
Reinventing Consumer Protection

David Adam Friedman

Follow this and additional works at: <https://via.library.depaul.edu/law-review>

Recommended Citation

David A. Friedman, *Reinventing Consumer Protection*, 57 DePaul L. Rev. 45 (2007)
Available at: <https://via.library.depaul.edu/law-review/vol57/iss1/3>

This Article is brought to you for free and open access by the College of Law at Via Sapientiae. It has been accepted for inclusion in DePaul Law Review by an authorized editor of Via Sapientiae. For more information, please contact digitalservices@depaul.edu.

REINVENTING CONSUMER PROTECTION

*David Adam Friedman**

INTRODUCTION

Since the dawn of the last century, consumer fraud¹ has presented a continual puzzle.² In the United States alone, there are significant federal, state, and private consumer protection, enforcement, and education mechanisms.³ Despite these efforts, the United States pays an enormous price for consumer fraud each year. In 2006, the Federal Trade Commission (FTC) measured reported consumer fraud losses in the United States at \$1.1 billion,⁴ but this figure failed to account for undetected or unreported transactions. Nor did it account for the hidden costs left unmeasured from “non-transactions”—the value foregone from failed transactions due to fear of fraud.⁵

* Visiting Assistant Professor of Clinical Legal Studies, Willamette University. B.A., J.D., Yale University. Thank you to Christine Hurt at The Conglomerate Blog for selecting this paper for the Third Annual Junior Scholars Workshop and, specifically, for the comments and guidance of Larry Garvin, Robert Lawless, Adam Levitin, and Ronald Mann. I thank Ian Ayres and Joel Waldfoegel for their encouragement and Michael Abramowicz, Laura Appleman, Babette Boliek, Gilbert Carrasco, Paul Diller, Jeffrey Dobbins, Kristin Madison, Terrance O'Reilly, Jeffrey Standen, Norman Williams, and the Willamette Faculty Colloquium for their comments on earlier drafts.

1. This includes financial fraud along with consumer fraud. Broadly, deceptive or unfair practices can also attach to the analysis in this Article. These practices are more widespread and, as this Article will briefly explore in Part II.A, potentially more easily deterred.

2. See generally Norman Silber, *From The Jungle to The Matrix: The Future of Consumer Protection in Light of Its Past*, in CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY': MARKETS AND THE LAW 15 (Jane K. Winn ed., 2006).

3. See *infra* notes 27–48 and accompanying text for illustrations of these mechanisms and the entities that govern them.

4. See FED. TRADE COMM'N, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA: JANUARY-DECEMBER 2006 2 (Feb. 2007) [hereinafter 2006 FTC COMPLAINT DATA], available at <http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf>.

5. See generally George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970). A good (in the Akerlof instance, a used automobile) may have a market price below what it would actually be worth if consumers had perfect information because of both the risk associated with the unknown nature of the used automobile's quality (compared to a new automobile) and the comparative uncertainty of the individual seller's reputation (compared to that of an established dealership). The lower market price may cause the seller to refrain from selling the good, leading to an inefficient non-transaction. If fraud were less of a risk, the market price would be higher, making the transaction more likely to occur.

Despite the large, widespread, and diverse resources allocated to the problem, the specter of consumer fraud still haunts every consumer transaction. The United States has a sprawling, reactive consumer protection regime that fails to fully address this important social and economic problem. This problem calls for a new and innovative approach.

Yet consumer fraud presents a number of challenging questions. First, how can agencies improve the current consumer protection system? Second, how can policymakers ensure that the system is both effective and cost-efficient? Finally, how can they engage the current, highly complex enforcement system to solve the problem, rather than engage in lengthy and arduous structural reform?

This Article contends that a novel answer to each of these questions lies in identifying concentrated, less resource-intensive, “surgical” tactics that leverage both consumer behavior and fraud perpetrators’ incentives. Policymakers can neither transform the entire consumer protection system overnight nor allocate more resources to the problem. But agencies can engage in more practical tactics, such as protecting definable or randomly selected groups. Such tactics would ultimately make fraud less attractive within the larger economy.

Currently, U.S. agencies approach consumer protection from three perspectives: (1) the perpetrator perspective via direct enforcement of consumer protection and fraud laws and the combat of specific schemes;⁶ (2) the individual consumer perspective through the provision of tools for self-protection⁷ and consumer education;⁸ and (3) the

6. For example, authorities can bring an action against fraud related to auto repair. See Press Release, Cal. Dep’t of Consumer Affairs, Bureau of Automotive Repair Seeks to Shut Down Southern California EZ Lube Shops (Sept. 20, 2006), available at http://www.dca.ca.gov/publications/press_releases/2006/0920_bar.shtml. Another example is the multi-state agreement with Western Union to combat consumer fraud involving money wire transfers. See Press Release, Conn. Att’y Gen.’s Office, Attorney General Announces Multi-State Agreement with Western Union to Curb Fraudulent Money Transfers (Nov. 14, 2005), available at <http://www.ct.gov/ag/cwp/view.asp?A=1949&Q=306584>.

7. The “cooling-off” period for consumers entering into certain types of contracts exemplifies a legislative provision for self-protection. For a discussion of the paternalism of “cooling-off” periods for door-to-door sales, which enable consumers to rescind contracts within seventy-two hours of a door-to-door sale, see Cass R. Sunstein & Richard H. Thaler, *Libertarian Paternalism is Not an Oxymoron*, 70 U. CHI. L. REV. 1159, 1187–88 (2003).

8. Given this aspect of consumer education, “[t]he transnational nature of a scam may make it very difficult for law enforcers to catch the perpetrators and to compensate the victims. In particular, complicated questions of jurisdiction and choice of law can pose barriers to effective enforcement.” Comm’r Roscoe B. Starek III, Fed. Trade Comm’n, Consumer Protection in the Information Society: A View from the United States, Prepared Remarks Before the European Consumer Forum on the Consumer and the Information Society at Dublin Castle (Sept. 4, 1996), available at <http://www.ftc.gov/speeches/starek/ireland.shtm>. Because of this difficulty, the government has focused on educating the public to identify and avert these transnational scams. See

perspective of a definable consumer group.⁹ However, there are significant problems with the first two approaches.

The first approach engages perpetrators through civil causes of action, criminal laws, and government enforcement tools that aim to stamp out specific schemes. This primary approach has achieved limited success due to the expense of general enforcement and the failure of the regulatory imagination to anticipate fraud innovation.¹⁰

The second approach engages the individual consumer through state and federal consumer rights mechanisms and general consumer education. This approach fails, because vulnerable groups may be inherently difficult to educate.¹¹ It also fails because of limited resources and fraud innovation.

However, the third approach—defining a protected consumer group—is significantly different. Instead of racing to beat the next big scam and attempting to solve the fraud problem for the entire population, it carves out a category of consumers and provides that group with heightened protection. Policymakers may select a group according to any of three criteria: unique vulnerability, reticence to report victimization, or susceptibility to specific schemes. Much like the second approach, this approach uses empowerment and education to engage the consumer's perspective as a group member. It also includes elements of the first approach by signaling to perpetrators that targeting the group could be significantly more costly.

This third approach has the potential to achieve significant outcomes if it is artfully designed and reaches beyond the mere group perspective. This Article demonstrates that imposing dramatically enhanced protection ("hyper-protection") on carefully selected consumer groups can enhance consumer protection across the board. This carefully selected consumer group may either be an externally identifiable group (for instance, a group based on age, income level, or ethnicity) or a carefully constructed group.

If legislators granted hyper-protection to the right consumer group, it would change the fraud equation by compelling scammers to turn to more sophisticated targets. These targets are more likely to detect

FTC Consumer Alert, *The "Nigerian" Scam: Costly Compassion* (July 2003), available at <http://www.ftc.gov/bcp/online/pubs/alerts/nigeralt.shtm>. In this alert, the FTC also referred consumers to two other agencies for enforcement: the Secret Service and the Department of State.

9. One example is older consumers. See FED. TRADE COMM'N, *FRAUD AND IDENTITY THEFT COMPLAINTS RECEIVED BY THE FEDERAL TRADE COMMISSION FROM CONSUMERS AGE 50 AND OVER* (May 2005) [hereinafter *AGE 50 AND OVER*].

10. See Samuel W. Buell, *Novel Criminal Fraud*, 81 N.Y.U. L. REV. 1971, 1972-73 (2006).

11. A group's educational problems may be the reason they are fraud targets in the first instance.

and report fraud and may absorb the financial detriment caused by scams more easily.¹² In turn, this plan would deter scammers from committing fraud throughout the general population. By focusing protection on the right groups, policymakers would maximize the effect of their limited resources upon the overall level of consumer protection in the economy, while incidentally protecting that group. In effect, this method would create the consumer equivalent to "LoJack."¹³

This Article proposes a plan for reinventing consumer protection through selection of protected groups and concentrated resource reallocation. Part II examines the flaws in the current approach and describes the impact of the United States's diffuse and reactive consumer protection enforcement regime.¹⁴ Part III uncovers the economic forces behind the commission of fraud and explores the various ways in which policymakers can manipulate those forces.¹⁵ It then demonstrates how a reinvented approach toward protecting consumer groups can significantly change the economic viewpoint of all players and minimize consumer fraud effectively and efficiently.¹⁶ Part IV proposes and defines two consumer groups for which enhanced protection would work well: a subset of the African-American community and a group consisting of randomly selected individuals.¹⁷ Finally, this Article concludes that applying hyper-protection to both a defined group and a randomly selected group is necessary to decrease incidents of fraud.¹⁸

II. THE FAILURES OF CURRENT CONSUMER PROTECTION

Two problems pervade the current consumer protection regime. First, a veritable alphabet soup¹⁹ of state and local agencies have both

12. There is a secondary consequence to consider: in theory, a scammer would shift her target from the hyper-protected vulnerable group to the unprotected vulnerable group. This Article addresses this issue below in Part IV.C.

13. See Ian Ayres & Steven D. Levitt, *Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack*, 113 Q.J. ECON. 43, 43 (1998) (discussing how a concealed device that enables the recovery of stolen vehicles increased overall auto theft deterrence).

