

---

# Index

[References are to paragraphs (§) and appendixes (App.).]

(Bank Security Desk Reference—second revision 2004)

## A

- Access control, 4.08
- Advance-fee schemes, 2.03[6]
- Affidavits of forgery, 14.03[4]
- Al Qaeda, 601[1][c]
- Alarm systems
  - anti-ambush, 4.02[5][c]
  - ATMs, 4.02[4][c]
  - Bank Protection Act requirements, 1.02[2], 4.02
  - burglar alarms, 4.02[2]
  - cellular alarm transmission, 4.02[2][e]
  - central station, 4.02[2][c]
  - definitions, 4.02[1]
  - duress alarms, 4.02[5][d]
  - false alarms, 1.01[2][a]
  - fire, 4.02[6]
  - foot rails, 4.02[5][b]
  - holdup buttons, 4.02[5][a]
  - line security, 4.02[2][e]
  - local, 4.02[2][a]
  - money clips, 4.02[5][c]
  - night depositories, 4.02[4][c]
  - perimeter protection, 4.02[3]
  - piggybacking, 4.02[2][d]
  - police connect, 4.02[2][b]
  - proprietary, 4.02[2][d]
  - robbery, 4.02[5]
  - safes, 4.02[4][b]
  - updating, 4.02[7]
- Underwriters Laboratories (UL)
  - certificate, 4.01[1]
  - testing, 4.01[2]
  - vault, 4.02[4][a]
- Alcoholism. *See* Substance abuse
- American Bankers Association
  - ATM crime study, 2.02[4]
  - certification, security officer, 3.02[3][d]
  - check fraud survey, 14.01[2]
  - digital signature rules, 8.04[2][b]
  - fingerprinting, 7.01[3]
  - touch signature fingerprint program, 14.07[6]
- American Bankers Professional and Fidelity Insurance Company, 3.03[2][f]
- American Society for Industrial Security Code of Ethics, 3.06
- Americans With Disabilities Act, 7.05
- ANSI, 4.08[3], 8.04[4][d]
- Anti-ambush alarm, 4.02[5][c]
- Anti-crime legislation. *See* Crime legislation
- Applicant screening, 7.01
  - Americans With Disabilities Act, 7.05
  - applicant's signature, 7.01[2][d]
  - arrest information, 7.01[2][b]
  - computerized source records, 7.01[5][e]
  - consent agreements, 7.01[2][c]
  - credit checks, 7.01[2][c]
  - criminal records, 7.01[2][b]
  - employment application, 7.01[2]
  - Fair Credit Reporting Act, 7.01[6]
  - FDIC Act, Section 19, 7.01[4]
  - fingerprinting, 7.01[3], 14.07[6]
  - gas chromatograph test, 7.01[7]
  - honesty test, 7.01[5][d]
  - interviewer, 7.01[1]
  - investigative agencies, 7.01[5][b]
  - mail reference checks, 7.01[5][a]
  - medical history, 7.01[7]
  - polygraph, 7.01[5][c], 10.07
  - Private Security Officer Employment Authorization Act, 7.01[8], App. 15
  - urinalysis, 7.01[7]
  - verification procedures, 7.01[5]
- Arrest elements, 10.13[1]
- Arrest information, 7.01[2][b], 7.01[3], 7.01[4]
- Arrest powers, 10.14
- Arrest records, 7.01[2][b], 7.01[3], 7.01[4]
- Arrest, without a warrant, 10.14[3]
- Arson, 6.02[1][h]
- ATM
  - access control, 11.03[2][c], 11.03[4]
  - alarm protection, 4.02[4][c], 11.03[1][b]
  - burglary, 2.02[2]
  - camera surveillance, 4.03, 11.03[1][c], 11.03[4]
  - card and PIN distribution, 11.03[3][c]
  - card and PIN management, 11.03[3]
  - checklists, 11.05
  - civil liability, 2.02[4][c]
  - consumer education, 11.03[4]
  - crime
    - card fraud, 2.03[5][b]
    - customer attacks, 2.02[4]
    - fraud investigations, 2.03[5][b]
  - currency
    - replenishment, 11.04[2][a]
    - transport, 11.04[2][c]
  - customer deposits, 11.04[2][a]
  - customer safety, 11.03[4]
  - dual control, 11.04[1]
  - dye packs, 4.12
  - environment, 11.03[2]
  - FDIC smart card overview, 11.01[4][b]
  - food stamp payments, 11.03[4][c]

## BANK SECURITY DESK REFERENCE

[References are to paragraphs (§) and appendixes (App.).]

- fraud investigation, 11.03[3][e]
  - free-standing, 11.01[1][b]
  - functions, 11.01
  - Gramm-Leach-Bliley Act, 11.02
  - “hot card” list, 11.03[3][d]
  - internal control questionnaire, 11.05[6]
  - legislation, security, 11.03[5]
  - lighting, 4.04[1][c], 11.03[2][b], 11.03[4]
  - local laws, 11.03[5][c]
  - lost and stolen cards, 11.03[3][d]
  - on-premises ATMs, 11.01[1]
  - personal identification number, 11.03[3]
  - personnel access to, 11.03[2][c], 11.03[4]
  - point-of-sale terminals, 11.01[4]
  - Regulation E, 11.02, App. 7.3
  - remote, FDIC approval, 11.03[2][d]
  - repairs, 11.04[2][b]
  - safe, 4.06[3], 11.03[1][a]
  - security
    - checklist, 11.05
    - consideration for installation, 11.03
    - service personnel, 11.04[2], 11.05[5]
    - shared networks, 11.01[3]
    - site selection, 11.03[2]
    - smart cards, 11.04[4]
    - state laws, 11.03[5][b]
    - vendor personnel, 11.04
    - welfare payments, 11.03[4][c]
  - Audit committees, 2.01[2][b]
  - Auditing
    - EDP, 5.04[1][d], 5.05[2]
    - scope of security audit, 3.04[2], App. 12.2, App. 12.5
    - security department, 3.04[2]
    - security officer’s role, 3.04[3], App. 12.2
  - Authentication, 8.02[2][c], 8.03[4]
  - Automated Clearing House, 8.05[3][c]
  - Auxiliary safes, 4.06[1]
- B**
- Bad debt, 10.12
  - Bahamas Monetary Act of 1968, 2.03[7]
  - Bait money, 6.05[2][e]
  - Bandit barriers, 4.09[3]
  - Bank Administration Institute
    - ATM crime study, 2.02[4], 2.03[5][b]
    - bank interior design, 4.09
    - Bank Protection Act survey, 1.03[1]
    - bank robbery study, 4.09
  - Bank bribery. *See* Code of conduct
  - Bank Bribery Amendments Act of 1985, 7.04[3]
  - Bank failures, 2.01[2][a]
  - Bank fraud. *See* Crime in financial institutions
  - Bank Protection Act of 1968
    - alarm system, 4.02
    - cameras, 4.03
    - compliance by banks, 1.03
    - congressional hearings, 1.02
    - daily operating procedures, 9.02
    - directors, 1.02[1], 1.02[2][c]
    - law, App. 1.1
    - lighting, 1.02[2], 4.04
    - locks, 1.02[2], 4.05
    - overview, 1969 regs., 1.02[1]
    - regulations, App. 1
    - reports
      - compliance, 1.02[2][c]
      - crime, 1.02[2][c]
      - security devices, 1.02[1][b]
    - required equipment, 1.02[2][b]
    - safes, 1.02[2], 4.06
    - security officer, designation, 1.02[2][a]
    - security program, 1.02[2][b]
    - training, 9.01[1]
    - U.S. Marshals’ survey, 1.03[1]
    - vaults, 1.02[2], 4.07
    - violations, penalty for, 1.02
    - written security procedures, 1.02[1][c], 3.07
  - Bank robbery
    - prevention, 9.02[4][a]
    - profile of bank robbers, 2.02[1][a]
    - prosecutions, 2.02[1][b]
    - response, 9.02[4][c]
    - statistics, 1.01, 2.01[1], 2.02[1][c]
    - study by BAI, 4.09
    - training of employees, 9.02[4]
  - Bank Secrecy Act
    - bulletin board, 13.03
    - businesses not excluded from reporting, 13.03[2][c]
    - cedular card, 13.03[8]
    - CHIPS, 13.02[1][b]
    - compliance requirements, 13.03[4], 13.03[5], App. 12.1
    - currency transactions reporting, 13.03[2][a]
    - customer identification program, 14.02[1]
    - disabled persons, 13.03[2][a][i]
    - elderly persons, 13.03[2][a][i]
    - employee training, 13.03[5]
    - examination guidelines, 13.03[6][b], 13.03[7], App. 2.9
    - exempt persons, 13.03[2][b]
    - exempt transactions, 13.03[2][a]
    - Fedwire, 13.02[1][b]
    - Financial Action Task Force, 13.02[1][b]
    - FinCEN, 13.02
    - foreign banks, 13.03[2][c]
    - internal controls, 13.03[5]
    - “know your customer,” 9.02[8], 13.03[5][c], 14.02
    - laundering money, 13.01, 13.02
    - law, App. 2.1, App. 2.2, App. 2.3
    - Money Laundering Control Act of 1986, 13.04[2], App. 2.3
    - Money Laundering Suppression Act of 1994, 13.01[5]
    - multiple transactions, 13.03[2][a][ii], 13.03[2][g]
    - “payable through” accounts, 13.02[2], 13.03[5][f], App. 12.9
    - penalties for violations, 13.03[7]

