (Council of Europe), 59
- Civil law systems, 43–44
  - admissibility of evidence in, 47, 48
  - client privileges in, 56
  - exceptions to character evidence rule in, 49
  - hearsay in, 50–51
- Clean Company Act (Brazil), 269
- Closed questions, in interviews, 190
- Closing questions, in interviews, 193–194
- Co-conspirators, 186
- Code of conduct, and fraud risk assessment, 99
- Codexis Academia, 257
- Collusion:
  - with company employees, 36–37
  - internal controls limited by, 111
  - with other vendors or contractors, 35–36
- Commission schemes, 21
- Committee of Sponsoring Organization of the Treadway Commission (COSO), 85
  - Fraud Risk Management Guide*, 85, 109
  - internal controls – integrated framework, 109–110

## INDEX

- Commodity Futures Trading Commission (CFTC), 334
- Common law systems, 43–44
  - admissibility of evidence in, 46–48
  - Australia, 215–216
  - client privileges in, 56
  - rule against character evidence in, 48–49
- Commonwealth Fraud Control Framework, 217
- Communication:
  - about fraud, 77, 138
  - about fraud risk, 98
  - of fraud risk assessment results, 97–98
- Companies:
  - ethical culture of, 76
  - promoting communication throughout, 98
- Companies Register (New Zealand), 228
- Company Act (Japan), 223
- Company credit cards, 91
- Company funds, personal purchases with, 17
- Competition Authority (France), 347
- Complementary bidding, 36
- Compliance, with regulations and professional standards, 79
- Compliance risk, 108
- Computer hacking, 39–41
- Computer Misuse and Cybersecurity Act (Singapore), 67
- Concealment, as component of fraud, 4
- Confessions:
  - in criminal cases, 63
  - in interviews, 205–208
- Confidential communications privilege, 55
- Confidentiality:
  - in anti-fraud policies, 106
  - in investigations, 149
  - in whistle-blowing policies, 118–119
  - of whistle-blowing reports, 107
- Conflicts of interest, 29–30
- Consent searches, 64–65
- Consequences:
  - of inherent fraud risks, 89
  - outlined in anti-fraud policies, 106
- Constitution of the Republic of Singapore, 67
- Consultants, on investigation team, 146
- Contractors:
  - collusion with company employees, 36–37
  - external fraud committed by, 35–37
- Contractual rights of employees, 58
- Controls, risk of management's override of, 87
- Control weaknesses, 7
- Conversion, as component of fraud, 4
- Corporate culture, *see* Organizational culture
- Corporation Registration System (Japan), 222
- Corroborative witnesses, 186
- Corruption, 27–30
  - in Asia-Pacific region, 211
  - in Canada, 245
  - in Eastern Europe and Western/Central Asia, 251
  - in Latin America and the Caribbean, 265
  - in Middle East and North Africa, 287
  - in Southern Asia, 303
  - in Sub-Saharan Africa, 315
  - in the United States, 329
  - in Western Europe, 337
  - bribery/kickbacks, 27–28
  - conflicts of interest, 29–30
  - defined, 27
  - economic extortion, 28–29
  - gratuities, illegal, 28
  - internal controls to address risk of, 134–135
- Corruption Perception Index (CPI), 176
- Cost(s):
  - of cross-border investigations, 173
  - of fraud, 7–8
  - of fraud risk, estimation of, 94
- Cost capitalization, improper, 33
- Counsel:
  - consulting with, as result of fraud, 137
  - right to, 62
- Countermeasures, evaluation of, 96
- Cover bidding, 36
- Credit cards:
  - customer fraud, 37
  - false refunds via, 18
- Credit checks, 123
- Cressey, Donald, 5
- Criminal Code Act (1995) (Australia), 216
- Criminal law, individual rights and obligations under, 61–63
- Cross-border investigations, 172–178
  - and access to information, 176
  - cost of, 173
  - and cultural differences, 174–175
  - in high-risk regions, 175–176
  - and language differences, 173–174
  - and legal differences, 175
  - logistical issues with, 177–178
- Cross-training, of employees, 128
- Cultural differences:

## Index

- in cross-border investigations, 174–175
- and interviews, 181
- Culture:
  - in international whistle-blowing, 119–120
  - organizational, *see* Organizational culture
- Customers, fraud committed by, 37
- Cybersecurity Law (China), 219, 221
- Cyprus, 289–292
  - anti-fraud programs in, 291
  - legal/regulatory environment in, 290–291
  - sources of information in, 289–290
  - special considerations with fraud investigations in, 292
- Czech Corporate Governance Code, 258
- Czech Republic, 256–259
  - anti-fraud programs in, 258
  - legal/regulatory environment in, 257–258
  - sources of information in, 256–257
  - special considerations with fraud investigations in, 258–259
  - trials in, 63
  