14. See *infra* notes 19–87 and accompanying text.

15. See *infra* notes 88–151 and accompanying text.

16. See *infra* notes 152–162 and accompanying text.

17. See *infra* notes 163–201 and accompanying text.

18. See *infra* Part V.

19. "The term 'alphabet soup' . . . gained currency in the early days of the New Deal as a description of the proliferation of new agencies." Bernard Schwartz, *Some Recent Administrative Law Trends: Delegations and Judicial Review*, 1982 WIS. L. REV. 208, 232 (1982) (quoting *Chrysler Corp. v. Brown*, 441 U.S. 281, 286 n.4 (1979)).

the authority to prosecute consumer fraud and the mandate to provide consumer education. Second, fraud is continuously evolving, and fraud merchants are continually frustrating the consumer protection regime's attempts to stay ahead of the curve.²⁰

The problem of novel fraud is not novel.²¹ In 1914, Walter Lippmann wrote that "consumers in America no longer had the time, information or equipment to 'candle every egg, test the milk . . . inquire into the shoddy [or] find out whether the newspapers are lying.'"²² This problem continues today in the form of evolving consumer technologies and cunning efforts to create the next great scheme.²³ Section A describes the challenges facing the United States's diffuse enforcement mechanisms.²⁴ Section B discusses the problems associated with taking a reactive approach to consumer fraud.²⁵ Finally, Section C demonstrates how enforcement diffusion combines with reactive enforcement to create a flawed system.²⁶

A. Enforcement Diffusion

Despite the enormous amount of resources poured into detection, enforcement, and prosecution of consumer fraud at every level of government, consumer protection often falls between the cracks, because each agency has a limited jurisdiction and a limited budget. In the federal sphere alone, a multitude of entities are charged with protecting the consumer or serving as a consumer complaint window. The major enforcement entity on the federal level is the FTC. The FTC also serves as the primary federal complaint window, although lawmakers have carved out certain jurisdictional zones for other entities to regulate.²⁷

20. See generally Buell, *supra* note 10.

21. *Id.*; see generally Silber, *supra* note 2.

22. Silber, *supra* note 2, at 15 (quoting WALTER LIPPMANN, DRIFT AND MASTERY 68 (1914)).

23. See Jane K. Winn, *Introduction: Is Consumer Protection an Anachronism in the Information Economy?*, in CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY': MARKETS AND THE LAW 1 (Jane K. Winn ed., 2006).

24. See *infra* notes 27–47 and accompanying text.

25. See *infra* notes 48–81 and accompanying text.

26. See *infra* notes 82–87 and accompanying text.

27. The FTC is empowered and directed as follows:

[To] prevent persons, partnerships, or corporations, *except* banks, savings and loan institutions . . . Federal credit unions . . . common carriers . . . air carriers and foreign air carriers and . . . persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

15 U.S.C. § 45(a)(2) (2000) (emphasis added).

For instance, the Consumer Product Safety Commission (CPSC) supplements the FTC and has a narrower charge focused specifically on product quality as it relates to safety.²⁸ Additionally, the Food and Drug Administration (FDA) is concerned with the safety and integrity of specific categories of consumer goods.²⁹

Several other federal agencies handle consumer complaints. Under the auspices of the Department of Transportation, the National Highway Traffic Safety Administration (NHTSA) regulates the safety of motor vehicles and motor vehicle equipment.³⁰ The Federal Aviation Administration (FAA) is responsible for air transportation safety,³¹ while the Aviation Consumer Protection Division (ACPD) accepts complaints from consumers who experience air travel service problems.³² The Federal Communications Commission (FCC)³³ has jurisdiction over cellular phone fraud.³⁴ Having trouble with your retail bank? The obscure Office of the Comptroller of the Currency (OCC) is the regulator.³⁵ Although an exhaustive list of federal enti-

28. The CPSC “is charged with protecting the public from unreasonable risks of serious injury or death from more than 15,000 types of consumer products under the agency’s jurisdiction.” CPSC Home Page, <http://www.cpsc.gov/about/about.html> (last visited July 10, 2007). The Commission has a statutory declaration of purpose:

(1) to protect the public against unreasonable risks of injury associated with consumer products; (2) to assist consumers in evaluating the comparative safety of consumer products; (3) to develop uniform safety standards for consumer products and to minimize conflicting State and local regulations; and (4) to promote research and investigation into the causes and prevention of product-related deaths, illnesses, and injuries.

15 U.S.C. § 2051(b) (2000).

29. The FDA has responsibility “for ensuring that foods are safe, wholesome and sanitary; human and veterinary drugs, biological products, and medical devices are safe and effective; cosmetics are safe; and electronic products that emit radiation are safe. The FDA also ensures that these products are honestly, accurately and informatively represented to the public.” What FDA Regulates, U.S. Food & Drug Admin., <http://www.fda.gov/comments/regs.html> (last visited July 10, 2006). The FDA is the “granddaddy” of consumer protection, predating the FTC’s existence by eight years. Silber, *supra* note 2, at 19–20. Silber observes that the creation of the FDA by the Pure Food and Drug Law of 1906 is “[p]aradigmatic of the foundational, pioneering, enduring consumer protection laws that were enacted during the Progressive era.” *Id.* at 19.

30. Under 49 U.S.C. § 30101, the NHTSA is charged with “prescrib[ing] motor vehicle safety standards for motor vehicles and motor vehicle equipment in interstate commerce” and is additionally charged with “carry[ing] out needed safety research and development.” 49 U.S.C. § 30101(1)–(2) (2000).

31. The FAA can exercise authority governing aviation safety and may issue regulations that are related to flight safety. 49 U.S.C. §§ 44701–44723 (2000).

32. ACPD, Air Travel Service Problems: How Complaints are Handled, <http://airconsumer.ost.dot.gov/problems.htm> (last visited July 10, 2007).

33. See 47 U.S.C. § 332 (2000).

34. The FCC maintains a Consumer and Government Affairs Bureau. See <http://www.fcc.gov/cgb> (last visited Feb. 20, 2007).

35. Office of the Comptroller of the Currency: Consumer Complaints and Assistance, <http://www.occ.treas.gov/customer.htm> (last visited July 10, 2007).

ties that provide consumer protection would be endless, the oft-overlooked U.S. Postal Inspection Service, which wields extraordinary power over scams and fraud, should not be omitted.³⁶

State-level authorities also play prominent roles in the consumer protection realm. State attorneys general prosecute consumer protection complaints, and a variety of other state agencies receive and address consumer grievances, ranging from public utilities commissions to state insurance commissions.³⁷ Even some local police departments³⁸ and prosecutors³⁹ are involved in consumer protection. Finally, civil causes of action⁴⁰ and private systems of self-regulation⁴¹

36. Under 18 U.S.C. § 1028, the United States Postal Inspection Service has authority to investigate identity takeovers and identity fraud. Further, under 18 U.S.C. §§ 1029, 1030, 1343, and 2701 (2000), and 18 U.S.C. § 1037 (Supp. 2005), the Postal Inspection Service has authority to investigate “electronic” offenses including “fraud schemes and other crimes that may occur online and involve the misuse of the mail or of the Postal Service.”

This includes using or selling stolen or counterfeit access devices, such as credit card numbers; using protected computers without proper authority or exceeding authorized access; using computer communications in a scheme to defraud; using a false identity when sending commercial e-mails to mislead or deceive recipients, as with spam; and unauthorized access to communications that are stored electronically via a communications service.

U.S. POSTAL INSPECTION SERVICE, JURISDICTION AND LAWS, <http://www.usps.com/postalinspectors/jurislaw.htm> (last visited July 10, 2007). Under more familiar authority, the Postal Inspection Service can investigate mail fraud. “Inspectors place special emphasis on mail fraud scams related to advance fees, boiler rooms, health care, insurance, investments, deceptive mailings and other consumer frauds, especially when they target the elderly or other susceptible groups.” This authority is granted by 18 U.S.C. §§ 1341, 1342, and 1345, and 39 U.S.C. §§ 3005 and 3007. U.S. POSTAL INSPECTION SERVICE, JURISDICTION AND LAWS, <http://www.usps.com/postalinspectors/jurislaw.htm> (last visited July 10, 2007).

37. State enforcement mechanisms also include state prosecutors, state health departments, and state licensing departments.

38. For a mechanism for reporting identity theft to the Seattle Police Department, see http://www.seattle.gov/police/general_info/report.htm#ID%20theft (last visited July 10, 2007).

39. See L.A. County Dist. Att’y Consumer Prot. Home Page, <http://da.co.la.ca.us/cpd/default.htm> (last visited July 10, 2007).

40. Private causes of action exist under tort, contract, and unlawful trade practices statutes that enable consumers to recover damages from fraud. Class action is often the chosen vehicle when recovery amounts are small. For example, in December 2006, a group of gasoline consumers in California filed suit against seventeen gasoline service stations and oil companies claiming that they were being defrauded and overcharged “at the pump” when the stations and companies failed to “compensate for changes in gasoline volumes when temperatures rise.” *Suit Charges Warm Gasoline*, N.Y. TIMES, Dec. 15, 2006, at C10.

41. Some examples include market competitors reporting on the unfair practices of each other, as well as private and third-party certification associations (e.g., Better Business Bureau, Underwriters Laboratory). Local and national media (through consumer investigations and exposés) also enter as a player in the consumer protection realm. For a brief aside about the positive impact of the media on the justice system at large (within the context of an article about the negative impact on the criminal side), see Sara Sun Beale, *The News Media’s Influence on Criminal Justice Policy: How Market-Driven News Promotes Punitiveness*, 48 WM. & MARY L. REV. 397, 402–03 (2006). Many professions self-regulate through self-credentialing and internal discipline. See, e.g., Am. Inst. of Certified Pub. Accountants Code of Prof’l Conduct, Composi-

also provide consumer protection. For example, a consumer defrauded by an attorney can sue the attorney for malpractice *and* rely on the state bar to discipline the attorney.

