

Table of Contents

<i>Acknowledgments</i>	ix
<i>Introduction</i>	xi
Chapter 1 — Cyberfraud Defined	1
1. What Is Cyberfraud?	1
(a) Related Definitions	2
(b) Existing Definitions	4
(c) A Fresh Definition of Cyberfraud	5
(i) From the <i>mens rea</i> to the <i>actus reus</i>	5
(ii) What Constitutes Value?	6
2. What Isn't Cyberfraud?	7
(a) Cybercrime vs. Cyberfraud	8
(i) People as Instruments	8
(ii) Does the Human Factor Turn Cybercrime into Cyberfraud?	9
(iii) The Shift from Cybercrime to Cyberfraud	10
(b) When Is Cybercrime Not Cyberfraud?	13
(i) The Cyberheist as a Prelude to Cyberfraud	14
A. ATM Thefts	15
B. Ransomware and Cyberextortion	16
C. Malware	17
(ii) Global Banks	18
(iii) Virtual Currencies	18
(iv) Money Transfer Organizations	21
(v) Credit Bureaus	22
(vi) Affiliate Programs	22
(vii) Government-funded Cyberattacks	24
Chapter 2 — A Fresh Approach to Cyberfraud Classification	25
1. Why is Classification Important?	25
(a) The New Normal	26
(i) What We Know About Cyberfraud	27
(ii) What We Don't Know About Cyberfraud	28
(b) The Growing Value of Personal Information	30
2. A New Cyberfraud Classification Framework	33
(a) Introduction	34

(b) Framework Categories	34
(c) Cyberfraud Classification in Practice	36
(i) Unauthorized Access — General	
Malware (A-1.1)	36
(ii) E-commerce Fraud — Malicious Ad	
Networks (B-2.5)	37
(iii) E-commerce Fraud — Fraudulent	
Promoters (B-2.6)	38
(iv) Email and Social Media Fraud —	
Deceptive Emails and Phishing (C-3.3)	39
(v) Identity Fraud — Synthetic Identity	
Fraud (D-4.2)	40
(vi) Investment and Securities Fraud —	
Pyramid Schemes (E-5.3)	40
(vii) Investment and Securities Fraud —	
Phony Investor Alert and Recovery	
Services (E-5.7)	41
(viii) Financial System Abuse — CRA Scams	
and Telephone Extortion (F-6.4)	42
(ix) Money Laundering — Individual	
Focus (G-7.1)	42
(x) Advance Fee Fraud (H)	44
(xi) Advance Fee Fraud — Romance	
Swindles (H-8.3)	45
(xii) Advance Fee Fraud — Phony Job Offers	
and Business Opportunities (H-8.4)	46
Chapter 3 — The Roots of Cyberfraud	49
1. Some Things Never Change	49
2. The Short Con	49
(a) Origins	49
(b) Example: The Chain Letter	50
(c) The Cyberfraud Version: Email and Social	
Media Fraud (Category C)	51
3. The Long Con	52
(a) Origins	52
(b) Example: The Spanish Prisoner Scam	53
(c) The Cyberfraud Version: Advance Fee Fraud	
(Category H)	54
4. Money Laundering	56

(a) Origins	56
(b) The Cyberfraud Version: Money Laundering (Category G).	57
5. The Ponzi Scheme	58
(a) Origins	58
(b) Dare We Call It Evolution?	60
6. The Human Dimension: Why Fraud Still Works	61
(a) The Anonymity of the Internet	61
(b) The Cognitive Peculiarities of Human Nature	61
Chapter 4 —The Victims of Cyberfraud	63
1. Individuals	63
(a) Are People Predisposed to Being Scammed?	63
(i) Self-selection	65
(ii) Sucker Lists	66
(b) Advance Fee Fraud (Category H)	67
(c) Money Mules (Category G)	68
(d) Identity Fraud (Category D).	70
(i) Social Media Hoaxes (Category C-3.2).	72
(ii) Phishing and Social Engineering (Category C-3.3)	73
(iii) Synthetic Identity Fraud (Category D-4.2).	76
A. How does it Work?	77
B. But is it Cyberfraud?	78
2. Organizations	81
(a) How Vulnerable are Businesses to Cyberfraud?.	81
(b) Commercial Bank Fraud (Category A-1.6)	82
(i) Bank Fraud Losses	83
(ii) Cyber Loss Insurance Coverage.	84
(c) Identity Fraud as it Applies to Corporations (Category D).	85
(i) Phishing and Social Engineering (Category C-3.3)	86
A. Domain Name Fraud (Category C-3.3).	87
B. Business Email Compromise/CEO Fraud (Category C-3.4).	90
(ii) Impersonating an Entity to Commit Tax Fraud (Category D-4.1)	92
(d) Big Problems for Small Business.	93

3. Nations	94
Chapter 5 — Cyberfraud as a Career	97
1. Deception as a Way of Life	97
2. Individuals	98
(a) Money Mules	98
(b) Rationalizers	99
(c) Crooks and Perps	100
3. Organized Crime	102
(a) High-Speed Cyberfraud	103
(i) Cyberextortion (Category H-8.7)	104
(ii) Cyberfraud Against Banking Institutions (Category G)	106
(b) Tax Fraud (Category D-4.1)	107
4. Crime-as-a-Service (CaaS)	108
(a) Booter Sites	109
(b) Exploit Kits	111
Chapter 6 — Preventing and Detecting Cyberfraud	113
1. Awareness and Prevention	113
(a) Cyber’s Most Wanted	113
(b) Basic Guidance	114
(i) General Tips	114
(ii) Avoiding Identity Fraud	115
(iii) Keeping the Conversation Going	116
(c) Why Simple Prevention Often Fails	116
(i) Emotional Investment	116
(ii) The Illusion of Simplicity	119
(iii) The Exploitation of Public Awareness	122
(iv) The Absence of a Common Language	123
2. Detection	124
(a) Is Cyberfraud Hiding in Plain Sight?	125
(b) How to Spot Cyberfraud	127
(i) The Three Conditions of Fraud	127
A. Pressure	128
B. Opportunity	128
C. Rationalization	129
(ii) Illustration: Business Email Compromise/CEO Fraud (Category C-3.4)	130

(c) The Problem of Under-reporting	133
(i) Embarrassment	134
(ii) The Prestige Effect	135
(iii) Understandable Skepticism.	135
(iv) Ignorance or Disincentive.	138
(v) Negative Consequences.	139
Chapter 7 — Combatting Cyberfraud	143
1. Technology to the Rescue.	143
2. Successes.	143
(a) Money Laundering (Category G).	143
(b) Phony Online Pharmacies (Category B-2.3).	145
3. Opportunities	146
(a) The Four Types of Safeguards	146
(b) Increased Reporting.	147
(i) Scam Victims	147
(ii) Money Mules.	148
(iii) Organizations and Employees	149
(iv) Financial Institutions	150
(c) Centralized Data Collection	153
(d) Disrupting Criminal Profit Centres	153
(e) Assessing Environmental Factors.	155
(f) Global Collaboration.	156
(i) Managing Identity Fraud Across Borders.	156
(ii) Combatting Illegal Online Gambling.	157
(iii) Law Enforcement Education and Collaboration.	158
(iv) Changes to Data Retention Laws	159
Chapter 8 — Global Trends in Cyberfraud	161
1. Identifying Common Elements Across Continents.	161
2. Trends in Australia	162
3. Trends in the United States	164
4. Trends in Canada	167

Chapter 9 — The Future of Cyberfraud	171
Appendix — Cyberfraud Reference Library: 100 Illustrative Examples	179
<i>Index</i>	269