- Data, as evidence, 155–156
- Data analysis, 165
- Database(s):
  - establishing a, 162–163
  - media, 162
- Data breaches, 39
- Data extraction, 165
- Data leaking, in bidding process, 37
- Data monitoring and analysis, 130–131
- Data privacy laws, 70–73
- Data transfers, international, 72–73
- Deception:
  - discussing, during interview, 199–200
  - nonverbal signs of, 203–204
  - recognizing, in interviews, 200–204
  - verbal signs of, 201–203
- Deep Web, 161
- Defamation, and investigation in private actions, 65–67
- Demonstrative evidence, 45–46
- Denials, increasingly weak, 202
- Denmark, 339–342
  - anti-fraud programs in, 341–342
  - legal/regulatory environment in, 340–341
  - sources of information in, 340
  - special considerations with fraud investigations in, 342
- Departments, as information sources, 157–159
- Deposit, theft of cash from, 12–13
- Detection, fear of, 131
- Detection controls, as deterrent, 96
- Detection methods:
  - in Asia-Pacific region, 211, 212*e*
  - in Canada, 245, 246*e*
  - in Eastern Europe and Western/Central Asia, 251, 252*e*
  - in Latin America and the Caribbean, 265, 266*e*
  - in Middle East and North Africa, 287, 288*e*
  - in Southern Asia, 303, 304*e*
  - in Sub-Saharan Africa, 315, 316*e*
  - in United States, 329, 330*e*
  - in Western Europe, 337, 338*e*
- Detective controls, 110
- Deterrent to fraud, sanctions as ineffective, 6–7
- DiCom, 271
- Direct evidence, 46
- Disbursements, fraudulent, 13–21
  - billing schemes, 16–17
  - cash register disbursement schemes, 18
  - check and payment tampering, 13–16
  - expense reimbursement schemes, 18–20
  - payroll schemes, 20–21
- Discharge, wrongful, 70
- Disciplinary actions:
  - in anti-fraud policies, 106
  - facing perpetrators of fraud, 136–137
- Disciplinary guidelines, 137
- Disclosures:
  - improper, 34–35
  - public, of private facts, 68–69
- Disorganization, in cross-border investigations, 177
- Documents:
  - as evidence, 155–156
  - segregation of, 162
- Document analysis, 165
- Dodd-Frank Act, 335
- “Doing Business” reports, 176
- Dress codes, 241
- Duplicate reimbursements, 19–20
- Duties:
  - of employees, 57–63
  - rotation of job, 128
  - separation of, 129
- Duty to cooperate, employees’, 57

## INDEX

- Early revenue recognition, 31–32
- Eastern Europe and Western/Central Asia, 251–264
- anti-fraud controls in, 251, 253*e*
  - Bulgaria, 253–255
  - Czech Republic, 256–259
  - detection methods in, 251, 252*e*
  - Poland, 259–261
  - scheme types in, 251, 252*e*
  - Slovenia, 262–264
- Economic conditions, 75
- Economic extortion, 28–29
- Economist Intelligence Unit (EIU), 176
- EDGAR database, 332
- Educational background, of interviewee, 181
- Egypt, 292–293
- anti-fraud programs in, 293
  - legal/regulatory environment in, 293
  - sources of information in, 292
- Electronic access controls, 129
- Electronic Disclosure for Investors Network (EDINET) (Japan), 222
- Electronic evidence, chain of custody of, 52
- Electronic evidence, preserving, 163–164
- Electronic payment tampering, 15–16
- Email:
- as reporting mechanism, 117
  - vulnerabilities of, 39–41
- Emotional distress, intentional infliction of, 70
- Emotive words, avoidance of, 202
- Employees:
- anti-fraud training for, 125
  - collusion with vendors/contractors, 36–37
  - duties and rights of, 57–63
  - educating, about fraud risk, 85
  - ethics of, 76
  - ghost, 20–21
  - involved in conducting of fraud risk assessment, 80
  - misappropriation of information by, 26
  - organizational culture influenced by, 103–104
  - responsibilities of, in anti-fraud program, 115
  - wrongful discharge of, 70
- Employee policies, and anti-fraud programs, 124, 128
- Employee support, and anti-fraud programs, 121–122
- Encryption, software, 39–41
- Endorsements, forged, 14
- Entity-level controls, 110–111
- Equipment, for interviews, 185–186
- Ethics:
- of companies and employees, 76
  - guidance for ethical dilemmas, 121–122
  - management’s and executives’ commitment to, 102–103
  - performance metrics based on, 124
- Ethics policies, and fraud risk assessment, 99
- EU Data Protection Directive (EU Directive 95/46/EC), 71–72
- Europe, 67. *See also* Eastern Europe and Western/Central Asia; Western Europe
- European Commission, 73
- European Convention on Human Rights, 63–64, 67
- European Parliament, 72
- European Union (EU):
- data privacy in, 71–72
  - employee privacy rights in, 60–61
  - individuals’ rights under criminal law in, 62
  - international data transfers in, 72–73
- Evidence, 44–48
- admissibility of, 46–48
  - chain of custody of, 51–52
  - collection/analysis of, 155–166
  - defined, 44
  - destruction of, 58
  - forms of, 45–46
  - legal considerations for, 164
  - organization of, 162–163
  - in plain view, 65
  - preservation of, 163–164
  - reaction to, as sign of deception, 204
  - reviewing/analyzing, 164–166
  - and rights of the individual, 56–57
- Evidence Act (Australia), 46
- Evidentiary privilege, 149
- Evidentiary rules, 48–51
- Excuses, making, 202
- Executives:
- anti-fraud training for, 126–127
  - organizational culture influenced by, 102–103
- Executive management, responsibilities of, in anti-fraud program, 114
- Executive summary (case reports), 170
- Exit interviews, 128
- Expectations, in hiring processes, 123
- Expenses:
- altered/overstated, 19
  - fictitious, 18–19