[References are to paragraphs (§) and appendixes (App.).]

- purpose, 13.01[1]
  - questions and answers, 13.03, 13.03[8]
  - Ratzlaf v. United States, 13.02[2][g]
  - record-keeping requirements, 13.03[2], 13.02[2][d]
  - reporting requirements, 13.03[2]
  - “Safe Harbor” law, 13.02[2][h]
  - Seychelles, republic of, 13.02[1][b]
  - study by Indiana Univ., 2.02[1][a]
  - suspicious conduct, 9.02[8][c]
  - SWIFT, 13.02[1][b]
  - taxpayer identification records, 13.03[3]
  - tellers, 9.02[8]c[i]
  - training requirement, 13.03[4], 13.03[5]
  - transactions of exempt persons, 13.03[2][b]
  - transportation of currency report, 13.03[2][b]
  - violations, 13.03[7]
  - wire transfer, 13.03[5][a]
  - Bank security
    - history, 1.01
  - Bankers blanket bond. *See* Financial institution bond
  - Banking office interior design, 4.09
  - Banking office security
    - bait money procedures, 9.02[4][b]
    - Bank Protection Act requirements, 1.02[2], 9.01[1]
    - bank robbery prevention, 9.02[4][a]
    - bank robbery response, 9.02[4][c]
    - bomb threats, 6.03[2][c], 6.05[1]
    - burglary alarms, 9.02[12][b]
    - burglary response, 9.02[5]
    - cash control procedures, 9.02[3][a]
    - closing procedures, 9.02[2]
    - during banking hours, 9.02
    - keys and locks, 9.02[3][b]
    - opening procedures, 9.02[1]
    - protective lighting systems, 9.02[2]
    - robbery alarms, 9.02[11][a]
    - surveillance cameras, 9.02[12][c]
    - testing records, 9.02[12][e]
    - transport of cash, 9.02[3][a][iii]
    - vault procedures, 9.02[3][a][i]
    - wastepaper, 9.02[3][a][iv]
  - Banks operating without authorization, 2.05
  - Baseline security controls, 5.03[3]
  - Belize, unauthorized banks, 2.05[2]
  - Biometric identification systems, 8.04[4][e]
  - Biological weapons, 6.05[9]
  - Bomb threat
    - advance precautions, 6.05[1][b]
    - emergency planning, 6.03[2][c], 6.05[1]
    - evacuation, 6.05[1][d]
    - intelligence assessment, 6.05[1][a]
    - safe-deposit boxes, 6.05[1][e]
    - training, response, 9.02
    - warning checklist, 6.05[1][b]
  - Bombings
    - Oklahoma City, 6.03[2][c][i]
    - World Trade Center, 6.01, 6.03[2][c][i]
  - Branch interior design, 4.09
  - Bribery, 7.04[3]
  - Brokered loan fraud, 2.03[8]
  - Bugging, 4.10
  - Bullet-resistant barriers, 4.09[3]
  - Burglar alarms, 4.02[2], 9.02[12][b]
  - Burglary, 2.02[2], 9.02[5]
  - Burning bar, 2.02[2]
- C**
- California ATM law, Ex. 11.1
  - Camera surveillance equipment
    - ATMs, 11.03[1][c]
    - Bank Protection Act requirements, 4.03
    - check fraud prevention, 14.05[3][c]
    - closed-circuit television, 4.03[1][d]
    - demand cameras, 4.03[1][b]
    - film camera vs. video, 4.03[1][e]
    - intelligent video, 4.03[1][a]
    - lens selection, 4.03[1][c]
    - positioning cameras, 4.03[2]
    - selection, 4.03[1]
    - sequence cameras, 4.03[1][a]
    - testing, 9.02[12]
    - Underwriters Laboratories (UL), testing, 4.03[1]
  - Canada, unauthorized banks, 2.05[3]
  - Card access, 4.08
  - Cash control, 9.02[3][a]
  - Cash transport, 9.02[3][a][iii]
  - Cedular card, 13.03[8]
  - Cellular alarm transmission, 4.02[2][e]
  - Centers for Disease Control, 6.05[9][a][iii]
  - Central station alarms, 4.02[2][c]
  - Certification, security officer, 3.02[3][d]
  - Certificate authorities, 8.04[3]
  - Check 21, 14.04[3][e]
  - Check cashing
    - customer identification, 9.02[8], 14.02
    - Federal Reserve routing numbers, Ex. 14.5
    - Treasury rules, 14.04[4]
  - Check clearing, 14.04[3][e]
  - Check dishonor, 14.04[4][b]
  - Check fraud, Chapter 14
    - advice from a forger, 14.06[5]
    - ASI/16 detection, 14.07[1]
    - ASI/19 detection, 14.07[2]
    - authenticated electronic checks, 14.07[14]
    - automated fraud management system, 14.07[8]
    - counterfeit checks, 14.03[5], 14.07
    - electronic check presentment, 14.07[12]
    - enhanced check paper, 14.07[7]
    - false identification, 14.02[6]
    - forgery, 2.03[4][a], 14.03, 14.06[6][a]
    - FraudBAN, 14.07[9]
    - handwriting analysis, 14.05[3][b]
    - Identity Theft and Assumption Deterrence Act of 1998, 14.02[6][b][i], App. 9.5
    - insiders, 14.08[2]
    - investigation, 14.05

## BANK SECURITY DESK REFERENCE

[References are to paragraphs (§) and appendixes (App.).]