It would seem that this cornucopia of regulatory and enforcement entities could knock out fraud using a combination of specialization and sheer muscle. Yet, as evidenced by the number of complaints⁴² and increased monetary losses,⁴³ consumers are still greatly susceptible to fraud. This can be partially explained by the fact that consumer protection is primarily driven by consumer complaints.⁴⁴ Thus, the question arises: in this diffuse institutional universe,⁴⁵ how does the consumer know if there is a complaint window? Furthermore, which window should she approach? Even the sophisticated consumer might be confused about where to lodge a claim. This diffuse regime works inefficiently by leading consumers to attempt to lodge complaints at multiple windows successively, raising fraud reporting costs, or leading consumers to believe that complaining is futile.

For example, if a consumer had a complaint about a fraudulent charge from her cellular phone company on her bank credit card,⁴⁶ she might contact the credit card marketer, the issuing bank, the cellular phone company, the FCC, her state attorney general, her state public utilities commission, or even the OCC.⁴⁷ But even if she is familiar with this alphabet soup, it is unclear where responsibility for enforcement ultimately lies. Simply put, there is no single entity that can address the problem.

The system for handling identity theft further illustrates the diffusion problem. An identity theft victim would not likely know where to start restoring her credit record. Although postal inspectors, the local police, the FTC, and the state attorney general all have authority, there is no central clearinghouse for the problem. Thus, identity theft victims are left confused and unprotected.

tion, Applicability, and Compliance, *available at* <http://www.aicpa.org/about/code/comp.htm> (last visited July 10, 2007); Am. Bd. of Psychiatry & Neurology, Inc., Mission Statement, *available at* <http://www.abpn.com/mission.htm> (last visited July 10, 2007).

42. Consumer Sentinel, the “complaint database developed and maintained by the Federal Trade Commission” contained “over 3.5 million fraud and identity theft complaints” as of the end of 2006. 2006 FTC COMPLAINT DATA, *supra* note 4, at 2–3.

43. The total dollar amount “paid out” per fraudulent transaction nearly doubled from 2004 to 2006. *Id.* at 6.

44. Education, vigilance, and self-protection also enhance consumer protection.

45. Thank you to Stephen Skowronek, who first introduced me to the term “institutional universe” in his class in 1991.

46. For this example, assume a wrongful surcharge.

47. This assumes that the consumer knows and can navigate the system.

B. *The Reactive Enforcement Paradigm*

In addition to the problem of diffusion, consumer protection is largely complaint-driven. In other words, current law enforcement is reactive, rather than proactive.⁴⁸ In this multi-pronged enforcement system atmosphere, lawmakers' current approaches to enforcing fraud are frustrated by their inability to anticipate the next creative scheme.⁴⁹ Changes in technology and markets, combined with human ingenuity, can create innumerable permutations of unanticipated and not clearly unlawful fraudulent schemes.⁵⁰ In short, "[i]t is in the nature of markets and human ingenuity to produce new iterations and technologies of economic predation."⁵¹

Currently, selection of consumer groups for protection, like the selection of schemes to target, is largely *ad* and *post hoc*.⁵² As an unlawful practice emerges, it inevitably invites a *post hoc* approach that fails to anticipate the next scam to emerge or group to be targeted. As the time-worn military aphorism says, "generals are always fighting the *last war*"⁵³ and are, therefore, unprepared and ineffective in the next

48. See generally CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY': MARKETS AND THE LAW (Jane K. Winn ed., 2006).

49. See generally Buell, *supra* note 10.

50. *Id.* at 2043.

51. *Id.*

52. *Id.* at 1987–96. Enforcement agencies identify vulnerable groups, single out scams for enforcement, and implement educational initiatives. The search function of the FTC Bureau of Consumer Protection About Us Home Page, <http://www.ftc.gov/bcp/about.shtm>, yields a basic indication of how the FTC is addressing both groups and scam typologies. For example, queries on January 20, 2007 for "senior citizens" yielded 313 results; for "senior citizens and telemarketing," 249 results; and for "Hispanic," 345 results. Queries for "telemarketing" yielded 24,211 results; for "door-to-door," 179 results; and for "Nigerian," FTC Consumer Alert, *supra* note 8, 44 results. State websites reveal much the same. See, e.g., N.Y. State Consumer Prot. Bd. Home Page, <http://www.consumer.state.ny.us> (last visited July 10, 2007). This website contains items directed at several groups. See, e.g., Press Release, N.Y. State Consumer Prot. Bd., Nueva Ley para Prevenir el Robo de Identidad [New Law for Prevention of Identity Theft] (Nov. 8, 2006), available at <http://www.consumer.state.ny.us/pressreleases/2006/nov082006.htm> (Spanish-speakers); Press Release, N.Y. State Consumer Prot. Bd., Two Different Companies with Same Name Offer LSAT Course (Oct. 13, 2006), available at <http://www.consumer.state.ny.us/pressreleases/2006/oct132006.htm> (law school admissions test-takers); Press Release, N.Y. State Consumer Prot. Bd., CPB Announces Winner of the Latest International Sweepstakes: Nobody (Sept. 7, 2006), available at <http://www.consumer.state.ny.us/pressreleases/2006/sept72006.htm> (sweepstakes and lottery players).

53. Winston Churchill wrote the most famous version of this aphorism: "It is a joke in Britain to say that the War Office is always preparing for its last war." WINSTON CHURCHILL, I THE SECOND WORLD WAR 426 (Houghton Mifflin 1985) 1948.

innovative battle. Policymakers, regulators, and enforcement officials face the same challenge⁵⁴ in addressing fraud's unending novelty.⁵⁵

The challenge of addressing novel consumer fraud is everywhere. To better illustrate the problem, the following subsections briefly explore three examples of novel consumer fraud: (1) telemarketing scams targeting older Americans; (2) fraudulent practices targeting non-English speakers; and (3) predatory lending targeting low-income and minority communities.

1. *Telemarketing Scams*

In the early 1990s, an FBI investigation into telemarketing fraud in Salt Lake City led to the enactment of targeted legislation.⁵⁶ The enactment of the Senior Citizens Against Marketing Scams Act (SCAMS Act)⁵⁷ was a classic *post hoc* effort. Under that law, consumers over the age of fifty-five receive special protection against telemarketing scams.⁵⁸ The protection includes enhanced sentences for perpetrators who conduct telemarketing in connection with various other fraud-related crimes.⁵⁹ Thus, in this instance, Congress addressed a specific activity—telemarketing scams—in the broader context of protecting the intended group.

That type of legislative approach begs the question: given the size of the protected class, was the enforcement mandate truly attainable? By 2002, nearly sixty million Americans were over the age of fifty-five⁶⁰—over 20% of the total population.⁶¹ How can the government

54. See, e.g., Usha Rodrigues, *Let the Money Do the Governing: The Case for Reuniting Ownership and Control*, 9 STAN. J.L. BUS. & FIN. 254, 257 (2004) (arguing that regulators are prone to fight the last battle in the Sarbanes-Oxley context).

55. Buell, *supra* note 10, at 1996.

56. U.S. SENTENCING COMM'N, REPORT TO CONGRESS: ADEQUACY OF PENALTIES FOR FRAUD OFFENSES INVOLVING ELDERLY VICTIMS 2-3 (1995).

57. See SCAMS Act of 1994, 18 U.S.C. § 2326 (2000):

A person who is convicted of an offense under section 1028, 1029, 1341, 1342, 1343, or 1344, or a conspiracy to commit such an offense, in connection with the conduct of telemarketing—(1) shall be imprisoned for a term of up to 5 years in addition to any term of imprisonment imposed under any of those sections, respectively; and (2) in the case of an offense under any of those sections that—(A) victimized ten or more persons over the age of 55; or (B) targeted persons over the age of 55, shall be imprisoned for a term of up to 10 years in addition to any term of imprisonment imposed under any of those sections, respectively.

For the SCAMS Act in a broader context, see Ryan Y. Blumel, *Mail and Wire Fraud*, 42 AM. CRIM. L. REV. 677, 678-79, 697-98 (2005).

58. See 18 U.S.C. § 2326 (2000).

59. *Id.*

60. DENISE SMITH, U.S. CENSUS BUREAU, CURRENT POPULATION REPORTS, THE OLDER POPULATION IN THE UNITED STATES: MARCH 2002 1 (Apr. 2003), available at <http://www.census.gov/prod/2003pubs/p20-546.pdf>.

effectively educate a group this size about a single issue? How can the government efficiently enforce such a broad, protective mandate without wasting resources?

Additionally, could scammers simply use a different technological means of defrauding seniors than the telephone? Would this defeat the legislative scheme? Moreover, would the protected class understand when they were being defrauded? Would they know where to file a grievance or how to report an inchoate SCAMS Act violation? This example illustrates the problems of limited government resources, continuous fraud innovation, and the impracticalities of teaching the protected class⁶² how to interact with a diffuse environment for registering complaints.⁶³

2. *Non-English Speakers*

Non-English speakers constitute another group that has received targeted protection. In 2004, the FTC launched a consumer fraud awareness campaign directed toward Spanish-speakers, encouraging them “to identify fraudulent and deceptive business practices and to inform the FTC when they occur.”⁶⁴ This program was intended to “complement the agency’s enforcement initiative against frauds targeting Hispanic consumers.”⁶⁵ The campaign exemplified the classic approach and used both the consumer’s perspective (education) and the perpetrator’s perspective (enforcement initiatives⁶⁶ encouraging targets to report) to combat a problem for a single group.

Policymakers should view this particular consumer fraud issue as only one symptom of a larger political and cultural problem that is not

61. In 2002, the U.S. Census estimated the total United States population at 288 million. See <http://www.census.gov/popest/states/tables/NST-EST2006-01.xls> (last visited July 10, 2007).

62. If the class was sufficiently narrow, education could potentially be more effective in this type of case.

63. Members of this protected class could also simply call their local police about a telemarketing scam. Reporting to the FTC, the FBI, or the local office of the U.S. Attorney is a less convenient scenario.