## Index

- mischaracterized, 19
- understated, 32–33
- Expense reimbursement schemes, 18–20, 133
- Expert reports, 169
- Expert witnesses, 45, 50
- External fraud, 35–41
  - by agents/brokers/fiduciaries, 37
  - by customers, 37
  - by unrelated third parties, 37–41
  - by vendors/contractors, 35–37
- External management, of whistle-blowing reports, 118
- External notifications, 150
- External parties, access to whistle-blowing procedures for, 118
- External sources of information, 159–162
- Extortion, economic, 28–29
- Fact witnesses, 45
- Fair Information Practices, 71
- Fake smiles, 204
- False imprisonment, 69
- False invoicing, through shell companies, 16
- False refunds, 18
- False voids, 18
- Federal Bureau of Investigation (FBI), 41
- Federal Deposit Insurance Corporation (FDIC), 334
- Federal Reserve System (Fed), 334
- Federal Rules of Evidence (FRE), 45, 51
- Feedback mechanisms, in fraud risk assessment, 84
- Feigned unconcern, 203
- Fictitious expenses, 18–19
- Fictitious revenues, 31
- Fidelity coverage, 96
- Fiduciaries, external fraud by, 37
- Finance department, as information source, 157–158
- Financial Crimes Enforcement Network (FinCEN), 334
- Financial Industry Regulatory Authority (FINRA), 334
- Financial Markets Authority (AMF) (France), 346
- Financial Markets Authority (FMA) (New Zealand), 229
- Financial risk, 108
- Financial Services Act (FSA) (Malaysia), 226
- Financial statement fraud, 30–35, 135
  - assets/revenues, overstated, 30–32
  - improper disclosures, 34–35
  - internal controls to address risk of, 135
  - liabilities/expenses, understated, 32–33
- Findings section (case reports), 170–171
- Finland, 61
- Fixed assets, theft of, 22
- Focus groups, 83
- Follow-up and recommendations (case reports), 171
- Follow-up interviews, 208
- Foreign Corrupt Practices Act, 334
- Foreign governments, working with, 172
- Foreign Investment Review Board (FIRB) (Australia), 216
- Foreign jurisdiction privileges, judicial treatment of, 56
- Forged endorsements, 14
- Forged maker schemes, 14
- France, 342–349
  - anti-fraud programs in, 348
  - employee privacy rights in, 61
  - jury trials in, 63
  - legal/regulatory environment in, 345–348
  - sources of information in, 342–345
  - special considerations with fraud investigations in, 349
- Fraud:
  - actions constituting, 104–106
  - common elements in, 4
  - components of, 4
  - costs of, 7–8
  - defined, 3–4
  - as hidden cost, 3
  - susceptibility to, 7
- Fraud Act (2006) (United Kingdom), 370
- Fraud Examiners Manual*, 217
- Fraud response plans, 142
- Fraud risk(s):
  - acceptable level, of fraud risk, 93
  - assumption, of fraud risk, 97
  - avoidance of fraud risk, 95
  - classification of, 109
  - defining, 75–76
  - inherent, 86–91
  - residual, 93–97
- Fraud risk assessment, 75–99
  - benefits of, 77–79
  - definition of fraud risk, 75–76
  - inherent fraud risks in, 86–91
  - internal controls in, 91–93



## INDEX

- Fraud risk assessment (*continued*)
  - ongoing impact of, 98–99
  - preparation for, 82–85
  - reporting results of, 97–98
  - residual fraud risks in, 93–97
  - responsibility for, 79–82
- Fraud risk management, 109
- Fraud Risk Management Guide* (COSO and ACFE), 85, 109, 217
- Fraud theory, 151–152
- Fraud Triangle, 5–7, 5e
- Freedom of Information Act (FOIA) (Canada), 249
- Freedom of Information Ordinance (FOIO) (Pakistan), 309
- French Data Protection Act (FDPA), 345
- Frequency, in estimation of fraud risk, 88–89
  
- Gender, of interviewee, 180
- General Data Protection Regulation (GDPR) (EU), 72
- General Information Sheet (GIS) (Philippines), 231–232
- Germany, 349–351
  - anti-fraud programs in, 351
  - employee privacy rights in, 61
  - legal/regulatory environment in, 350–351
  - sources of information in, 349–350
  - special considerations with fraud investigations in, 351
- Ghost employees, 20–21
- Good faith reporting, 107
- Governance, of anti-fraud programs, 101–107
- Government, search and seizure by, 63–65
- Gramm-Leach-Bliley Act, 333
- Gratuities, illegal, 28
- Greece, 352–353
  - anti-fraud programs in, 353
  - legal/regulatory environment in, 352–353
  - sources of information in, 352
  - special considerations with fraud investigations in, 353
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD), 71
- Gvin.com, 262
- Hacking, 39–41
- Hands over mouth, 204
- Health, of interviewee, 181
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), 333
- Hearsay, 50–51
- Heat map, plotting risks on, 94–95
- High-risk areas, identifying, 98–99
- High-risk regions, cross-border investigations in, 175–176
- Hiring processes, 122–124
- Hong Kong, 219
- Human error, internal controls limited by, 111
- Human resources (HR) personnel:
  - as information source, 158
  - on investigation team, 146
- Hungary, 63
- Hybrid legal systems, 44
  
- Identity theft, business, 37–41
- Illegal gratuities, 28
- Illustrators, 204
- Immigration, and cross-border investigations, 177–178
- Impartiality, of case reports, 168–169
- Improper asset valuation, 32
- Improper cost capitalization, 33
- Improper disclosures, 34–35
- Incentives, to commit fraud, 87
- Incoming cash, theft of, 131–132
- Independence, in fraud risk assessment, 81
- India, 305–309
  - anti-fraud programs in, 308
  - employee privacy rights in, 61
  - legal/regulatory environment in, 307–308
  - sources of information in, 306–307
  - special considerations with fraud investigations in, 309
  - trials in, 63
- Indirect costs, of fraud, 8
- Individual rights, 56–57, 61–63
- Informants, confidential, 55–56
- Information:
  - access to, in cross-border investigations, 176
  - as evidence, 156–159
  - gathering, for fraud risk assessment, 82
  - seeking, via interview, 187
- Informational questions, in interviews, 190–192
- Information technology (IT) personnel:
  - as information source, 158–159
  - on investigation team, 146
- Infrastructure limitations, and cross-border investigations, 178