- kitting, 2.03[4][b], 14.03[6], 14.06[6][b], 14.07[4]
- laws, 14.05[1]
- losses, 2.03[4], 14.01
- new technology, 14.07
- opening new accounts, 14.02
- payment on uncollected items, 14.04[4][c]
- Payment Solutions Network, Inc., 14.07[5][a]
- Positive pay, 14.07[10]
- prevention checklist, 14.06[6]
- Primary Payment Systems, Inc., 14.07[5][b]
- reverse positive pay, 14.07[11]
- Touch Signature Fingerprint Program, 14.07[6]
- training, detection, 14.06
- Uniform Commercial Code, 14.04[4]
- U.S. Secret Service investigations, 2.03[4]
- Check kiting, 2.03[4][b], 14.03[6], 14.06[6][b]
- Check Print program, 14.05[5]
- Check processing, 14.04
- Chemical weapons, 6.05[11]
- Child pornography, preventing, 2.04[24]
- Civil defense, 6.03[1]
- Civil disturbances, 6.02[1][f], 6.05[3]
- Civil liability, 2.01[2][e], 2.02[4][c]
- Closed-circuit television, 4.03
- Closing procedures, 9.02[2]
- Code of conduct, 7.04, 7.04[3][b]
  - Comprehensive Crime Control Act of 1984, 7.04[3]
    - elements, 7.04[1]
    - FDIC guidelines, 7.04[4]
    - federal regulations, 7.04[3][b]
    - Foreign Corrupt Practices Act, 7.04[2]
- Code of ethics for security personnel, 3.06
- Color copy reproductions, 9.02[10][b]
- Combination locks, 4.05[2]
- Commercial loans, 10.12[1]
- Communications
  - emergency, 6.04[5]
- Compliance reports, 1.02[6]
- Comprehensive Crime Control Act of 1984, 7.04[3]
- Comptroller of the Currency
  - ATM security, 11.05[6]
  - Bank Protection Act of 1968, 1.02, App. 1.4
  - crime reports, 2.04
  - unauthorized banks, 2.05[1]
- Computer crime, 2.03[9], 5.01, 8.02
- Computers
  - See also* Data security
  - access control, 5.04[6][d]
  - alarm systems, 4.02
  - assignments, 5.04[5][a]
  - audit checklist, 5.04[1][f]
  - auditor, 5.04[1][d], 5.04[1][f]
  - baseline security controls, 5.03[3]
  - bulletin board, Bank Secrecy Act, 13.03
  - business driven, 5.01[1]
  - communications control, 5.04[2]
  - compliance statement, 5.04[5][a], Ex. 5.6
  - Computer Fraud and Abuse Act of 1986, 5.02[1][a], 8.01[6]
  - contingency planning, 5.04[7], 6.04[4][a], App. 12.3
  - crime, 2.03[9], 5.01, 8.01[6], 8.02, 10.11
  - data processing management, 5.04[1][c]
  - data security officer, 5.04[1][e]
  - design and construction, 5.04[6][b]
  - Electronic Communications Act of 1986, 5.02[1][b]
  - encryption, 8.04[1]
  - end-user computing, 5.05
  - exposure, 5.01, 8.02
  - fire protection, 5.04[6][c]
  - firewalls, 8.04[5]
  - fraud, 5.01[5][a]
  - fraud legislation, 5.02
  - glossary, 5.01[4], Ex. 5.1
  - hacker prevention, 8.04[6]
  - hackers, 8.03[3][b]
  - home banking, 8.01[3]
  - information integrity, 5.04[2][b]
  - information security, Ch. 15
  - Internet, 8.01[1], 8.02, 8.03, 8.04, 8.05
  - legal, 5.01[3]
  - on-line terminals, 8.01
  - personal, 5.05, 8.04[10]
  - personnel security, 5.04[5]
  - physical security, 5.04[6]
  - privacy, 5.04[3][c], Ch. 15
  - safety and soundness, 5.01[2]
  - security control domains, 5.04
  - security program, 5.03
  - security protection, 8.04
  - service contracts, 5.01[5][f], App. 12.6
  - site selection, 5.04[6][a]
  - software, 5.01[5][b]
  - state crime laws, 5.02[2]
  - telecommunications law, 5.02[1][b]
  - theft of customer data, 5.01[5][d]
  - theft of financial assets, 5.01[5][a]
  - theft of hardware/software, 5.01[5][b]
  - users, 5.04[1][b]
  - viruses, 5.01[5][e], 5.04[3][d], 8.02[4], 8.04[11]
- Confidence schemes, 9.04[1]
- Consultants, use in security department, 3.05
- Consumer Credit Protection Act, 7.01[6]
- Contingency management officer, 6.04[1]
- Contingency management team, 6.04[2]
- Contingency planning
  - alternative locations, 6.04[5][c]
  - anthrax, 6.05[9][a]
  - biological weapons, 6.05[9]
  - bomb threats and bombings, 6.03[2][c], 6.05[1]
  - Centers for Disease Control, 6.05[9][a][iii]
  - Checklist for evaluating readiness, 6.06Ex.6.8
  - chemical weapons, 6.05[11]
  - command center, 6.04[3]
  - communications, 6.04[4]

[References are to paragraphs (§) and appendixes (App.).]

- contingency management officer, 6.04[1]
- contingency planning, 6.01, App. 12.4
- continuity of management, 6.03[2]
- corporate responsibility, 6.03[2]
- critical infrastructure, 6.01[3]
- data processing, 6.03[2][a], 6.04[5][d]
- defined, 6.01
- developing the plan, 6.05
- electrical blackouts and brownouts, 6.03[2][h], 6.05[4]
- electronic imaging, 6.04[8]
- elements of an emergency plan, 6.04
- exercising the plan, 6.05[13]
- fire, 6.03[2][i], 6.05[5]
- FS-ISAC, 6.01[3][b]
- FSSCC, 6.01[3][a]
- homeland security, 6.01[2], App. 13.3
- human-induced emergency, 6.03[1]
- information technology systems, 6.03[2][a], 6.04[5][d]
- interagency policy, 6.01[3], 6.06, App. 12.4
- international terrorism, 6.01[4], 6.01[5]
- key personnel, 6.04[5][b]
- kidnapping, hostage taking, and extortion, 6.03[2][b], 6.05[2]
- mail bombs, 6.05[1]
- mutual aid, 6.01
- natural emergencies, 6.03[3], 6.05[6]
- nuclear war, 6.03[2][f], 6.05[7]
- officer designate, 6.04[1]
- operational considerations, 6.04
- pandemics, 6.03[3], 6.05[10]
- policy statement, 6.02[2]
- recovery checklist, 6.06
- riots and civil disturbance, 6.03[2][g], 6.05[3]
- risk assessment, 6.03
- sabotage, 6.03[2][e]
- senior management, 6.04[1]
- temporary offices, 6.04[5][c]
- terrorism, 6.01, 6.03[2][d]
- testing the plan, 6.05[10]
- U.S. government responsibility, 6.02[2]
- vital records protection, 6.04[7]
- Continuity of management, 6.02[2]
- Corporate security, 3.01
- Costs
  - controllable/noncontrollable, 3.04[1][b]
  - direct/indirect, 3.04[1][a]
  - fixed/variable, 3.04[1][c]
- Counter audio
  - countermeasures, 4.10[2]
  - listening devices, 4.10[1]
- Counterfeit checks, 14.04[5]
- Counterfeit commercial instruments, 2.03[11][c]
- Counterfeit currency, 2.03[11][a], 9.02[10][a]
- Counterfeit securities, 2.03[11][b]
- Credit card fraud, 2.03[5][a], 8.02[3][a]
- Credit Card Fraud Act of 1984, 2.03[5][c]
- Crime growth
  - Post-World War II, 2.01
  - Pre-World War II, 1.01
- Crime in financial institutions
  - advance-fee schemes, 2.03[6]
  - ATM fraud, 2.03[5][b]
  - bank bribery, 2.03[14]
  - bank failures, 2.01[2][a]
  - Bank Fraud Statute, 2.03[2][b]
  - bank robbery, 2.02[1]
  - brokered-loan fraud, 2.03[8]
  - burglary, 2.02[2]
  - causes for increase, 2.03[1]
  - check forgery, 2.03[4][a], 14.01
  - check fraud, 2.03[4], 14.01
  - check kiting, 2.03[4][b], 14.03[6], 14.06[6][b]
  - computer crime, 2.03[9], 5.01, 8.01[6], 8.02
    - definition of, 10.11[2]
    - investigating, 10.11
  - confidence schemes, 9.04[1]
  - cost, 1.01, 2.01
  - counterfeiting, 2.03[11]
  - credit card fraud, 2.03[5][a], 8.02[3][a]
  - customer attacks, 2.02[4]
  - cyber crime, 8.02[3][a]
  - economic espionage, 2.03[22]
  - embezzlement, 2.03[2]
  - embezzler traits, 2.03[2][d]
  - extortion, 2.02[3]
  - false bank entries, 2.03[2][c]
  - fraud penalties, 1.07[2]
  - Identity theft, 2.03[20], 8.02[5][c], 14.02[6][b][i], App. 9.5
  - impact on banks, 2.01[2][a]
  - interstate commerce of stolen property, 2.03[15]
  - kidnapping, 2.02[3]
  - laws, App. 9.1
  - loan fraud, 2.03[3], 9.02[9]
  - mail fraud, 2.03[17]
  - offshore shell bank, 2.03[7]
  - pretexting, 2.03[23], 8.02[3][f]
  - prevention, 9.02
  - reports, 2.04, App. 9.4
  - RICO, 2.03[18]
  - severity, 1.01[1]
  - telemarketing fraud, 2.03[16]
  - theft of securities, 2.03[12]
  - travelers' check fraud, 2.03[10]
  - violent crimes, 2.02
  - white-collar crime, 2.03
  - wire fraud, 2.03[13]
  - workplace violence, 7.06
- Crime investigation. *See* Investigation of internal crime
- Crime legislation
  - Anti-Drug Abuse Act, 13.01[3]
  - Bank Protection Act, App. 1
  - Bank Secrecy Act, 13.01[1]
  - embargoed countries, 2.03[19]
  - Federal Deposit Insurance Act, Section 19, 7.01[4]