64. Press Release, Fed. Trade Comm’n, FTC Launches Consumer Fraud Awareness Campaign Targeted to Spanish Speakers (Sept. 9, 2004), available at <http://www.ftc.gov/opa/2004/09/scampaign.htm>.

65. *Id.*

66. See FED. TRADE COMM’N, *HISPANIC OUTREACH FORUM & LAW ENFORCEMENT WORKSHOP: A SUMMARY OF THE PROCEEDINGS* (Oct. 2004), available at <http://www.ftc.gov/reports/hispanicoutreach/hispanicoutreach.pdf> [hereinafter *HISPANIC OUTREACH FORUM*]; Press Release, Fed. Trade Comm’n, FTC Continues Campaign to Stop Scams Aimed at Hispanics (Jan. 24, 2006), available at <http://www.ftc.gov/opa/2006/01/ohiorelease.shtm>; Press Release, Fed. Trade Comm’n, Recent Law Enforcement Actions Involving Hispanic Consumers (Apr. 17, 2002), available at http://www.ftc.gov/opa/2004/04/hispanic_oldcases.shtm.

limited to fraud.⁶⁷ Here, the regulators did their best to educate the consumer group (both about fraud schemes and the safety of reporting fraudulent activity) and even invested extra resources to protect them from fraud. Nonetheless, the question again arises: will this tool ultimately be effective?

One scholar concluded that the best way to enable the non-English speaking community to feel safe enough to report crime is to enact a wholesale preemptive federal provision for “use and derivative use immunity . . . for unauthorized aliens who are victims of or witnesses to crime.”⁶⁸ In the absence of such a dramatic provision, it would take extensive education about our diffuse system⁶⁹ to protect this group. Our current efforts may help on the margin, but resource limitations will prohibit the authorities from reaching groups that do not trust authority.

3. *Predatory Lending and Low-Income or Minority Communities*

In 2000, the Department of Housing and Urban Development (HUD) and the Treasury Department recommended that residents of lower-income and minority communities be protected against predatory lending.⁷⁰ They also singled out borrowers, including minorities, females, the elderly, and low-income individuals.⁷¹ This kind of protection created several intersections of potentially protected groups, while using borrowers as the driving category.

Special regulation of sub-prime lending at the federal, state, and local levels is not a novel concept.⁷² Congress created the Truth in Lending Act (TILA)⁷³ and the Real Estate Settlement Procedures Act of 1974⁷⁴ to use disclosure and education to broadly address predatory lending.⁷⁵ The Home Ownership and Equity Protection Act

67. See, e.g., Orde F. Kittrie, *Federalism, Deportation, and Crime Victims Afraid to Call the Police*, 91 IOWA L. REV. 1449, 1450–54 (2006) (arguing that unauthorized aliens are less likely to report crime than other citizens).

68. *Id.* at 1457.

69. This is a system often mistrusted by non-English speaking victims. See *id.* at 1450–54.

70. See DEP'T OF HOUS. & URBAN DEV. & DEP'T OF TREASURY, HUD-TREASURY JOINT REPORT ON PREDATORY LENDING 72 (2000) [hereinafter HUD-TREASURY JOINT REPORT] available at <http://www.hud.gov/library/bookshelf12/pressrel/treasrpt.pdf>.

71. *Id.* at 71.

72. R. Stephen Painter, Jr., *Subprime Lending, Suboptimal Bankruptcy: A Proposal to Amend §§ 522(f)(1)(B) and 548(a)(1)(B) of the Bankruptcy Code to Protect Subprime Mortgage Borrowers and Their Unsecured Creditors*, 38 LOY. U. CHI. L.J. 81, 95 (2006).

73. Truth in Lending Act, 15 U.S.C. §§ 1601–1667f (2000).

74. Real Estate Settlement Procedures Act of 1974, 12 U.S.C. §§ 2601–2617 (2000).

75. See Painter, *supra* note 72, at 95.

(HOEPA)⁷⁶ attempted to regulate the lenders directly by limiting contractual terms.⁷⁷ Yet, decades later, HUD and the Department of Treasury still found it necessary to address the problem of predatory lending by recommending that new enforcement efforts focus on “Hot Zones” in urban centers.⁷⁸

The “Hot Zones” effort is an example of a *post-post hoc* approach. When the agencies found that legislating broadly from above was ineffective, they renewed their efforts. The breadth of the category in this renewed effort, which included minority, female, elderly, and low-income groups, again proved to be too large of a target for effective enforcement—similar to the SCAMS Act. Additionally, adding groups to a special protection list tends to spread resources thin. Unsurprisingly, politics dictate the expansion of the protected set.

The three aforementioned case studies nicely illustrate some of the drawbacks of the reactive approach. First, in each example, authorities chased activities that had already exacted significant damage on consumers. Second, despite these efforts, the groups intended for protection often remained unprotected, and the activities intended for extinction survived. Despite the aggressive approaches in these case studies, older consumers remain a prime target for fraud, with individuals ages fifty and over reporting⁷⁹ \$152 million in losses in 2004.⁸⁰ Fraud targeted at Spanish-speakers persists in spite of federal and local education efforts.⁸¹ As for the final predatory lending example, laws that attempt to protect broad groups have proven ineffective.

Finally, in each of these cases, there are examples of ineffective group definition or inadequate matches of enforcement resources to agency mandates. In rethinking an approach to consumer protection, policymakers must consider ways to break out of the *post hoc* method. It is often excessively ambitious in its enforcement goals relative to its resources and political reality and occasionally so inclusive in group definitions that the protected core constituency receives only diluted protection.

76. Home Ownership and Equity Protection Act of 1994, Pub. L. No. 103-325, 108 Stat. 2190 (codified at scattered sections of 15 U.S.C.).

77. See Painter, *supra* note 72, at 96.

78. See HUD-TREASURY JOINT REPORT, *supra* note 70, at 114-19.

79. Granted, there is no way to calculate exactly how much unreported and undetected fraud there is within this population.

80. AGE 50 AND OVER, *supra* note 9, at 4.

81. See HISPANIC OUTREACH FORUM, *supra* note 66, at 7-10.

C. *Flaws with the Current Approach*

Despite the extensive consumer protection system in the United States, the two dynamics described above—diffuse enforcement and a reactive approach—have intersected to create a permanent system of failure. This happened despite the spate of resources aimed directly at addressing the consumer protection problem.

As noted earlier in this Part, fraud innovation is difficult to anticipate and address.⁸² This issue can be called the Transportation Safety Administration (TSA) problem. The TSA authorities, charged with the responsibility of keeping air travel safe,⁸³ are more effective at protecting against behavior that they have already observed.⁸⁴ Because staying ahead of innovative perpetrators is challenging, the TSA tends to focus enforcement efforts on recognizing the patterns of past threats. This means that each new type of fraud may go undetected and unpunished.

The TSA problem is worse in the twenty-first century.⁸⁵ As technology evolves, new, corporate-driven products and services become increasingly difficult to understand. As stand-alone swindlers develop new schemes, regulators will constantly fail to think ahead of the perpetrators. Predicting the next round of fraud is an exercise in institutional frustration.

Furthermore, the alphabet soup of agencies charged with enforcement has had great difficulty addressing *known* schemes. As discussed above, consumers face a confusing arena for lodging complaints. There is also an inter-institutional problem that may be termed the “Texas Leaguer” problem. Texas Leaguer is baseball slang for a short, softly hit fly ball that tantalizingly falls in between multiple infielders and outfielders for a base hit.⁸⁶ Similarly, with limited resources, agencies will not often catch fraud schemes, because a player

82. See generally Buell, *supra* note 10.

83. “The Transportation Security Administration protects the Nation’s transportation systems to ensure freedom of movement for people and commerce.” See TSA: Mission, Vision, and Core Values, http://www.tsa.gov/who_we_are/mission.shtm (last visited July 10, 2007).

84. Examples include actions prohibiting passengers from carrying sharp objects on commercial aircraft after the terrorist attacks of September 11, 2001 or requiring passengers to remove their shoes for inspection after an individual attempted to ignite a “shoe bomb” on a flight from Paris to Miami.

85. For an example of a twenty-first-century consumer protection problem and a proposed resolution, see Jean Braucher, *New Basics: Twelve Principles for Fair Commerce in Mass-Market Software and Other Digital Products*, in CONSUMER PROTECTION IN THE AGE OF THE ‘INFORMATION ECONOMY’: MARKETS AND THE LAW 177 (Jane K. Winn ed., 2006).

86. See Dictionary.com Unabridged (version 1.1), Texas Leaguer Definition, <http://dictionary.reference.com/browse/texas%20leaguer> (based on RANDOM HOUSE UNABRIDGED DICTIONARY (2006)) (last visited July 10, 2007).

(the enforcement agency) will not “dive” for it, because an agency believes it is beyond its mandate or jurisdiction. Granted, when addressing egregious schemes, the entities occasionally cooperate better.⁸⁷ Many schemes fall through the cracks, however, or, to push the analogy, fall as base hits to the perpetrators’ benefit and to the public’s detriment.

As noted in the Introduction, the United States has an expensive, reactive consumer protection system that requires significant improvement. Initiatives to improve the patchwork system often fall short for institutional reasons. Yet the system is not doomed. Policymakers can put the current system and its expertise to better use. Put simply, policymakers can reduce consumer fraud effectively and efficiently if they identify and modify the incentives of the players in the transactional world.

III. REBALANCING INCENTIVES FOR FRAUD PERPETRATORS AND CONSUMERS

In every transaction, policymakers want the fraud perpetrator to take on more risk and the consumer to take on less. The current system aspires to accomplish this, but has a flawed regulatory network and broadly tailored, cost-prohibitive laws. The approach proposed herein would be narrow enough to implement effectively, but would still have sufficient impact to diminish the incentives for perpetrators to commit fraud.

At its most basic level, this Article proposes that policymakers hyper-protect two definable groups of consumers. In so doing, they can simultaneously achieve several objectives: (1) protecting those groups; (2) shifting fraudulent activity away from the vulnerable to those more likely to detect and report fraud and better able to absorb it; and (3) enhancing consumer fraud deterrence throughout the population.