## Index

- Inherent fraud risks, 86–91
  - defined, 76
  - identification of potential, 86–88
  - impact of, to organization, 89–91
  - likelihood of, 88–89
- Injury, caused by defamation, 67
- In-person reporting, 117
- Inquisitorial proceedings, 44
- Insiders, misappropriation of information by, 26
- Institute of Internal Auditors, 114
- Intangible assets, misappropriation of, 25–26
  - by employees/insiders, 26
  - intellectual property, 25–26
  - personally identifiable information, 26
- Intellectual ability, of interviewee, 181
- Intellectual property, 25–26
- Intentional infliction of emotional distress, 70
- Internal audit and compliance department, as information source, 158
- Internal auditors, responsibilities of, in anti-fraud program, 114–115
- Internal controls:
  - to address risk of accounts payable and cash disbursement fraud, 132
  - to address risk of corruption, 134–135
  - to address risk of expense reimbursement fraud, 133
  - to address risk of financial statement fraud, 135
  - to address risk of fraud involving vendors, 136
  - to address risk of misappropriation of investment assets, 134
  - to address risk of misappropriation of physical noncash assets, 134
  - to address risk of payroll fraud, 133
  - to address risk of theft of incoming cash, 131–132
  - and anti-fraud programs, 109–111
  - assessment of, 78–79
  - effectiveness of, 76
  - in fraud risk assessment, 91–93
- Internal fraud, *see* Occupational fraud
- Internal management, of whistle-blowing reports, 118
- Internal notifications, 149–150
- Internal parties, access to whistle-blowing procedures for, 118
- Internal sources of information, 157–159
- International data transfers, 72–73
- International operations:
  - anti-fraud training in, 127
  - hiring processes in, 124
  - whistle-blowing considerations in, 119–120
- International Organization for Standardization (ISO), 108, 134–135
- Internet archives, 161
- Interpersonal skills, 147
- Interrogating (term), 179
- Interviews, 179–208
  - confessions in, 205–208
  - exit, 128
  - follow-up, 208
  - in fraud risk assessment, 82–83
  - in investigations, 166
  - legal considerations with, 182
  - methodologies for conducting, 194–200
  - note taking during, 185
  - planning and preparing, 179–186
  - by purpose, 187
  - question types in, 188–194
  - recognizing deception in, 200–204
  - recording of, 184–185
  - reluctance to terminate, as sign of deception, 203
  - remote, 183–184
  - sensitive issues/questions in, 205
  - strategies for conducting, 187–200
  - by subject, 186–187
- Interviewing (term), 179
- Introductory questions, in interviews, 188–190
- Intrusion into and individual's private matters, 68
- Invasion of privacy, civil, 67–69
- Inventory, theft of, 22
- Investigations, 141–178
  - in anti-fraud policies, 105–106
  - assessing need for, 143
  - case report in, 166–171
  - cross-border, 172–178
  - defining goal/purpose of, 148
  - determination of scope of, 152–154
  - evidence collection/analysis in, 155–166
  - and finalization of case plan, 154–155
  - and fraud response plans, 142
  - and fraud theory, 151–152
  - interviewing witnesses/suspects in, 166, 187
  - leaders of, 147
  - methodology for, 141, 155–172
  - and notification of relevant parties, 149–150
  - preparation for, 143–155

## INDEX

- Investigations (*continued*)
  - in private actions, 65–73
  - and working with foreign governments, 172
  - and working with law enforcement, 171–172
- Investigation team, assembly of, 144–148
- Investigative techniques, development of, 78
- Investment assets, misappropriation of, 134
- Invisible Web, 161
- IPPF – Practice Guide: Internal Auditing and Fraud* (Institute of Internal Auditors), 114
- Israel, 63
- Italy, 61
- IUS-Info, 263
  
- Japan, 221–225
  - anti-fraud programs in, 224
  - employee privacy rights in, 61
  - legal/regulatory environment in, 223–224
  - right to counsel in, 62
  - sources of information in, 222–223
  - special considerations with fraud investigations in, 224–225
- Job duties, rotation of, 128
- Jordan, 294–296
  - anti-fraud programs in, 295
  - legal/regulatory environment in, 294–295
  - sources of information in, 294
  - special considerations with fraud investigations in, 296
- Jury, trial by, 62–63
  
- Kenya, 317–320
  - anti-fraud programs in, 319–320
  - legal/regulatory environment in, 318–319
  - sources of information in, 318
  - special considerations with fraud investigations in, 320
- Key-document files, 162
- Kickbacks, 27–28
- Knowledge, of interviewee, 181
- Land Online (New Zealand), 228
- Language:
  - as factor in cross-border investigations, 173–174
  - and international whistle-blowing, 119
  - of interviewee, 181
  - in signed statements, 206–207
- Lapping, 11
  