*[References are to paragraphs (§) and appendixes (App.).]*

Identity Theft and Assumption Deterrence Act of 1998, 14.02[6][b][i], App.9.1  
 International Emergency Economic Powers Act, 2.03[19][b]  
 International Security and Development Corporation Act, 2.03[19][e]  
 Iraq Sanctions Act, 2.03[19][c]  
 SEC Rule 17 F-1, 1.04  
 SEC Rule 17 F-2, 1.05  
 Telephone Records and Privacy Protection Act of 2006, 2.03[23], App.9.1  
 Title 18 of the U.S. Code, 2.03[19][f], App. 9  
 Trading With the Enemy Act, 2.03[19][a]  
 United Nations Participation Act, 2.03[19][d]  
 Crime prevention  
     duties of security officer, 3.02  
     workplace violence, 7.06  
 Crime reports. *See* Reports  
 Criminal activity reporting, 2.04  
 Criminal prosecution, 2.03, 10.18  
 Criminal victimizations, 1.01, 2.06  
 Crisis management. *See* Contingency planning  
 Currency and Foreign Transactions Reporting Act, 13.01  
 Currency transactions reports. *See* Bank Secrecy Act  
 Currency, color, Ex. 9.4.A  
 Customer identification program, 13.03[2]  
 Customers, 2.02[4], 9.04, 11.03[4], 14.02  
 Cyber crime, 8.02[3][a]

**D**

Daily operating procedures. *See* Banking office security  
 Data encryption standard, 8.04[1]  
 Data processing terms, 5.01[4], Ex. 5.1  
 Data integrity, 8.02[2][b], 8.03[3]  
 Data privacy, 8.02[2][a], 8.03[2]  
 Data security  
     *See also* Computers, Internet  
     ANSI, 8.01  
     authentication, 8.02[2][c], 8.03[4]  
     biometrics, 8.04[4][d]  
     contingency controls, 5.04[7], 6.04  
     certificate authorities, 8.04[3]  
     crime, 5.01, 8.01[6], 8.02  
     data encryption standard (DES), 8.04[1]  
     digital signatures, 8.04[2]  
     electronic data interchange (EDI), 8.01[2]  
     encryption, 8.04[1]  
     end-user computing, 5.05  
     firewalls, 8.04[5]  
     hacker, 8.02[3]  
     home banking, 8.01[3]  
     information integrity, 5.04[2][b]  
     Internet, 8.01[3], 8.03[1]  
     management responsibility, 5.04[1]  
     message testing, 5.04[2][b][i]  
     non-repudiation, 8.02[2][d], 8.03[5]  
     operational controls, 5.04[4]

password security, 8.04[4][a]  
 passwords, 5.04[3][a], 8.04[4][a]  
 privacy, 8.05, Ch. 15  
 processing controls, 5.04[4][b]  
 risk assessment, 5.01[1]  
 Rivest-Shamir-Adelman (RSA), 8.04[1]  
 security protection, 8.04  
 sensitive data, 5.04[3][c]  
 smart cards, 8.04[4][c]  
 software vulnerabilities, 8.02[6]  
 systems/applications controls, 5.04[3]  
 systems logging, 5.04[5][b]  
 telegraphic testing, 5.04[2][b][ii]  
 text validation, 5.04[2][b][iii]  
 tokens, 8.04[4][b]  
 verification controls, 5.04[4][c], 8.03[5]  
 viruses, 5.01[e], 8.02[4], 8.04[11]  
 Web-linking risks, 8.02[4]  
 wireless technology, 8.02[5]  
 Data security officer, 5.04[1][e]  
 Debit card, 11.01  
 Demand cameras, 4.03[1][b]  
 Department of Homeland Security, 6.01[2], Ex. 6.10, Ex. 6.11  
 Depository trust company, 5.01  
 Depressants, 7.02[4][a][iii]  
 Deputization powers, 10.15[3][c]  
 DES, 8.04[1]  
 Digital signatures, 8.04[2]  
 Directors, 1.02[2][a], 2.01[2][e]  
 Dirty bomb, 6.03[7][e]  
 Disaster recovery checklist, 6.06  
 Document examiner, 14.05[3][b]  
 Driver's licenses, 14.02[6][c]  
 Drug abuse. *See* Substance abuse  
 Drug testing. *See* Substance abuse  
 Dual control, 4.05[6][b], 11.04[1]  
 Duress alarms, 4.02[5][d]  
 Dye pack, 4.12

**E**

Eavesdropping. *See* Counter audio  
 e-commerce, 8.01[5], 8.02[3][a], 15.04  
 Economic Espionage Act of 1996, 2.03[22]  
 EFTs  
     contingency planning, 6.04[4]  
 Electrical blackouts, 6.02[1][g], 6.05[4]  
 Electromechanical locks, 4.05[5]  
 Electronic card access, 4.08  
 Electronic commerce, 8.01[5], 15.04  
 Electronic data interchange, 8.01[2]  
 Electronic Fund Transfer Act, App. 7.3  
 Electronic imaging systems, 6.04[8]  
 Electronic payment processing, 8.01, 9.02[11], 14.04[3][e], 14.07[12], 14.07[14]  
 Electronic surveillance, 4.10, 10.10  
 E-mail, 8.05[1][c]  
 Embargoed countries, 2.03[19]  
 Embezzler traits, 2.03[2][d]  
 Embezzlement, 2.03[2]

[References are to paragraphs (§) and appendixes (App.).]