In order to identify the most effective and efficient policies for consumer fraud deterrence, policymakers must dissect the incentive structures for fraud perpetrators and consumers. This dissection requires basic microeconomic analysis. Policymakers can rebalance incentives

87. One example is the multi-state investigations into tobacco companies and Enron in the wake of the 2000-2001 California power crisis. See NAT’L ASS’N OF ATTY’S GEN., *MULTISTATE SETTLEMENT WITH THE TOBACCO INDUSTRY*, available at <http://www.library.ucsf.edu/tobacco/litigation/msa.pdf>. See also Press Release, Wash. State Office of the Att’y Gen., *Multi-State Settlement with Enron Signed Today* (Aug. 24, 2005), available at http://www.atg.wa.gov/press_release.aspx?&id=4062.

if they examine each of the players separately and understand how they interact when certain policy actions are taken.

As mentioned above, analysis of the incentive structures reveals that, by selecting narrowly defined groups for hyper-protection, policymakers will both protect these groups and enhance overall consumer fraud deterrence. The selected group population receives direct protection. If the group is socially vulnerable, this effect has societal value in and of itself.

Further, group protection enhances the perpetrator's risk in targeting that group and shifts fraud activity toward the total pool of less vulnerable individuals. This makes fraud generally less attractive as a business proposition. There is a question of whether protecting one vulnerable group from fraud will compel the perpetrator to single out another vulnerable group. There is some power to this claim, but there would need to be perfect fluidity in the fraud perpetration labor market to fully support it—perpetrators who specialize in scamming a group might not be able to translate their expertise into scamming another group. For example, a member of the Latino community operating an immigration scam targeted at unauthorized aliens may not easily move into the realm of scamming the elderly by selling them ersatz vitamins.

Finally, if members of the hyper-protected group are distributed broadly across the population and membership is narrow enough to match enforcement resources, scammers targeting the general population would become concerned that they might inadvertently hit a more costly target. There are two types of groups policymakers could choose to protect. One would be an externally identifiable group. The other group might be artificially designed for maximum concealment from the perpetrator for the purpose of enhancing economy-wide deterrence.

In order to understand the theory of this systemic change, this Part analyzes the economic incentives of the actors in the consumer fraud world. Section A establishes that fraud perpetrators are rational actors.⁸⁸ This is critical, because rational operators will respond to incentives. If fraud perpetrators were irrational, the tool kit for changing behavior would be vastly diminished.

Section B discusses perpetrators' motivating factors and explores how the risk of detection and the degree of potential sanctions for fraud interplay through the use of a basic equation.⁸⁹ It then shows

88. See *infra* notes 91–104 and accompanying text.

89. See *infra* notes 105–127 and accompanying text.

how policymakers can manipulate this equation to the public's advantage. Section B also dissects the decision-making equation for the corporate or enterprise perpetrator.

Finally, Section C explores how the enhanced protection of certain groups can shift a scammer's focus toward those who are better situated to combat it.⁹⁰ Furthermore, hyper-protection can enhance deterrence in the general population. Section C demonstrates this by showing the impact of this strategy on the decision-making equations for both perpetrators and consumers. If implemented properly, such a strategy increases the risks to perpetrators (reducing incidence of fraud) and encourages more transactional activity as consumers become more confident that fraud has been diminished.

A. Individual Fraud Perpetrators Are Rational Actors

In order to influence an actor through incentives, the actor must be rational. Furthermore, for a broad policy to be influential, the net set of actors must be rational. Economic incentives, detection, or punishment modifications could not deter psychopaths from committing offenses.⁹¹ The question is plain: is fraud a rational activity for a set of individuals? If so, policymakers can alter perpetrators' behaviors by increasing their risk factors and potential consequences for their actions.

The literature indicates that some individuals choose non-organized crime as their career path.⁹² In a seminal 1992 work, James Q. Wilson and Alan Abrahamse asked the age-worn question, "does crime pay?"⁹³ Their survey showed that certain types of high-rate offenders believed that crime paid better than a straight job.⁹⁴ This applied specifically to the offenses of auto theft (the most comparatively lucrative

90. See *infra* notes 128–162 and accompanying text.

91. This is not to dismiss that certain fraud perpetrators might be "in the game" partially (or perhaps, totally) for the thrill. That behavior could be defined as rational in that these perpetrators are seeking to maximize utility, but through non-monetary means. The evidence in the literature, however, indicates that the monetary rewards are sufficient incentive—and this Article limits the definition of the rational perpetrator to an individual who is only factoring risk and monetary reward into decision-making. See generally Part III.A.1, which addresses the differential in risk appetites across perpetrators.

92. See ROBERT COOTER & THOMAS ULEN, *LAW AND ECONOMICS* 417 (4th ed. 2004).

93. James Q. Wilson & Allan Abrahamse, *Does Crime Pay?*, 9 *JUST. Q.* 359 (1992).

94. *Id.* at 367. The inmates surveyed in the study did not account for "the costs of arrest, prosecution . . . incarceration . . . stigma . . . lawyers and bondsmen . . . and the discomfort, violence and loss of freedom associated with prison life." *Id.* at 369. The authors admittedly could not estimate these costs.

criminal business), robbery, and swindling.⁹⁵ Robbery and swindling yielded an expected income roughly twice that of the legal working alternatives for the actor.⁹⁶ Interestingly, those engaged in swindling had the highest legal working income alternatives,⁹⁷ which may reflect the more cerebral nature of their chosen criminal specialty. Given that swindling pays from the perspective of the high-rate offender⁹⁸ and that these offenders have the best straight alternatives, it is unsurprising that sophisticated swindling schemes emerge.

Wilson and Abrahamse reached the general conclusion that, in most other cases, crime did not pay better than the alternative. They explained that the individuals they studied were "temperamentally disposed to overvalue the benefits of crime and to undervalue its costs,"⁹⁹ because they were more focused on the immediate gains from their crime rather than the potential costs and risks. Fraud perpetrators, however, may be less susceptible to this rule. Wilson and Abrahamse noted that, when prison time was factored into the equation, crime did not pay for any frequently committed crime. In contrast, the survey showed that expected income for those engaged in burglary and theft was \$5,711 versus a legitimate earnings alternative of \$5,540.¹⁰⁰ Swindlers, however, earned \$14,801 versus a legitimate earnings alternative of \$6,245.¹⁰¹

A swindler would need to discount the expected value of crime much more than the burglar to make commission of his crime look less attractive. Even if swindlers are temperamentally disposed to overvalue the benefits of crime, there would be comparatively more benefits to discount in the case of the swindler.¹⁰² Fraud perpetrators may have absorbed the notion that fraud is more lucrative than going straight. Further, many fraud schemes could purposely teeter on the edge of legality or could be craftily designed to avoid detection.

95. Swindling probably matches best with the activities addressed here, as the authors used fraud and forgery as their proxies for this category. *Id.* at 361.

96. *See id.* at 367.

97. *Id.*

98. Wilson and Abrahamse also noted that for the "mid-rate" offender (as opposed to the high-rate offender), only auto theft paid more than the straight legal working alternative. *Id.* However, again reflecting the potentially more "cerebral" nature of the offender, the mid-rate swindlers had the highest legal working wage alternatives of all mid-rate and high-rate offenders. *Id.*

99. Wilson & Abrahamse, *supra* note 93, at 372.

100. *Id.* at 367.

101. *Id.*

102. Wilson and Abrahamse's general conclusions about the discounting of costs and risks may fit well with other more impulsive crimes (they use burglary, auto theft, and armed robbery as examples). *Id.* at 375.

Fraud perpetrators may implement more marginally unlawful schemes due to overvaluation of the potential benefits of the scheme.¹⁰³

Wilson and Abrahamse's work demonstrates that a consumer fraud perpetrator is the classic Holmesian "bad man."¹⁰⁴ In other words, consumer fraud perpetrators make calculations about risks and payoffs in determining their behavior and course of action. This means that policymakers can derive the perpetrator's internal decision-making equation and influence it for the benefit of consumers. While this Article focuses mostly on deterring fraud that rises to the level of criminal conduct, the approach offered here can—and should—also be applied more broadly to unfair and deceptive conduct. That conduct is often more routinized and common among repeat players, including large and small firms. Deterrence may be more effective with repeat players and players with reputations than it would be for lone scammers.

B. *Dissecting The Fraud Perpetration Equation*

What would a fraud perpetration calculation look like? What would the key elements be? How could policymakers manipulate these elements to affect the behavior of the perpetrator? Assuming a rational fraud perpetrator, she would weigh the benefit of her scheme against the elements of the deterrence regime.¹⁰⁵ Does deterrence

103. One concern is that "over-deterrence" may kill legitimate activity at the margin. Those who engage in activity that is lawful but approaches the line may not engage in legitimate transactions, because they are more cautious. The loss of the societal benefit from these borderline transactions should be considered.

104. As Holmes famously wrote:

You can see very plainly that a bad man has as much reason as a good one for wishing to avoid an encounter with the public force, and therefore you can see the practical importance of the distinction between morality and law. A man who cares nothing for an ethical rule which is believed and practised by his neighbors is likely nevertheless to care a good deal to avoid being made to pay money, and will want to keep out of jail if he can.

O.W. Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 459 (1897). In an address to the students and faculty of Boston University School of Law, Holmes said, "[Y]ou must look at [the law] as a bad man, who cares only for the material consequences which such knowledge enables him to predict, not as a good one, who finds his reasons for conduct, whether inside the law or out of it, in the vaguer sanctions of conscience." M.H. Fisch, *Justice Holmes, the Prediction Theory of Law, and Pragmatism*, 39 J. PHIL. 85, 86 (1942) (quoting OLIVER WENDELL HOLMES, *The Path of the Law*, in COLLECTED LEGAL PAPERS 167, 171 (1920)). Thank you to Brad Wendel for inspiring me to re-read Holmes.