- Larceny:
  - cash, 12–13
  - unconcealed, 22–23
- Latin America and the Caribbean, 265–285
  - anti-fraud controls in, 265, 267*e*
  - Brazil, 267–270
  - Chile, 270–277
  - detection methods in, 265, 266*e*
  - Mexico, 277–281
  - Peru, 281–285
  - scheme types in, 265, 266*e*
- Law enforcement:
  - investigations and working with, 171–172
  - notification of, 150
- Law enforcement privilege, 55–56
- Lay witnesses, 45, 50
- Leading questions, in interviews, 191
- Leave time, mandatory, 128
- Legal advice privilege, 55
- Legal counsel, on investigation team, 145
- Legal department, as information source, 158
- Legal environment, as fraud risk, 76
- Legal issues, 43–73
  - chain of custody, 51–52
  - employee duties and rights, 57–63
  - evidence, 44–48
  - evidentiary rules, 48–51
  - government search and seizure, 63–65
  - in hiring process, 124
  - individual rights, 56–57
  - in international whistle-blowing, 119
  - investigations in private actions, 65–73
  - privileges and protections, 52–56
  - and types of legal systems, 43–44
- Legal misconduct, risk of, 87–88
- Legal professional privileges, 53–54
- Legal systems, 43–44
- Legal work privileges, 54
- Lexgalaxy, 257
- LEX Informator Prawno-Gospodarczy, 260
- Liabilities:
  - omitted, 34
  - understated, 32–33
- Liability omissions, 34
- Libel, 66
- Likelihood, of fraud risk, 88–89
- Location (of investigation), 153
- Logistics:
  - of cross-border investigations, 177–178
  - and fraud investigation, 153–154

## Index

- Macau, 219
- Malaysia, 225–227
- anti-fraud programs in, 227
  - data privacy in, 73
  - legal/regulatory environment in, 225–227
  - sources of information in, 225
- Malware, 39–40
- Management:
- controls overridden by, 87
  - failure to prevent or detect misconduct by, 137
  - on investigation team, 146
  - organizational culture influenced by, 102
  - responsibilities of, in anti-fraud program, 113–114
  - responsibility for fraud risk assessment, 79
- Management fraud, 35
- Management override, internal controls limited by, 111
- Mandatory time off, 128
- Manipulation schemes, in bidding, 36–37
- Manipulators, 204
- Marital privilege, 55
- Market division, 36
- Matching principle, 31
- Mauritius, 320–323
- anti-fraud programs in, 322–323
  - legal/regulatory environment in, 321–322
  - sources of information in, 320–321
- Measurable goals, of investigations, 148
- Media databases, 162
- Memory, selective, 202
- Mens rea*, 182
- Mental health, of interviewee, 181
- Merchandise shipments, fraudulent, 24, 35
- Metasearch engines, 160
- Mexico, 277–281
- anti-fraud programs in, 280–281
  - legal/regulatory environment in, 279–280
  - sources of information in, 277–279
  - special considerations with fraud investigations in, 281
  - trials in, 63
- Middle East and North Africa, 287–301
- anti-fraud controls in, 287, 289e
  - Cyprus, 289–292
  - detection methods in, 287, 288e
  - Egypt, 292–293
  - Jordan, 294–296
  - Oman, 296–297
  - scheme types in, 287, 288e
  - United Arab Emirates, 298–301
- Middle management:
- anti-fraud training for, 126–127
  - organizational culture influenced by, 103
  - responsibilities of, in anti-fraud program, 113–114
- Misappropriation:
- of assets, 8-26, 131–134
  - of intangible assets, 25–26
  - of investment assets, 134
  - of physical noncash assets, 22–25, 134
- Mischaracterized expenses, 19
- Misuse of physical assets, 22
- Mitigation of risks, 78, 96–97, 108
- Modus operandi*, 182
- Monitoring policies, and privacy rights, 60–61
- Motivational interviewing, 196
- Motor Vehicle Register (New Zealand), 228
- Mouth, hands over, 204
- Multiple reimbursements, 19–20
- National Center for Procedural and Extra-Procedural Information (Brazil), 268
- National Database and Registration Authority (NADRA) (Pakistan), 310
- Nationmaster, 176
- Nation-state actors, 39
- Nature, of business, 75
- Need recognition schemes, in bidding, 36
- Netherlands, 354–357
- anti-fraud programs in, 356–357
  - legal/regulatory environment in, 355–356
  - sources of information in, 354–355
  - special considerations with fraud investigations in, 357
  - trials in, 63
- Network hacking, 39–41
- Neutrality, of witnesses, 186
- New Zealand, 227–231
- anti-fraud programs in, 230
  - legal/regulatory environment in, 229–230
  - sources of information in, 227–228
  - special considerations with fraud investigations in, 230–231
- Nonadversarial proceedings, 44
- Noncash assets:
- internal controls to address the risk of misappropriation of, 134