- Emergency communications, 6.04[4]
  - Emergency planning, *See* Contingency planning
  - Employee searches, 10.13
  - Employee training. *See* training
  - Employment application, 7.01[2]
  - Encryption, 8.04[1]
  - End-user computing, 5.05
  - Entities operating without authorization, 2.05
  - Environmental audits, 9.02[9]
  - Environmental risk, 3.03[3], App. 12.10
  - Environmental safety, 4.09[4]
  - Espionage, 2.03[22]
  - Ethics, security personnel, 3.06
  - Evidence from searches, 10.13[2]
  - Executive Orders
    - emergency preparedness, 6.02[2]
      - homeland security, 6.01[2], App. 13.3
      - targeting terrorist assets, App. 13.2
  - Expedited Funds Availability Act, 14.04[3]
  - Extortion
    - emergency planning, 6.03[2][b], 6.05[2]
    - statistics, 2.02[3]
    - training, prevention/response, 9.02[6]
  - Eye scan, 4.08[3][b], 8.04[4][ii]
- F**
- Fair Credit Reporting Act, 7.01[6]
  - Fallout shelter, 6.03[7][e]
  - False alarms, 1.01[2][a]
  - False identification, 14.02[6]
  - Fast Track Program, 10.18[1]
  - FDIC
    - code of conduct guidance, 7.04[4]
    - e-mail guidance, 8.05[1][c]
    - instant messaging guidance, 8.05[1][d]
    - study on identity theft, 8.05[5]
  - FDIC Improvement Act of 1991, 2.01[2][b]
  - Federal Bureau of Investigation
    - bank robbery, 2.02[1]
    - burglary, 2.02[2]
    - computer crime, 8.01[6]
    - embezzlement, 2.03[2]
    - fingerprinting, 7.01[3]
    - kidnapping, 2.02[3], 6.03[2][b]
    - loan fraud, 2.03[3]
    - offices, App. 5.3
    - violent crimes subprogram, 2.02
  - Federal Computer Crime Law
  - OCC guidance, 5.02[1][c][ii]
    - Statute, 5.02[1][c]
  - Federal Deposit Insurance Corp., 1.02
    - Bank Protection Act of 1968, App. 1.3
    - banks supervised, 2.01[2][a]
    - FDIC Act, Section 19, App. 6.1, 7.01[4], App. 6.2
    - FDIC Act, Section 39, 3.03[4]
    - Internet security risks, 8.05[2][b]
    - online privacy guidance, 8.05[2]
    - remote ATM approval, 11.03[2][d]
    - smart card overview, 11.01[4][b]
    - vacation policies, 7.07[4]
  - Federal Privacy Laws and Self-Regulation
    - banking industry, 15.02
    - Gramm-Leach-Bliley Act, 15.02[1]
    - Insurance industry, 15.03[2]
    - Investment companies, 15.03[10]
    - Securities industry, 15.03[9]
  - Federal Reserve System
    - Bank Secrecy Act examinations, 13.03[7], App. 2.9
    - banks supervised, 1.02
    - information security guidance, 8.05[4]
    - postwar attack, 6.05[7][d]
    - Regulation CC, 14.04[3]
    - routing numbers, Ex. 14.5, 14.04[1]
    - vital records defined, 6.04[7]
  - FFIEC Internet authentication guidance, Ex. 8.3
  - File transfer controls, 8.03[6]
  - Files, investigative, 10.17
  - Financial institution bond, 3.03[2][a]
  - FinCEN, 13.02
  - Fingerprinting, 7.01[3]
    - Access control, 4.08[3][a], 8.04[4][d][i]
    - FDIC Act, Section 19, 7.01[4]
    - guards, 7.01[8], App.15
    - SEC Rule 17 F-2, 1.05
    - Touch Signature Fingerprint Program, 14.07[6]
  - Fire alarms, 4.02[6], 6.05[5]
  - Firearms, 1.01[2][a], 4.11[5]
  - Fire classification, 6.05[5]
  - Fire evacuation, 6.05[5][b]
  - Fire planning, 6.02[1][h], 6.05[5]
  - Fire training, 9.03[3]
  - Firewalls, 8.04[5]
  - Fire wardens, 6.05[5][a]
  - Food stamp payments, 11.03[4][c]
  - Foot-candle measurement, 4.04[1][a]
  - Foreign assets control regulations, App. 13
  - Foreign Corrupt Practices Act, 7.03[2]
  - Foreign governments, 8.02[3][d]
  - Forgery. *See* Check fraud
  - FS-ISAC, 6.01[3][b]
  - FSSCC, 6.01[3][a]
  - Funds availability, 14.04[3]
- G**
- Gambling, 7.03
  - Gifts, acceptance of, 7.03
  - Gramm-Leach-Bliley Act, 15.02[1], App. 2.7.1, 3.03[4]
  - Guards
    - armed vs. unarmed, 4.11[5]
    - bulletproof vests, 4.11[4]
    - contract, 4.11[2]
    - fingerprinting, 7.01[8], App.15
    - job description, 3.02[1]
    - justifying, 4.11[1]
    - Private Security Officer Employment Authorization Act, 7.01[8], App. 15

## BANK SECURITY DESK REFERENCE

*[References are to paragraphs (§) and appendixes (App.).]*

- qualifications, 4.11[2]
  - regulation, 4.11[6]
  - using public police, 4.11[3], 1.01[2]
- H**
- Hackers, 8.02[3][a][b]
  - Hair testing, 7.01[7][b]
  - Hand geometry, 4.08[3][c], 8.04[4][v]
  - Handwriting analysis, 14.05[3][b]
  - Hidden assets, 10.12[3]
  - Hobbs Act, 2.02[3], 6.02[1][a]
  - Holdup alarms, 4.02[5]
  - Home banking, 8.01[3]
  - Homeland security, 6.01[2]
  - Honesty tests, 7.01[5][d]
  - Hostage situations, 6.03[2][b], 6.05[2], [9.02[6]
  - Human resources. *See* Personnel security
  - Hypnosis, 10.08
- I**
- IC3, 8.01[3]
  - Identification
    - biometric systems, 4.08[2], 8.04[4][d]
    - customer identification program, 13.03[2]
    - customers, 9.02[8], 14.02
    - personal, 4.08[2]
    - RFID systems, 4.08[4]
  - Identity Theft and Assumption Deterrence Act of 1998, 14.02[6][b][i], App. 9.5
  - Identity theft, 8.02[3][f], 8.02[5][c], 8.05[5]
  - Inbound traffic controls, 8.02[2]
  - Information security
    - classification, 15.01[2][b]
    - definitions, 15.01[2][a]
    - federal privacy laws, 15.02
    - Gramm-Leach-Bliley Act, 15.02[1], App. 2.7.1
    - online privacy, 15.04
    - pretext calling, 2.03[23], 8.02[3][f], App. 9.1.
    - risk identification, 15.01[1][2][d]
    - training, 15.05
    - written program, 15.01[2]
  - Information sharing, 6.01[3][c]
  - Instant messaging, 8.05[1][d]
  - Institute of Certified Bankers, 3.02[3][a]
  - Insurance
    - Bank Insurance Fund, 1.07
    - deductibles, 3.03[2][b]
    - financial institution bond, 3.03[2][a]
    - kidnap and extortion, 3.03[2][e], 6.05[2][f]
    - master trust policies, 3.03[2][d]
    - miscellaneous policies, 3.03[2][e]
    - savings association insurance fund, 1.07
  - Insurance services office, 4.07[1]
  - Intelligent video, 4.03[1][a]
  - Interior design, banking office, 4.09
  - International Association of Credit Card Investigators, 2.03[5][a]
  - International Biometric Association, 4.08[2]
  - International Emergency Economic Powers Act, 2.03[19][b]
  - International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, 13.01[6]
  - International Security and Development Corporation Act, 2.03[19][e]
  - Internet
    - access control, 8.02[2][e]
    - attacks, 8.02[7]
    - authentication, 8.03[4]
    - biometrics, 8.04[4][e]
    - cyber crime, 8.01[6], 8.02[3][a]
    - definition, 8.01[1]
    - digital signatures, 8.04[2]
    - e-commerce purchases, 8.01[5]
    - electronic information superhighway, 8.01
    - encryption, 8.04[1]
    - foreign government threats, 8.02[3][d]
    - firewalls, 8.04[5]
    - glossary of terms, Ex. 8.2
    - hackers, 8.02[3][b]
    - identity theft, 8.02[3][f]
    - integrity, 8.03[3]
    - Internet Crime Complaint (The), 8.01[3]
    - intrusion detection, 8.04[6]
    - mutual authentication, 8.04[4][h]
    - non-repudiation, 8.03[5]
    - on-line banking, 8.01[3]
    - on-line trading, 8.02[4]
    - on-line privacy, 8.05, 15.04
    - one-time password scratch card, 8.04[4][f]
    - passwords, 8.04[4][a]
    - password-generating token, 8.04[4][c]
    - personal computer controls, 8.04[10]
    - phishing, 8.02[3][f]
    - second channel authentication, 8.04[4][g]
    - secure transaction, 8.04
    - security controls, 8.04
    - security incidents, 8.02
    - security policy, 8.03[1]
    - security protection, 8.04
    - security requirements, 8.03
    - security risks, 8.02
    - smart cards, 8.04[4][d]
    - software patches, 8.04[9]
    - software vulnerabilities, 8.05[6]
    - tokens, 8.04[4][b]
    - viruses, 5.01[5][e], 5.04[3][d], 8.02[3][c], 8.04[11]
    - VoIP, 8.02[8], 8.04[12]
    - Web-linking controls, 8.04[7]
    - Web-linking risks, 8.02[4]
    - wireless technology controls, 8.04[8]
    - wireless technology risks, 8.02[5]
  - Interpol, 10.19
  - Interrogation techniques, 10.06
  - Interviewing techniques, 10.05
    - psychological factors, 10.05[6]
    - questions, 10.05[2]
  - Intrusion detection, 8.04[6]
  - Investigation of internal crime
    - arrest power, 10.14

## INDEX

[References are to paragraphs (§) and appendixes (App.).]