105. In his seminal work on the economics of criminal law, Gary Becker suggests that individuals engage in an implicit cost-benefit analysis when deciding to commit a criminal act. See Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968). Since the publication of Becker's article, "well over two hundred articles have been written on the economics of enforcement." A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LITERATURE 45, 45 (2000). Polinsky and Shavell sur-

generally work for consumer fraud? Surveying the literature,¹⁰⁶ Robert Cooter and Thomas Ulen concluded that “increases in the probability of arrest, conviction, and punishment, and increases in the severity of punishment, have a significant deterrent effect on the population at large, as well as on that small portion of the population . . . most likely to commit crime.”¹⁰⁷ Given that fraud perpetrators are, by and large, rational actors—especially within the general population of criminal actors—Cooter and Ulen’s conclusion applies to these individuals.

1. *The Basic Individual Criminal Fraud Model*

A fraud perpetrator should behave in ways that maximize the expected economic value of her scheme. There are several variables that an actor in the fraud business must consider when crafting a scheme or deciding whether to embark on that scheme: expected reward, likelihood of detection, likelihood of prosecution, and likeli-

veyed this literature and offered a refined view about determining optimal levels of enforcement in theory and practice. *Id.* at 70–72. This Article will rest on the Polinsky-Shavell survey and analysis. Richard Posner famously observed that “the substantive doctrines of the criminal law . . . can be given an economic meaning and can indeed be shown to promote efficiency.” Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM. L. REV. 1193, 1994 (1985). For the heritage of the economic approach to crime, see also Cesare Beccaria, *On Crimes and Punishments*, in *ON CRIMES AND PUNISHMENTS AND OTHER WRITINGS* 1, 21 (Richard Bellamy ed., Richard Davies et al. trans., 1995). Baron de Montesquieu and Jeremy Bentham also offered early economic analyses of crime and deterrence. See Polinsky & Shavell, *supra*, at 45 (citing MONTESQUIEU, *THE SPIRIT OF THE LAWS* (1748); JEREMY BENTHAM, *AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION* (1789)). For a critique of the limitations of the basic crime and economics literature, and a prescription for its improvement, see Alvin K. Klevorick, *On the Economic Theory of Crime*, in *CRIMINAL JUSTICE: NOMOS XXVII* 289 (J. Roland Pennock & John W. Chapman eds., 1985).

106. In answering the question concerning deterrence, Cooter and Ulen cited Isaac Ehrlich, *Participation in Illegitimate Activities: A Theoretical and Empirical Investigation*, 81 J. POL. ECON. 521, 559–61 (1973) (evincing a mixed answer on deterrence); Alfred Blumstein & Daniel Nagin, *The Deterrent Effect of Legal Sanctions on Draft Evasion*, 29 STAN. L. REV. 241 (1977) (finding that a higher probability of conviction combined with higher penalties lowered the incidence of draft evasion); and Kenneth I. Wolpin, *An Economic Analysis of Crime and Punishment in England and Wales, 1894-1967*, 86 J. POL. ECON. 815 (1978) (finding that United Kingdom crime rates were an “inverse function” of deterrent factors). The Panel on Research on Deterrent and Incapacitative Effects in 1978 (established by the National Research Council of the U.S. National Academy of Sciences) reviewed the literature, and from their report, found that the “evidence certainly favors a proposition supporting deterrence.” PANEL ON RESEARCH ON DETERRENT AND INCAPACITATIVE EFFECTS, DETERRENCE AND INCAPACITATION: ESTIMATING THE EFFECTS OF CRIMINAL SANCTIONS ON CRIME RATES (Alfred Blumstein et al. eds., 1978); accord Ann Dryden Witte, *Estimating the Economic Model of Crime with Individual Data*, 94 Q.J. ECON. 57 (1980) (supporting deterrence); CHARLES A. MURRAY & LOUIS A. COX, JR., *BEYOND PROBATION: JUVENILE CORRECTIONS AND THE CHRONIC DELINQUENT* 176–81 (1979) (imprisonment is a deterrent for a specified group of high-risk youth). See also COOTER & ULEN, *supra* note 92, at 413–15 nn.13–18.

107. COOTER & ULEN, *supra* note 92, at 416.

hood and degree of punishment. It is helpful to set out these variables in a basic equation.

The economic equation that guides an individual's criminal enterprise has simple elements.¹⁰⁸ At its most basic, microeconomic theory indicates that an individual will take action when marginal revenue from an action exceeds the marginal cost from taking said action ($MR > MC$).¹⁰⁹ Here, it is important to break the equation into components to see what drives the decisions of fraud perpetrators.

Substitute extracted value (EV) of the operation for marginal revenue. On the cost side of the equation, first take into account the simple marginal costs associated with engaging in the enterprise (MC_E).¹¹⁰ Then, take into account the expected magnitude of the sanction for the activity (S)¹¹¹ if the activity was detected and discount that by the aggregate probability (p)¹¹² of detection and prosecution. The basic equation is illustrated as follows:

$$EV > MC_E + p * S^{113}$$

When the extracted value from the crime (EV) exceeds potential costs (potential sanctions (S) discounted by the probability (p) of detection and conviction and the other marginal costs associated with committing the crime (MC_E)), the crime, absent other socio-psychological factors, may be rational to commit.¹¹⁴

108. For a labor-based model of an approach to criminal activity, see M.K. Block & J.M. Heineke, *A Labor Theoretic Analysis of the Criminal Choice*, 65 AM. ECON. REV. 314 (1975).

109. See generally ROBERT S. PINDYCK & DANIEL L. RUBINFELD, MICROECONOMICS (6th ed. 2005).

110. The marginal cost for a consumer fraud crime can be as basic as time or as sophisticated as the marginal operating costs of an offshore banking operation designed to bilk consumers.

111. Sanctions can include everything from public shame, to the costs of navigating the legal system, to systemic punishment—fines, sentences, and restrictions on future social or economic activities.

112. Detection is a staged proposition. Detection can happen at different stages in the scheme—ranging from conception, to completion, to the edge of the legal statute of limitations and beyond. Detection therefore interacts with the level of sanction. In a fraud scheme, for example, detection can involve the victim's mere discontinuation of the scam, which would leave the perpetrator with the sunk cost of the unfinished scam. Detection can also stop a scam at a point that renders it inchoate, mitigating the sanction.

113. This Article uses linear equations for the purpose of simple illustration. It is highly improbable that there would be one-to-one relationships between these variables. Quite likely, there is a "deterrence curve" that would deftly illustrate, in the aggregate, the trade-offs among risk, sanction, and incidence level of fraud commission. Deriving that curve would prove to be a broad but valuable empirical exercise, but it would best be the subject of economic study. For a robust example of a generalized, systematic, and encompassing "economic theory of public enforcement of law," see generally Polinsky & Shavell, *supra* note 105, at 45–70.

114. There is some crime, even some consumer fraud, that is not rational and may even be considered psychopathic. See PAUL BABIAK & ROBERT D. HARE, SNAKES IN SUITS: WHEN PSYCHOPATHS GO TO WORK (2006).

Whether the perpetrator commits a crime depends on a variety of factors: the perpetrator's risk aversion, the perpetrator's preference for crime as a source of income, and the accuracy with which the perpetrator can assess the risks and benefits of the crime. Yet policymakers can still adhere to a simple model, because they need only examine the general effects of adjusting these basic variables. Ultimately, policymakers should understand these variables so that they can manipulate them.

a. Illustration of the Individual Fraud Perpetrator Model

Consider the hypothetical case of a New York-based swindler who has exceptional skills in the realm of forging tickets for Madison Square Garden concert events.¹¹⁵ The swindler has the ability and equipment to create reasonable facsimiles of the holographic images that appear on these tickets. The tickets appear quite legitimate to most buyers—legitimate enough that the unfortunate buyer remains deceived until the ticket is rejected at the gate.

What is the swindler weighing? She is sophisticated enough to devise a scheme that involves production and online distribution. She also knows that the scheme will be exposed eventually. Assume that the swindler is selling front-row seats to a Rolling Stones concert—a group that appeals to a more mature demographic.¹¹⁶ Although members of the target market are often wealthy, they are sophisticated and could stymie the scheme or cause sanctions. The swindler weighs this in her calculation.

This swindler expects to retail a pair of tickets for \$2,000 (EV). Creating the tickets requires craftsmanship—she has to rent some equipment and buy special materials, costing her \$400 for the two tickets. She spends eight hours making the tickets and she values her time at \$25 per hour, because that is what she can take home working extra hours at her job in the copy shop. So her labor opportunity cost is \$200 (a total MC_E of \$600). The sanction is clear: on the local news, the District Attorney recently announced that any individual who forges and sells a ticket to a sporting or entertainment event will be prosecuted to the fullest extent of the law. Assume the punishment is six months of incarceration and a \$10,000 fine per occurrence (S).

115. For an in-depth look into this particular swindle, see Jeffrey Selingo, *When the Big-Game Ticket is Just a Big Fake*, N.Y. TIMES, Oct. 28, 2004, at G1.

116. Reviewing the 2007 Super Bowl half-time show, one advertising critic indirectly confirmed this conclusion: "Speaking for all aging baby boomers, we were delighted to see that the Rolling Stones lived long enough to perform at halftime." Bob Garfield, *The Sell-Out Bowl: And No, We're Not Talking About Ad Inventory*, ADVERTISING AGE, Feb. 6, 2006, at 1.

Knowing this, the swindler must decide whether \$2,000 exceeds the marginal costs of \$600 plus the sanction discounted by the probability of receiving the sanction. Before the rational swindler makes the decision to swindle, she will implicitly determine whether the equation weighs in favor of commission. If it does, she will have to weigh whether the surplus comports with her appetite for risk.

Viewing this equation, the swindler may also find ways to manage certain variables that tip the scale toward commission. She could decide that, instead of targeting older, presumably savvy baby-boomers with knock-offs, she will craft tickets for a hot, sold-out concert that appeals to minors, likely without parental permission to attend such a concert (for example, a Justin Timberlake concert).¹¹⁷ This possibility would lower the (p) variable, assuming that those under eighteen years old are less likely to report that they were defrauded than adults. All else being equal, it would be more appealing to alter the fraud to target different victims who are easier to induce, such as young people. The swindler may also have to weigh the fact that the more vulnerable group may have lower price points.