## INDEX

- Noncash assets (*continued*)  
schemes involving, 22–26  
theft of, in Asia-Pacific region, 211  
theft of, in Canada, 245  
theft of, in Eastern Europe and Western/  
Central Asia, 251  
theft of, in Latin America and the Caribbean,  
265  
theft of, in Middle East and North Africa, 287  
theft of, in Southern Asia, 303  
theft of, in Sub-Saharan Africa, 315  
theft of, in the United States, 329  
theft of, in Western Europe, 337
- Noncash asset schemes, 22–26  
intangible assets, misappropriation of, 25–26  
physical assets, misappropriation of, 22–25
- Nonfraud irregularities, 105
- Nonpublic records, 160
- Norming, 192
- North Africa, *see* Middle East and North Africa
- Norway, 357–361  
anti-fraud programs in, 360–361  
legal/regulatory environment in, 359–360  
sources of information in, 357–359  
special considerations with fraud investigations  
in, 361
- Note taking, during interviews, 185
- Notification, of relevant parties, 149–150
- Oaths, as sign of deception, 202
- Objectivity:  
in fraud risk assessment, 81  
in reporting of fraud risk assessment, 97
- Obligations under criminal law, of the  
individual, 61–63
- Occupational fraud, 8–35  
asset misappropriation, 8, 10–26  
corruption, 27–30  
defined, 8  
financial statement fraud, 30–35  
and Fraud Tree, 9*e*  
frequency by type, 9*e*  
median losses for, 10*e*
- Off-book schemes, 11
- Oman, 296–297  
anti-fraud programs in, 297  
legal/regulatory environment in, 297  
sources of information in, 296
- Omitted liabilities, 34
- On-book schemes, 12
- Online forms, as reporting mechanism, 117
- Online sources, 160–162
- Open-door policy, 121
- Open questions, in interviews, 190
- Operating effectiveness, of internal controls,  
92–93
- Operating environment,  
75–76
- Operational risk, 108
- Operations, changes in, 111
- Operations department, as information source,  
158
- Opinion testimony, rule against, 49–50
- Opportunities, to commit fraud, 87
- Opportunity, as component of Fraud Triangle, 6
- Organisation for Economic Co-operation and  
Development (OECD), 71, 276
- Organizational culture:  
and anti-fraud programs, 101–104  
and fraud risk, 76, 79  
support of whistle-blowing in, 120–121
- Organization-wide training,  
125
- Organized crime, 39
- Overbilling, through existing vendors, 17
- Overpayment of wages, 21
- Oversight, of anti-fraud programs, 101–107
- Overstated assets or revenues, 30–32
- Overstated expenses, 19
- Ownership, of fraud risk assessment process,  
99
- PACER database, 333
- Pakistan, 309–314  
anti-fraud programs in, 314  
legal/regulatory environment in, 311–313  
sources of information in, 309–311  
special considerations with fraud  
investigations in, 314
- Parties:  
likely to commit fraud, 91  
notification of relevant, 149–150
- Patient Protection and Affordable Care Act  
(ACA), 335
- Pay-and-return schemes, 17, 37
- Payroll fraud, internal controls to address risk  
of, 133
- Payroll schemes, 20–21

## Index

- PEACE framework, 194–196
- Peer pressure, 103–104
- Penn World Tables, 176
- Perceived opportunity, as component of Fraud Triangle, 6
- Performance goals, 124
- Personal Data Protection Act (Malaysia), 73, 225
- Personal Data Protection Act (Singapore), 67
- Personal Data Protection Act (Slovenia), 263
- Personal identity theft, *see* Identity theft
- Personal information, and data privacy laws, 71
- Personal Information Protection Act (South Korea), 239
- Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada), 73, 248
- Personally identifiable information (PII), 26, 41
- Personal Property Securities Register (Australia), 214
- Personal Property Security Register (New Zealand), 228
- Personal purchases, with company funds, 17
- Personnel-focused controls, 116–128
- Peru, 281–285
  - anti-fraud programs in, 284–285
  - legal/regulatory environment in, 282–284
  - sources of information in, 281–282
- Petty cash, conversion of, 4
- Philippines, 231–234
  - anti-fraud programs in, 233–234
  - legal/regulatory environment in, 232–233
  - sources of information in, 231–232
  - special considerations with fraud investigations in, 234
- Phishing, 40–41
- Physical assets, misappropriation of, 22–25, 134
  - larceny, unconcealed, 22–23
  - misuse, 22
  - receiving reports, falsified, 23–24
  - requisitions and transfers, fraudulent, 23
  - scrap inventory, 24
  - shipments of merchandise, fraudulent, 24
  - shrinkage, concealing, 25
- Physical evidence:
  - chain of custody with, 51–52
  - displaying, during interview, 198–199
  - preserving, 164
- Physical health, of interviewee, 181
- Physical security, 129
- Physician-patient privilege, 56
- Poland, 259–261
  - anti-fraud programs in, 261
  - legal/regulatory environment in, 260–261
  - sources of information in, 259–260
  - special considerations with fraud investigations in, 261
- Policy-focused controls, 128–131
- Policy statements, 104
- Polish Financial Oversight Commission, 260
- Polish Personal Data Protection Act, 259, 261
- Postal mail, as reporting mechanism, 117
- Predication, establishing, 143
- Preservation of evidence, employee failure in, 57–58
- Pressure to commit fraud, 5, 87
- Prevention of Electronic Crimes Act (Pakistan), 312
- Preventive controls, 110
- Priest-penitent privilege, 56
- Prioritization, of fraud risk, 93
- Privacy Act (Canada), 249
- Privacy laws:
  - data, 70–73
  - and private action investigations, 67–69
- Privacy rights:
  - of employees, 59–61
  - in the EU, 60–61
- Private facts, public disclosures of, 68–69
- Privileges:
  - and defamation, 66–67
  - legal, 52–56
  - waivers to, 53–54
- Probability, in estimation of fraud risk, 88–89
- Processes, changes in, 111
- Process-focused controls, 128–131
- Process-level controls, 110–111
- Professional standards, compliance with, 79
- Protection of Personal Information Act (POPI) (South Africa), 325
- Protections, legal, 52–56
- Protective bidding, 36
- Public disclosures, of private facts, 68–69
- Public Interest Disclosure Act (2013) (Australia), 216
- Publicity, of whistle-blowing helpline, 119
- Public recognition, of whistle-blowers, 121
- Public records, 159–160
- Punishment, as ineffective deterrent, 6–7