- avoiding pitfalls, 10.16
  - check fraud, 14.05
  - computer crime, 10.11
  - documentation, 10.04[2][a]
  - electronic surveillance, 10.10
  - files, 10.17
  - guide to investigative sources, App. 5.4
  - handwriting analysis, 14.05[3][b]
  - hypnosis, 10.08
  - internal investigative unit, 10.03
  - Interpol, 10.19
  - interrogation, 10.06
  - interviewing, 10.05
  - law enforcement restraints, 10.02
  - Miranda* ruling, 10.09
  - outsourcing the investigation, 10.03[3]
  - planning the investigation, 10.04[2]
  - polygraph, 10.07[1], 10.07[4]
  - presenting cases to the U.S. Attorney, 10.18
  - psychological stress evaluation, 10.07[2], 10.07[4]
  - report writing, 10.15
  - reporting criminal activity, 2.04, 10.18
  - search powers, 10.12
  - statements, written, 10.06[3]
  - suspect identification, 10.04[2][c]
  - threat analysis teams, 10.03[2]
  - Investigations
    - bad debt, 10.12
    - cameras, use of, 4.03[1][a]
    - check fraud, 14.05
    - damage control, 10.11[7]
    - definition of, 10.04
    - duties of security officer, 3.01[4]
    - evidence, 10.11[8]
    - incident response, 10.11[7]
    - preemployment, 7.01[5]
    - purpose of, 10.04
  - Investigators, personal traits, 10.03[1]
  - Iraq Sanctions Act, 2.03[19][c]
  - Iris scan, 8.04[4][ii]
  - Islamic fundamentalism, 6.01[1][c]
- J**
- Job descriptions
    - guard, 3.02[1]
    - guard force supervisor, 3.02[1]
    - investigation office, 3.02[1]
    - lock program manager, 3.02[1]
    - protection officer, 3.02[1]
    - security officer, 3.02[1]
  - Judicial districts, 10.01[1]
- K**
- Key locks, 4.05[1]
  - Keys. *See* Locks
  - Kidnapping
    - emergency planning, 6.03[2][b], 6.05[2]
    - employee profile, 9.02[6]
  - insurance, 6.05[2][g]
  - ransom payments, 6.05[2][d]
  - statistics, 2.02[3]
  - training, preventive/response, 6.05[2][a], 9.02[6]
  - Kiting, 2.03[5][b], 14.03[6], 14.06[6][b]
  - “Know your customer,” 9.02[8], 13.03[5][c], 14.02
- L**
- Law enforcement liaison, 1.02[2]
  - Lending officers training, 9.02[9]
  - Lighting. *See* Protective lighting
  - Line security, 4.02[2]
  - Loan fraud, 2.03[3], 9.02[9], 10.12
    - prime bank notes, 2.03[3][c]
  - Local alarm, 4.02[2][a]
  - Locks
    - combination, 4.05[2]
    - control system, 4.05[6]
    - delayed time, 4.05[4]
    - dual control, 4.05[6][b]
    - electromechanical, 4.05[5]
    - installation, 4.05[7]
    - key, 4.05[1]
    - new key technology, 4.05[3]
    - safe-deposit box, 4.05[1]
    - Underwriters Laboratories standard, 4.05[1], 4.05[2]
  - Loss prevention controls, 9.02
  - Lost securities, 1.04
- M**
- Mail bombs, 6.05[1][f]
  - Mail fraud, 2.03[17]
  - Medical history, 7.01[7]
  - Merchant fraud, 2.03[5][a]
  - Miranda* ruling, 10.09
  - Missing securities, 1.04
  - Modular vaults, 4.07[3]
  - Money clip, 4.02[5][c]
  - Money laundering, 9.03[3], 13.02
  - Money Laundering Control Act of 1986, 13.01[2]
  - Money Laundering Suppression Act of 1994, 13.01[5]
  - Moonlighting, 1.01[2][a]
  - Mortgage loans, 2.03[3][b]
  - Mutual authentication, 8.04[4][h]
- N**
- Narcotics. *See* Substance abuse
  - National Credit Union Administration, 2.04[5]
  - National threat advisory system, 6.01[2][a]
  - Natural emergencies, 6.03[2], 6.05[6]
  - New accounts, 14.02
  - New York City ATM law, 11.03[5]
  - Night depository
    - alarm protection, 4.02[4][c]

## BANK SECURITY DESK REFERENCE

[References are to paragraphs (§) and appendixes (App.).]

burglar attacks, 2.02[2], 4.02[2]  
civil liability, 2.02[4][c]  
customer attacks, 2.02[4]  
safes, 4.02[4][c], 4.06  
Non-repudiation, 8.02[2][d], 8.03[5]  
Nuclear war, 6.02[1][e], 6.05[7]

### O

OCC privacy guidance, 8.05[3]  
Office of Thrift Supervision, 1.02, 1.07  
Offshore shell bank, 2.03[7][a]  
Omnibus Crime Control and Safe Streets Act of 1968, 10.10[1], 10.10[2]  
One-time password scratch card, 8.04[4][f]  
Online banking, 8.01[3]  
Online privacy, 15.04  
Online Privacy and Information Security-Regulatory Guidance and Developments 8.05  
FDIC guidance on online privacy and security, 8.05[2]  
May 1996 interpretive release, 8.05[4][b]  
October 1995 interpretive release, 8.05[4][a]  
OCC and Department of Treasury guidance and initiatives, 8.05[3]  
    technology-related risk management guidance and checklists, 8.05[3][a]  
Online trading, 8.01[4]  
Opening procedures, 9.02[1]  
Organized crime  
    theft of securities, 2.03[12]  
    theft on the Internet, 8.02[3][a][i]  
Osama bin Laden, 6.01[1]  
Outbound traffic controls, 8.03[3]  
Outsourcing  
    investigation, 10.03[3]

### P

Pandemics, 6.03[3], 6.05[10]  
Parking lots, 4.04[1][d]  
Password-generating token, 8.04[4][c]  
Password security, 5.04[3][a], 8.04[4][a]  
Patriot Act, 13.01[6], 14.02  
“Payable through” accounts, 13.02[2], App. 12.9  
Personal computers. *See* Computers  
Personal crimes, 2.06, 2.07[1]  
Personal identification, 4.08[2], 14.02  
Personal identity theft, 14.02[6][b]  
Personnel screening. *See* Applicant screening  
Personnel security  
    applicant screening, 7.01  
    code of conduct, 7.04  
    drug abuse, 7.02  
    responsibilities, 3.01[2]  
    substance abuse, 7.02  
    vacation policies, 7.07  
    workplace violence, 7.06  
Phishing, 8.02[3][f], 14.03[7]  
Physical security  
    alarm systems, 4.02