The swindler may also calculate that she can tip the equation toward commission by changing her distribution system. Her current method—selling the tickets anonymously online—has inherent risks. Even though the sales are theoretically untraceable, there is no way to be sure. Instead, the swindler decides to network and meets a face-to-face distributor for her wares—a street scalper. Fully disclosing the bogus nature of the tickets (again, assume Rolling Stones tickets), she offers them to the fleet-of-foot street scalper for a highly discounted wholesale price of \$250 each. With an opportunity to flip the tickets for \$1,000 each, the street distributor gladly purchases the wholesale inventory with the intent to retail them to unsuspecting concertgoers.

Our swindler has now insulated herself from detection. Her scheme has a lower (p); however, it also has a lower payoff. Again, she can manipulate the equation until she gets a payoff that matches her appetite for risk. Some people are more willing to gamble than others, even when viewing the same set of odds. Policymakers cannot affect the swindler's appetite for risk, but can affect risk per se. It is important to note that, in this particular illustration, the counterfeiter adjusted the value of (p) to reflect different group profiles. The swindler even adjusted the nature of the scheme to manage the value of (p), given the profile of the different groups.

117. Thank you to the editors of the DePaul Law Review for keeping the author current.

2. *The Enterprise Fraud Perpetrator*

Although this Article has mostly discussed fraud commission calculus in the context of individual actors, the fraud commission equation can apply to enterprises of all sizes and degrees of legitimacy. Consumer fraud is not only the province of the lone, one-act scammer, but also the product of entities ranging from multi-national corporations¹¹⁸ to small businesses.¹¹⁹

Broad principal-agent questions surround the issue of how an organization manages a potentially fraudulent practice. (*EV*) for the enterprise represents a measure of shareholder-value creation. (*EV*) could also represent a corporate manager's individual interest in advancing her position in the institution, which may include monetary compensation. It could even be a crude measure of shareholder or partnership interests, even if the partnership is informal or illicit.¹²⁰ Nonetheless, (*EV*) must still exceed the cost side of the equation in order for the actor to commit the fraud.¹²¹

118. Examples of such entities include Enron and the tobacco industry. *See supra* note 87.

119. "Rogue" towing companies sometimes exemplify fraudulent local small businesses. *See* Press Release, Ill. Att'y Gen. Lisa Madigan, Attorney General Madigan Files Lawsuit Against Rogue Towing Companies (Feb. 22, 2007), available at http://www.illinoisattorneygeneral.gov/pressroom/2007_02/20070222.html.

120. For example, several scammers may collude in a Three Card Monte scheme. A New York City tourism website gives visitors the following warning about Three Card Monte:

Whenever a police car passes by, you can observe how quickly these games disperse. Sidewalk card games are both illegal and fraudulent for some very good reasons. Scenario[:] 1. Two or more people are standing around a cardboard box on a busy street trying to win money by choosing the correct card out of the three cards shuffled. 2. You notice that someone seems to be winning; this person is usually working with the dealer to lure people in. People who work these scams know that it will be less suspicious to plant a woman or someone in a business suit in the game. 3. The shuffler will purposely lose the first few rounds to get you to bet more money. 4. At this point, if you take your wallet out, someone may grab it and run—OR—it will be pick pocketed as you watch the game. 5. If by some fluke you win, you may be followed and mugged. How to avoid this[:] The hand is quicker than the eye and these are pros. Don't play—YOU CANNOT WIN!

NY.com, Three Card Monte, <http://www.ny.com/scams/3CardMonty.html> (last visited July 10, 2007).

121. If the operation otherwise operates legitimately, (*EV*) would be discounted by taxes. Illegitimate or underground enterprises have a lower threshold for rational fraud commission and should, not surprisingly, be more likely to commit fraud. While there may be correlation between "underground" business status and willful violation or evasion of regulations, perpetration of consumer fraud can be an entirely separate calculation. Underground business operators face similar economic and risk-based equations when calculating whether to comply with the regulations that drive them underground.

3. *The Policymaker's View of the Consumer Fraud Model*

This subsection returns to the basic model to explore what policymakers can do to alter behavior. Despite having little control over an individual's appetite for risk, policymakers can certainly manipulate other factors within the model. They can even add a few variables to the equation as follows:

$$EV > MC_E + (A)(p)*(B)(S)^{122}$$

In this enhanced equation, (A) represents the measures policymakers can take to enhance the probability of detection and successful prosecution of consumer fraud activity. (B) represents the magnitude of measures that can enhance the sanctions. Together, (A) and (B) are measures of the impact of public policy initiatives. By elevating or diminishing the right (cost) side of the equation, policymakers can affect the ultimate threshold for the decision to initiate fraud. Accordingly, when policymakers examine alternatives, including enhanced protection and shifting the fraud targets, they are examining modifications to (A) and (B) .

If (p) is the base-level state of sanction probability¹²³ for the fraud perpetrator in the absence of a marginal policy, then the product of $(A)(p)$ is the enhanced probability of ultimate sanction. If (S) is the base-level state of sanction magnitude, then the product of $(B)(S)$ is the enhanced sanction magnitude.

a. Increasing the Probability and Magnitude of Sanctions

Bear in mind that, as in the example of the ticket counterfeiter, the skilled fraud perpetrator will take measures to avoid detection. These measures only lower the perpetrator's sanction probability variable, (p) . Here, (A) stands for the magnitude of measures wholly under the control of policymakers. These measures, designed to deter, should be visible to the perpetrator.

The product of $(A)(p)$ is jointly controlled by policymakers and perpetrators. However, it is much easier for policymakers to fiat (A) than it is for perpetrators to wholly navigate, reduce, and achieve certainty around (p) . Essentially, policymakers often use (A) to deter all forms of crime.

122. Note that (p) and (S) are treated as the baseline variables; (A) and (B) represent the "controllable" coefficients.

123. Assume that $(A) = 1$ at this base level state. Public policy measures that reduce the probability of ultimate sanction would set a value of (A) at < 1 . Public policy measures that increase probability would set (A) at > 1 .

The product of $(B)(S)$ is the one item that policymakers wholly control.¹²⁴ Sanction magnitudes are the province of legislation, regulation, and prosecutorial discretion. Although the equation used (B) as a stand-in for the severity of punishment, (S) can stand for the range, shape, nature, and quality of potential punishments. For the aforementioned perpetrator, the threshold for fraud commission will be higher if policymakers enhance the baseline sanction.

These sanctions can take many forms. The nature and quality of (S) are particularly important in deterring behavior across the range of potential perpetrators. This is because individual actors can have different tastes regarding the relative disutility of undergoing shame, civil penalties, and imprisonment. Consider a perpetrator who cleverly funnels her ill-gotten gains into offshore accounts, thereby maintaining few assets. This fraudulent actor will not be deterred if (S) is shaped like a fine or forfeiture penalty. She might be deterred by a stronger (B) , however, such as heavy prison time. Although (B) is not intended to be viewed as a linear, monolithic variable for expanding sanctions, policymakers should view it as a means of enhancing the magnitude of (S) .

Tying this together, the would-be fraud perpetrator seeks situations where (EV) exceeds the enhanced probability of harsher sanctions or where (p) and (MC_E) can be managed downward. Additionally, the potential perpetrator will act with more confidence if she believes that she fully understands the variables and risks. Here, repeat players have an advantage, because they can make better-informed decisions. If there is uncertainty, the potential swindler will apply a discounting factor that would either elevate the expected risks or diminish (EV) , making fraud commission less viable.

Within the model, policies that efficiently increase the threshold for (EV) are the most sought after. Enforcement efforts to increase (A) across the board can be expensive and blunt, as can some efforts to increase (B) through enhanced punishment magnitude.¹²⁵ Moreover, there are natural limits to how many incremental resources policymakers might want to pour into (A) and (B) . At a certain point, the marginal benefit of enhancing (A) or (B) for fraud will diminish until it is lower than the marginal benefit of using those resources for other public purposes. Similarly, the resources used to enhance sanction (B) also have a diminishing return. At the extreme, life sentences for consumer fraud would certainly consume an exorbitant amount of re-

124. The one item that perpetrators entirely control and manage is (MC_E) .

125. This includes broadening the range of fraudulent acts subject to imprisonment, lengthening imprisonment, withdrawing licensures, or extending fines.

sources.¹²⁶ In sum, reallocation of resources to enhance (A) and (B) should reduce fraud incidence, but policymakers should not allocate resources beyond the point where it is more sensible to utilize them elsewhere.

The same equation and considerations apply whether policymakers are attempting to address the individual or the enterprise fraud perpetrator. The same tools for addressing fraud can be used to impact both the swindler and the multinational corporation. Despite some structural differences between the individual and enterprise perpetrator, the underlying risk equation remains the same. If policymakers increase (A) and (B), they will still raise the expected marginal cost (MC) and, therefore, raise the threshold for fraud commission. Perceived probabilities of detection should influence the rational “bad man” or the collective “bad men” that comprise the fraud-seeking enterprise.¹²⁷ Policymakers still confront the individual actor’s appetite for risk when (EV) exceeds the threshold. Thus, policymakers are compelled to return to seeking means of minimizing (EV) for the individual, hoping that, when risk-adjusted, the collaborative act will be less likely to occur.

4. *Seeking Policy Solutions in Light of the Perpetration Model*

As previously noted, blunt, obvious, across-the-board solutions to the fraud problem may prove directly effective, but are expensive and may be inefficient in a limited resource environment. Policymakers do have more finely tuned options at their disposal. These options enable policymakers to both change the equation and raise the fraud commission threshold for actors, individuals, and aggregate enterprises alike. Although they are still working with the same tools—(A) and (B)—policymakers can increase these variables selectively and strategically, while creating a greater impact.