## INDEX

- Qichacha (website), 218
- Question(s):
- answering with, as sign of deception, 202
  - presenting alternative, in interviews, 199–200
  - repetition of the, as sign of deception, 201
  - sensitive, in interviews, 205
  - types of, in interviews, 188–194
- Ranking, of fraud risk, 93
- Ransomware, 39–40
- Rationalizations:
- as component of Fraud Triangle, 6
  - establishing, 198
  - reinforcing, 200
- Real evidence, 45
- Realistic goals, 148
- Reasonableness, of searches, 64
- Receivables skimming, 11–12
- Receiving reports, falsified, 23–24
- Recommendations, in fraud risk assessment, 98
- Reconciliations, 130
- Recording, of interviews, 184–185
- Reference checks, 123–124
- Refunds, false, 18
- Register, theft of cash from, 12
- Registry Court (Poland), 259
- Registry of Commerce and Companies (France), 343
- Regulations, compliance with, 79
- Regulatory issues, in international whistle-blowing, 119
- Regulatory misconduct, risk of, 87–88
- Reimbursements, duplicate/multiple, 19–20
- Related-party transactions, 34
- Relevant evidence, 46–47, 58
- Relevant parties, notification of, 149–150
- Religious legal systems, 43
- Remediation, following fraud, 137–138
- Remote interviews, 183–184
- Reporting:
- of cases, 166–171
  - confidentiality in, 107
  - in good faith, 107
  - requirements outlined in anti-fraud policy, 105
  - results of fraud risk assessment, 97–98
- Reporting mechanisms:
- accessibility of, 120
  - in whistle-blowing policies, 117–118
- Report to the Nations on Occupational Fraud and Abuse*, 7, 10, 13, 116, 117, 126, 130, 211, 217, 251, 265, 287, 303, 315, 329, 337
- Reputation risk, 88, 108
- Requisitions, fraudulent, 23
- Reserve Bank of Australia, 216
- Residual fraud risks, 76, 93–97
- Response:
- to fraud, as component of anti-fraud program, 136–138
  - to fraud risk, 93
- Responsibility:
- for anti-fraud programs, 111–116
  - for fraud prevention and detection, 104
  - for fraud risk assessment, 79–82
  - for fraud risk management, 99
  - for investigations, 105
  - of investigation team members, 147
- Revenues, overstated, 30–32
- Reviews, 130
- Rewards, for whistle-blowers, 120–121
- Rights:
- of employees, 56–61
  - of individuals, 56–57, 61–63
- Risk:
- categories of, 108
  - identifying contributors to, 78
- Risk and control personnel, 115
- Risk management, 108–109
- Roman law, 44
- Rotation, of job duties, 128
- Rutificador, 270
- Safety concerns, in cross-border investigations, 177
- Sales skimming, 11
- Sanctions, as ineffective deterrent, 6–7
- Sarbanes-Oxley Act of 2002 (SOX), 240, 334, 335
- Scheme-specific control activities, 131–136
- Scheme types:
- in Asia-Pacific region, 211, 212e
  - in Canada, 245, 246e
  - in Eastern Europe and Western/Central Asia, 251, 252e
  - in Latin America and the Caribbean, 265, 266e
  - in Middle East and North Africa, 287, 288e

## Index

- in Southern Asia, 303, 304*e*
- in Sub-Saharan Africa, 315, 316*e*
- in United States, 329, 330*e*
- in Western Europe, 337, 338*e*
- Scope:
  - of anti-fraud policy, 104
  - of investigations, 152–154
- Scope section (case reports), 170
- Scrap inventory, theft of, 24
- Searches, workplace, and privacy rights, 60–61
- Search and seizure, government, 63–65
- Search engines, 160–161
- Search operators, 160
- Search warrants, 64
- Secrecy, 6
- Secular legal systems, 43
- Securities and Exchange Commission (SEC), 334
- Securities and Exchange Commission of Pakistan, 310
- Securities and Exchange Commission of the Philippines, 231
- Security, physical, 129
- Security personnel, on investigation team, 145–146
- Segmented training, 126
- Segregation:
  - of documents, 162
  - of duties, 129
- Selective memory, 202
- Self-dealing, 34
- Self-evaluation (self-critical) privilege, 54–55
- Semistructured interviews, 83
- Senior management:
  - responsibilities of, in anti-fraud program, 113–114
  - whistle-blowing programs supported by, 118
- Separation of duties, 129
- Service de la Publicité Foncière*, 343
- Shadow bidding, 36
- Shariah law, 226
- Shell companies, false invoicing through, 16
- Shipments, fraudulent merchandise, 24, 35
- Shrinkage, concealment of, 25
- Signed statements, 206–208
- Silence, right to, 61–62
- Singapore, 234–237
  - anti-fraud programs in, 236–237
  - employee privacy rights in, 61
  - legal/regulatory environment in, 235–236
  - privacy laws in, 67
  - sources of information in, 235
  - special considerations with fraud investigations in, 237
- Skimming, 11–12
- Slander, 66
- Slovenia, 262–264
  - anti-fraud programs in, 264
  - legal/regulatory environment in, 263–264
  - sources of information in, 262–263
  - special considerations with fraud investigations in, 264
- Smiles, fake, 204
- Social engineering, 40–41
- Social media, 161–162
- Social status, maintaining, 6, 8
- Software:
  - encryption, 39–41
  - vulnerabilities of, 39
- Solicitor-client privilege, 53
- South Africa, 323–328
  - anti-fraud programs in, 327
  - legal/regulatory environment in, 325–327
  - sources of information in, 323–324
  - special considerations with fraud investigations in, 327–328
  - trials in, 63
- Southern Asia, 303–314
  - anti-fraud controls in, 303, 305*e*
  - detection methods in, 303, 304*e*
  - India, 305–309
  - Pakistan, 309–314
  - scheme types in, 303, 304*e*
- South Korea, 237–241
  - anti-fraud programs in, 240
  - legal/regulatory environment in, 238–240
  - sources of information in, 237–238
  - special considerations with fraud investigations in, 240–241
- SOX, *see* Sarbanes-Oxley Act of 2002
- Spain, 361–365
  - anti-fraud programs in, 364
  - legal/regulatory environment in, 363–364
  - sources of information in, 362–263
  - special considerations with fraud investigations in, 364–365
- Spear phishing, 40–41
- Specifications schemes, 36
- Specific goals, 148
- Speech patterns, changes in, 201