camera surveillance equipment, 4.03  
counter audio, 4.10  
dye packs, 4.12  
equipment inventory, 4.01[1]  
guards, 4.11  
locks, 4.05  
planning goals, 4.01  
protective lighting, 4.04  
responsibilities, 3.01[1]  
safe-deposit box, 12.04[4]  
safes, 4.06  
vaults, specifications, 4.07  
Planning  
    physical security, 4.01  
    security department, 3.04  
Point-of-sale terminals, 11.01[3]  
Police, and security cooperation, 1.01[2][b]  
Police, as guards, 4.11[3]  
Polygraph  
    legal considerations, 7.01[5][c], 10.07[1], 10.07[4]  
    tests, 7.01[5][c], 10.07[4]  
    use, 10.07[1], 10.07[4], App. 11  
Polygraph Protection Act of 1988, App. 11  
Position descriptions. *See* Job descriptions  
Positive pay, 14.07[10]  
Postal inspectors, listing, App. 5.2  
Power failures, 6.03[2][h], 6.05[4]  
Pre-employment assessments. 7.01[5][d]  
Pretexting, 2.03[23], 8.02[3][f], 9.03[2], App.9.1  
“Prime bank” notes, 2.03[3][c]  
Privacy, consumers, Ch. 15  
Privacy, customer information, Ch. 15, 3.03[4]  
Privacy laws, 15.02, App. 7.1  
Private citizen arrest, 10.14[3][a]  
Private security, 1.01[2]  
Private Security Officer Employment Authorization Act, 7.01[8], App. 15, 3.03[4]  
Profile of bank robbers, 2.02[1][a]  
Property crimes, 2.07[2]  
Proprietary alarm, 4.02[2][d]  
Prosecution, 10.18  
Protective lighting  
    applications for financial institutions, 4.04[1]  
    ATMs, 11.03[2][b], 11.03[4]  
    banking office security, 9.02  
    Bank Protection Act requirements, 1.02[1][b], 4.04[1][a]  
    customer service area illumination, 4.04[1][c], 11.03[4]  
    high exposure area illumination, 4.04[1][b]  
    parking lots, 4.04[1][d]  
    positioning equipment, 4.04[3]  
    selection, 4.04[2]  
    sources of light, 4.04[2][b]  
    types, 4.04[2][a]  
    vault illumination, 4.04[1][a]  
Psychological factors, interviewing, 10.05[6]  
Psychological stress evaluator, 10.07[2], 10.07[4]  
Public keys, 8.04[1][a]

[References are to paragraphs (§) and appendixes (App.).]

## Q

Questioned documents, 14.05[3][b]  
 Questions, interviewing, 10.05[2]

## R

Radio-frequency identification systems, 4.08[4]  
 Radiological dispersion device, 6.05[8]  
 Ransom payment, 6.05[2][e]  
 Ratzlaf v. United States, 13.02[2][g]  
 Real estate loans, 10.12[2]  
 RealSecure, 8.04[6][d]  
 Records  
   Regulation E, 11.02[6]  
     vital, 6.04[7]  
 Regulation CC, 14.04[3]  
 Regulation E, 11.02  
   access devices, 11.02[2], 4.08[2]  
   amendment to, 11.02[4]  
   consumer liability, 11.02[3]  
   definitions, 11.02[1]  
   documentary transfers, 11.02[4]  
   error resolution, 11.02[5]  
   lost or stolen cards, 11.02[3][b]  
   record retention, 11.02[6]  
 Regulation P. *See* Bank Protection Act of 1968  
 Reporting level, security officer, 3.02[4]  
 Reports  
   apparent crimes, 2.04, App. 9.4  
   compliance, Bank Protection Act, 1.02[2][c]  
   crime, 1.02[2][c], 2.04  
   currency transaction, 13.03[2]  
   investigations, 10.14  
   suspicious activity reporting, 2.04, App. 9.4  
 Report writing, 10.15  
 Resolution Trust Corporation, 2.01[2][d]  
 Reverse positive pay, 14.07[11]  
 Rewards, teller, 14.06[3]  
 RICO, 2.03[18]  
 Riggs National Bank, 13.02[2][i]  
 Right to Financial Privacy Act, 15.02[2], App. 2.4  
 Riots, 6.03[2][g], 6.05[3]  
 Risk management  
   *See also* Insurance  
   analysis, 3.03, 4.01  
   assessment in emergency planning, 6.03  
   environmental risk, 3.03[3]  
   security officer's role, 3.03[1]  
   standards for safety and soundness, 3.03[4]  
   Year 2000 project analysis, 5.01[1][a]  
 Rivest-Shamir-Adelman (RSA), 8.04[1]  
 Robbery  
   *See also* Crime in financial institutions  
   alarms, 4.02[5], 9.02[12][a]  
   statistics, 2.02[1]  
   training, prevention and response, 9.02[4]  
 RSA, 8.04[1]

## S

Sabotage, 6.03[2][e]  
 Safe-deposit box security  
   access, 12.07[2]  
   audits, 12.09  
   bomb threats, 6.05[1][e], 12.07[5]  
   burglary, 2.02[2], 12.08  
   checklist for safeguards, 9.02[7][b]  
   contract, 12.06  
   customer access, 12.07[2]  
   insurance, 12.10  
   key and lock control, 12.05  
   liability, 12.02  
   vault  
     design, 12.03  
     physical specifications, 4.07, 12.04  
 Safes  
   alarm protection, 4.02[4][b]  
   ATMs, 4.06[3]  
   auxiliary, 4.06[1], 4.06[2][a]  
   Bank Protection Act requirements, 1.02[2]  
   night depositories, 4.06[1], 4.06[2],  
     4.06[3][a]  
   physical specifications, 4.06  
   selection, 4.06[3]  
   specifications, 4.06  
   Underwriters Laboratories classifications,  
     4.06[1]  
 Safety and soundness, 3.03[4]  
 Search powers, 10.13  
 Second channel authentication, 8.04[4][g]  
 Secret Service  
   check fraud investigation, 2.03[4]  
   counterfeiting, 2.03[11], 9.02[10][a]  
   credit and debit card investigations,  
     2.03[5][c]  
   offices, App. 5.5  
 SEC Rules 17 F-1 and 17 F-2  
   exceptions to rule, 1.04[2]  
   “hits,” 1.04[4][b]  
   inquiry requirements, 1.04[3]  
   institutions covered, 1.04[1]  
   person to be fingerprinted, 1.05[1]  
   records and recording, 1.05[3]  
   regulation, App. 3.1, App. 3.2  
   reporting requirements, 1.04[2]  
   securities information center, 1.04[4]  
 SEC regulation of confidential data, 8.05[5]  
 Securities, missing, lost, counterfeit, or stolen,  
   1.04, 2.03[12]  
 Securities Information Center, Inc.  
   access codes, 1.04[4][a]  
   response to “hits,” 1.04[4][b]  
   statistics, 1.04[4][c]  
 Securities theft, 2.03[12]  
 Security department  
   consultants, use of, 3.05  
   job descriptions, 3.02[1]  
   responsibilities, 3.01  
   security procedures, 3.07

*[References are to paragraphs (§) and appendixes (App.).]*

stress, 3.02[2]  
 structure of staff, 3.02  
 Security during banking hours. *See* Banking  
 office security  
 Security officer  
     Bank Protection Act, 1.02[2][a]  
     budgeting, 3.04[1]  
     certification, 3.02[3][d]  
     job description, 3.02  
     physical security planning, 4.01  
     psychological screening, 3.02[3][b]  
     qualifications, 3.02[3][a]  
     reporting level, 3.02[4]  
     stress, 3.02[2]  
     training, 3.02[3][c]  
 Security procedures, 3.07  
     administrative procedures, 9.02  
     Bank Protection Act requirements, 1.02[2],  
         9.01[1]  
     equipment testing, 9.02[12]  
     law enforcement, involvement of, 1.02[2]  
     vault, 9.02[3][a][i]  
 Security protection, Internet, 8.04  
 Sequence cameras, 4.03[1][a]  
 Service contracts, 8.04[7][c], App. 12.6  
 Seychelles, republic of, 13.02[1][b]  
 Shadow, 8.04[6][c]  
 Shared networks, 11.01[3]  
 Shell corporations, 2.03[7]  
 Smart cards, 11.01[4], 8.04[4][c], 8.04[4][d]  
 Snort, 8.04[6][c]  
 Social Security verification, 14.02[7][c]  
 Software vulnerabilities, 8.02[6]  
 Sources for information, App. 5.4, 7.01[5][e]  
 State ATM security laws, 11.03[5][b]  
 State banking authorities, App. 5.1  
 State computer crime laws, 5.02[2]  
 Statements, written, 10.06[3]  
 Stolen securities, 1.04  
 Stress, in security operation, 3.02[2]  
 Subpoenas, 15.02[2][b]  
 Substance abuse, 7.02  
     alcoholism, 7.02[3]  
     cannabis based, 7.02[4][a][vi]  
     controlled substance, 7.02[4]  
     hallucinogens, 7.02[4][a][v]  
     narcotics, 7.04[4][a][i]  
     narcotics, synthetic, 7.02[4][a][ii]  
     policy, 7.02[1], 7.02[2]  
     stimulant, 7.02[4][a][iv]  
     symptoms, 7.02[4][a], 7.02[4][b]  
     testing for, 7.01[7][a], 7.01[7][b]  
     types of drugs, 7.02[4][a]  
 Substitute checks, 14.04[3][e]  
 Surveillance systems. *See* Camera surveillance  
 equipment  
 Suspect identification, 10.04[2][b]  
 Suspicious activity reporting, 2.04  
 Suspicious conduct, 9.02[8][c], 9.02[8][c]

**T**

Telemarketing fraud, 2.03[16]  
 Telephone, wiretapping, 10.10  
 Telephone Records and Privacy Protection Act  
     of 2006, 2.03[23], 8.02[3][f], App. 9.1  
 Teller counter, 4.09[2]  
 Terrorism, 6.03[2][d], 8.02[3][a][ii]  
 Testing records, 9.02[12][e]  
 Threat analysis teams, 10.03[2]  
 Time locks, 4.05[4]  
 Title 18, U.S. Code, App. 9  
 Tokens, 8.04[4][b]  
 Touch Signature Fingerprint Program, 14.07[6]  
 Trading With the Enemy Act, 2.03[19][a]  
 Training  
     banking office employees, 9.02  
     bank robbery, 9.02[4]  
     Bank Secrecy Act, 13.03[5]  
     bomb threat, 9.03[2]  
     check fraud, 14.01, 14.06  
     check kites, 14.03[6], 14.06[6][b]  
     color copy reproductions, 9.02[10][b]  
     computer crime investigations, 10.11  
     counterfeit currency, 9.02[10][a]  
     counterfeit securities, 9.02[10][b]  
     customers, 9.04  
     customer privacy protection, 9.03[1], Ch. 15  
     fire, 6.05[5][c], 9.03[3]  
     importance of, 9.01  
     information security, Ch. 15  
     Gramm-Leach-Bliley Act, 15.02[1]  
     kidnapping, extortion, or hostage situations,  
         6.05[2][a], 9.02[6]  
     “know your customer,” 9.02[8]  
     lending officers, 9.02[9]  
     loan fraud, 9.02[9]  
     money laundering, 9.03[3], 13.03[5]  
     personnel interviewer, 7.01[1]  
     pretext phone calling, 9.03[2]  
     Regulation CC, 14.04[3]  
     safe-deposit operations, 9.02[7]  
     security indoctrination, 9.01  
     security officer, 3.02[3][c]  
     wire transfer, 9.02[11]  
 Transport of cash, 9.02[3][a][iii]  
 Transport of currency, 9.02[3][a][iii]  
 Travelers’ checks, 2.03[10]  
 Truncation, 14.04[3][e]

**U**

Underwriters Laboratories, 4.01[2]  
     alarms, 4.02  
     bullet-resistant barriers, 4.09[3]  
     camera surveillance equipment, 4.03[1]  
     combination locks, 4.05[2]  
     key locks, 4.05[1]  
     safe classifications, 4.06  
     vault and vault door classifications, 4.07[4]  
 Uniform Commercial Code, 14.04[4]

## INDEX

[References are to paragraphs (§) and appendixes (App.).]

- United Nations Participation Act, 2.03[19][d]
  - Urinalysis, 7.01[7][a], 7.01[7][b]
  - U.S. Attorney, presenting cases, 10.18
  - U.S. Attorneys list, App. 5.6
  - U.S. Code, Title 18, App. 9
  - U.S. Department of Homeland Security, 6.01[2]
  - U.S. Marshals' survey findings, 1.03[1]
  - U.S. Postal Inspection Service offices, App. 5.2
  - U.S. Secret Service
    - credit card fraud, 2.03[5]
    - offices, App. 5.5
  - USA PATRIOT Act, 13.01[6], 14.02
- V**
- Vacation policies, 7.07
    - exceptions to industry standard, 7.07[3]
    - FDIC policy, 7.07[4]
    - industry standard, 7.07[2]
  - Vault
    - access, 9.02[7], 12.07
    - alarm protection, 4.02[4]
    - Bank Protection Act standard, 1.02[2]
    - burglary, 2.02[2]
    - closing, 9.02[7], 12.07[1]
    - combination control, 4.05[6][b]
    - doors, 4.07[5]
    - Insurance Services Office standard, 4.07[2]
    - modular, 4.07[4]
    - opening, 9.02[1], 12.07[1]
    - physical specifications, 4.07
    - safe-deposit vaults, 12.04
    - security procedures, 9.02[7]
  - Violence. *See* workplace violence
  - Viruses, 5.01[e], 8.02[4], 8.04[11]
  - Vital records electronic imaging, 6.04[8]
  - Vital records protection, 6.04[7], 6.05[7][c]
  - Vital records storage, 6.05[7]
  - Voice recognition, 8.04[4][iii]
  - VoIP, 8.02[8], 8.04[12]
- W**
- Warning notices, 2.05, 14.06[4]
  - Wastepaper, 9.02[3][a][iv]
  - Weapons of Mass Destruction, 6.05[12]
  - Web-linking risks, 8.02[4]
  - Welfare payments, 11.03[4][c]
  - White-collar crime
    - See also* Crime in financial institutions
    - causes for increase, 2.03[1]
  - check fraud, 14.01
  - definition, 2.03
  - embezzlement, 2.03[2]
  - investigation of,
    - interviewing techniques, 10.05
  - legislation, 1.04, 1.05, 13.01, App. 9.1
  - loan fraud, 2.03[3]
  - loss to business, 2.01[2], 2.03
- Wireless technology, 8.02[5]
  - Wiretapping, 2.03[13], 10.10
  - Wire transfer crime, 2.03[9], 2.03[13], 9.02[11]
  - WMD, 6.05[12]
  - Workplace violence, 7.06
    - acts of violence, 7.06[5]
    - aggressor, 7.06[5][a][v]
    - applicant screening, 7.06[7][d]
    - assessment team, 7.06[6]
    - causes, 7.06[5][a][ii]
    - communications, 7.06[7][e]
    - criminal history, 7.06[5][a][vii]
    - criminal justice system, 7.06[12]
    - disputes, 7.06[5][a][i]
    - employee assistance program, 7.06[8]
    - history, 7.06[2]
    - homicides, 7.06[4]
    - hotline, 7.06[6]
    - Justice Department study, 7.06[3]
    - management's role, 7.06[7][a]
    - physical contact, 7.06[5][a][ix]
    - policies & procedures, 7.06[7][b]
    - prevention controls, 7.06[7]
    - security program, 7.06[10]
    - situational example, 7.06[1]
    - substance abuse, 7.06[5][a][x]
    - terminations, employee, 7.06[9]
    - threats, 7.06[5][a][viii]
    - training managers, 7.06[7][c]
    - training security personnel, 7.06[11]
    - victim provocation, 7.06[5][a][iv]
    - warning flags, 7.06[5][a]
    - weapons, 7.06[5][a][vi]
    - written plan, 7.06[6]
- Y**
- Year 2000 project analysis, 5.01[1][a]