## INDEX

- Sponsor:
  - agreement of fraud risk assessment work by, 84–85
  - for fraud risk assessment, 79–80
- Spouse privilege, 55
- Statements, signed, 206–208
- State Secrets Law (China), 219
- Strategic risk, 108
- Structured interviews, 83
- Subjects (of investigations), 153
- Sub-Saharan Africa, 315–328
  - anti-fraud controls in, 315, 317*e*
  - detection methods in, 315, 316*e*
  - Kenya, 317–320
  - Mauritius, 320–323
  - scheme types in, 315, 316*e*
  - South Africa, 323–328
- Subsequent events, 34
- Suggestion boxes, as reporting mechanism, 117–118
- Summary section (case reports), 171
- Superintendence of Insolvency and Entrepreneurship (Chile), 271
- Superintendence of Securities and Insurance (Chile), 272
- Supervisory Control and Resolution Authority (ACPR) (France), 346
- Supplies, theft of, 22
- Surveys, in fraud risk assessment, 84
- Susceptibility, to fraud, 7
- Suspects:
  - interviewing, 166, 187
  - refusal to implicate other, 205
- Switzerland, 365–368
  - anti-fraud programs in, 367
  - legal/regulatory environment in, 366–367
  - sources of information in, 365–366
  - special considerations with fraud investigations in, 367–368
- Tailoring, bid, 36
- Taiwan, 241–244
  - anti-fraud programs in, 243
  - legal/regulatory environment in, 242–243
  - sources of information in, 241–242
  - special considerations with fraud investigations in, 244
- Targeted training, 126
- Technology:
  - and cross-border investigations, 178
  - data breaches, 39
  - as fraud risk, 76
  - misappropriation of information using, 26
  - ransomware, 39–40
  - software vulnerabilities, 39
- Telephone, as reporting mechanism, 117
- Terranet (New Zealand), 228
- Testimonial evidence, 45, 48
- Theft:
  - of cash on hand, 10
  - of cash receipts, 11–13
  - of incoming cash, 131–132
- Third parties:
  - external fraud by unrelated, 37–41
  - required for defamation, 66
  - as witnesses, 186
- Tianyancha (website), 218
- Time frame:
  - chronology of events, 163
  - of fraud investigation, 154
  - for interviews, 184
- Time off, mandatory, 128
- Timing differences, 31–32
- Tolerant attitudes, as sign of deception, 203
- Trade secrets, 25
- Training, 124–128
- Transactions, related-party, 34
- Transaction-level controls, 110–111
- Transfer(s):
  - of fraud risk, 96
  - fraudulent, 23
- Transparency International, 176
- Transportation issues, with cross-border investigations, 177
- Traumatic experiences, of interviewees, 181–182
- Treaty Establishing the European Union, 67
- Trial by jury, right to, 62–63
- Trust, in fraud risk assessment, 81
- Trust violators, 5
- UCC filings, 332
- Unconcealed larceny, 22–23
- Unconcern, feigned, 203
- UNdata, 176
- Understated liabilities or expenses, 32–33
- United Arab Emirates, 298–301
  - anti-fraud programs in, 300–301
  - employee privacy rights in, 61
  - legal/regulatory environment in, 299–300

## Index

- sources of information in, 298–299
- special considerations with fraud investigations in, 301
- United Kingdom, 368–371
  - anti-fraud programs in, 371
  - legal/regulatory environment in, 370
  - right to remain silent in, 62
  - sources of information in, 368–369
  - special considerations with fraud investigations in, 371
- United States, 329–336
  - anti-fraud controls in, 329, 331*e*
  - anti-fraud programs in, 335–336
  - detection methods in, 329, 330*e*
  - legal/regulatory environment in, 333–335
  - scheme types in, 329, 330*e*
  - sources of information in, 331–333
  - special considerations with fraud investigations in, 336
- Valuation, improper asset, 32
- Vendors:
  - collusion with company employees, 36–37
  - external fraud committed by, 35–37
  - internal controls to address risk of fraud involving, 136
  - overbilling through existing, 17
- Venue, interview, 183
- Verbal confessions, 205–206
- Video interviews, 183–184
- Voids, false, 18
- Vulnerabilities:
  - detection of, 78
  - to fraud, assessing, 142
- Wages, overpayment of, 21
- Wales, 62
- Wayback Machine, 161
- Well-defined goals, 148
- Western Asia, *see* Eastern Europe and Western/Central Asia
- Western Europe, 337–371
  - anti-fraud controls in, 337, 339*e*
  - Denmark, 339–342
  - detection methods in, 337, 338*e*
  - France, 342–349
  - Germany, 349–351
  - Greece, 352–353
  - Netherlands, 354–357
  - Norway, 357–361
  - scheme types in, 337, 338*e*
  - Spain, 361–365
  - Switzerland, 365–368
  - United Kingdom, 368–371
- Whistleblower Protection Act, 335
- Whistle-blower protections, 59, 106–107, 116–121
- White-collar crimes, 6
- “Wildcard” symbols, 161
- Witnesses, 45, 49–50
  - discussing, during interview, 199
  - interviewing, 166
  - neutral third-party, 186
- Workplace searches, 60–61
- Workshops, 83
- World Bank Group, 176
- World Factbook*, 176
- World Intellectual Property Organization, 25
- Written statements, of commitment to ethics, 102
- Wrongful discharge, 70

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>



<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>