C. *Putting the Fraud Perpetration Equation to Work*

How can policymakers alter the behavior of fraud perpetrators most efficiently and cost-effectively? Section III.A took the position that they can alter the behavior of the fraud perpetrator, because that particular brand of actor is rational.¹²⁸ This Section contends that, by

126. Further, scholars should adhere to the principles of the theory of marginal deterrence: “[T]he law should be designed to discourage criminals from committing more serious offenses.” Robert A. Mikos, “Eggshell” Victims, Private Precautions, and the Societal Benefits of Shifting Crime, 105 MICH. L. REV. 307, 341 n.122 (2006).

127. See generally Holmes, *The Path of the Law*, *supra* note 104.

128. See *supra* notes 91–104 and accompanying text.

applying a basic microeconomic approach and relying on rational-choice theory, policymakers can modify the behavior expected from individuals, discounting the outliers.

Although individuals do not behave rationally at all times (and although criminal actors may have psychological income motives beyond (*EV*)),¹²⁹ policymakers can assume that changes in incentives and punishments will yield a change in results.¹³⁰ With that in mind, they must look for ways to examine the fraud equations derived above while attempting to reduce the overall incidence of fraud in the economy.

This Section first examines the impact of focusing on hyper-protection and shifting the fraud victimhood burden from a vulnerable group to a less vulnerable population. Simultaneously, this Section explores the potential deterrent impact of hyper-protecting a group that stealthily permeates the broader economy. Ultimately, by using the existing diffuse enforcement infrastructure described above, this Article tests the logic that a group protection approach provides a solution to a thorny problem.

1. Contextualizing the Law and Economics View on Victim-Shifting

In the basic law and economics model, Cooter and Ulen argued that unilateral precautions against crime are socially inefficient, because they merely shift victimhood from one individual to another.¹³¹ For example, if Neighbor A puts a visible alarm on his automobile and Neighbor B has no alarm, the rational criminal—assuming that the bounty is the same—will simply steal the car from Neighbor B. In the absence of the precaution, the probability of victimization would have been equal for both neighbors. The net amount of criminal activity is not reduced, and, as a matter of overall efficiency, the cost of the precaution is an unmitigated loss. Under this model, society is left poorer through resource misallocation.

Policymakers can apply Cooter and Ulen's approach in the fraud context. If policymakers visibly protect one group, fraud would merely shift to another group. The visible protections (for example, education or enforcement initiatives) would serve the same purpose as the visible car alarm. Cooter and Ulen's basic model, however, does not account for certain nuances related to the differences among groups (and the value inherent in shifting victimhood under certain

129. See generally BABIAK & HARE, *supra* note 114.

130. See COOTER & ULEN, *supra* note 92, at 413–15, 417.

131. *Id.* at 476.

circumstances), nor does it account for the effectiveness of invisible protections. Below, this Article accounts for these nuances.

a. Some Groups have Greater Protection Needs

A new critique of the basic Cooter and Ulen analysis, to which this Article will return in Part IV, holds that their model is flawed, because it treats all victims as similarly situated.¹³² This Article contends that an individual of lesser means absorbs a more substantial loss of marginal utility when his automobile is burglarized for \$1,000 than when a wealthy individual experiences the same. If the goal is maximizing social utility and efficiency, then the aforementioned equation has acquired new variables. Perhaps if the poorer individual takes the car alarm precaution, the general utility gain will exceed the loss of the precaution. Thus, there is an argument for shifting crime to different victims. As policymakers look toward protecting groups, they should consider that some groups may be inherently more valuable (morally and economically) for society to protect than other groups.¹³³

b. Policymakers Can Shift Perpetrators From Easy Targets Toward Harder Targets

Another detour from the basic model argues that there is value in compelling fraud perpetrators to shift away from easy target groups and toward harder target groups. That is, if perpetrators are deterred from targeting a hyper-protected group, they may target groups that are better able to protect themselves and are more likely to detect and report fraud. This shift would not only protect the larger group, but would also reduce the overall incidence of fraud.

In other words, if policymakers hyper-protect a vulnerable group, fraud perpetrators will forsake targeting that group to seek out new, comparatively attractive targets. The perpetrator faces a higher (*A*) and (*B*) for the vulnerable group, but is left with the less attractive option of targeting a general population with a higher (*p*) than the vulnerable group. Thus, perpetrators will commit less fraud if society shifts them away from the vulnerable target.

132. See generally Mikos, *supra* note 126.

133. See JOHN RAWLS, A THEORY OF JUSTICE (1971). Specifically, this Article refers to Rawls's "Second Principle of Justice," which argues that socioeconomic inequality should be arranged to be of "the greatest benefit [to] the least advantaged" members of society. *Id.* at 302. This Article does not ignore this principle, but rather holds it secondary to the larger goal of reducing consumer fraud at large. The distributive justice implications for this approach are significant and they are not fully addressed here.

In the realm of deception and unfair trade practices, perpetrators produce offerings that sophisticated consumers may recognize and avoid, while unsophisticated consumers may not. If aggrieved, sophisticated consumers may be in a superior position to report fraud. Thus, they would not only enable the authorities to enjoin the practice, but would also keep the authorities aware of cutting-edge nefarious practices.¹³⁴

It is possible that fraud perpetrators would merely shift activity from the hyper-protected vulnerable group toward the next unprotected vulnerable group. This assumes, however, that perpetrators have skills that can translate to other target groups. It is unlikely that all perpetrators have that ability.

c. Members of a Hyper-Protected Group Lurk in the General Population

Further, when an externally identifiable vulnerable group—such as single women over sixty-five—is hyper-protected, the fraud equation for that group should change. Assume that policymakers increased (*A*) by educating this group about scams and where to report them and increased (*B*) by adding significant jail time for scams that victimize someone in this class. The fraud commission threshold for scams directly targeting women in this age group would rise dramatically.

But if the legal construct is artfully designed, there would be a secondary effect. Fraud perpetrators would have to worry that a scam targeting the elderly as a whole, women between the ages of forty and sixty-five, or even at the public at large would incidentally sweep up a hyper-protected victim. Thus, while (*B*) is increased directly for the scammer targeting women over the age of sixty-five, (*B*) is also increased for the scammer targeting adjacent groups and even the general population. Hyper-protection of one group should have cascading protective effects—positive externalities—throughout the entire economy.

134. For examples of such practices in the credit card industry, see Press Release, Comptroller of the Currency, OCC Alerts National Banks on Unacceptable Credit Card Marketing and Account Management Practices (Sept. 14, 2004), available at http://www.occ.treas.gov/toolkit/news_release.aspx?Doc=LHMID9OG.xml; and Wayne Jekot, *Over The Limit: The Case for Increased Regulation of Credit Cards for College Students*, 5 CONN. PUB. INT. L.J. 109 (2005) (illustrating that college students are uniquely unsophisticated about credit). Thank you to Ronald Mann for directing the author to an industry example with which he is very familiar.

d. The Impact of Invisible Group Hyper-Protection

Finally, policymakers can revisit the first model (the Cooter and Ulen model) with a different approach. Perhaps there is a way that policymakers can protect a group of consumers with a concealed hyper-protection approach and, in the course of hyper-protecting this concealed group, deter consumer fraud across the board. This is analogous to the “LoJack” concept, which is described in the next subsection.

i. The LoJack concept

In 1998, Ian Ayres and Steven Levitt published an extensive and widely cited empirical study on the effectiveness of LoJack in reducing automobile theft.¹³⁵ LoJack is a concealed security system that enables authorities to track individual stolen vehicles.¹³⁶ Although LoJack may ultimately help the authorities recover an individual’s stolen vehicle, it does nothing to directly deter the initial act of theft because of its concealed nature.¹³⁷ Ayres and Levitt also noted that “the most important effect of LoJack” was disruption of physical chop-shop operations and the auto theft industry structure.¹³⁸

The Lojack study concluded that increases in vehicles equipped with LoJack were “associated with substantial declines in auto theft, without any evidence of increases in other crime categories.”¹³⁹ The LoJack effect proved strikingly different from the original hypothetical in this Article—a simple, but visible, car alarm that merely shifted victimization, while incurring a social cost. Ayres and Levitt calculated that “the estimated marginal social benefit of LoJack installation [was] roughly fifteen times greater than the marginal social cost.”¹⁴⁰ Most importantly, they concluded that “LoJack appear[ed] to be one

135. Ayres & Levitt, *supra* note 13.

136. The LoJack website states:

The patented LoJack System includes a small radio frequency transceiver hidden in up to 20 places in a . . . vehicle. Each LoJack System has a unique code that is tied into the Vehicle Identification Number (VIN). When a theft is reported to the police, a routine entry into the state police crime computer results in a match of the LoJack System’s unique code against the state VIN database. This automatically activates the LoJack System in your car, which emits an inaudible signal. Law enforcement authorities who are equipped with LoJack vehicle tracking units—in their police cruisers and aviation units—are always listening for a LoJack signal. Police use the LoJack vehicle tracking units to track and recover your LoJack equipped vehicle.

LoJack.com, What is LoJack?, <http://www.LoJack.com/what/index.cfm> (last visited July 10, 2007).

137. Ayres & Levitt, *supra* note 13, at 44–45.

138. *Id.* at 60.

139. *Id.* at 74–75.

140. *Id.* at 75.

of the most cost-effective crime reduction approaches documented in the literature."¹⁴¹

An illustration is useful. Assume that a perpetrator knows that LoJack was installed in one of two automobiles, but is unsure which. The putative thief may decide to attempt to steal either automobile, but the risk equation has changed for both—even the automobile without LoJack.¹⁴² Thus, even though only one individual in our two-individual model has taken a precaution, the overall incentive to commit crime drops due to an exogenous increase in (*A*).¹⁴³ Ultimately, both vehicles benefit from LoJack: the impact of the crime may be diminished to the installer of LoJack (as the vehicle may indeed be recovered), and the non-installer benefits from the probability of its installation.¹⁴⁴

ii. Application of the LoJack concept to consumer fraud

In the consumer protection context, how can the public create a device as effective as LoJack?¹⁴⁵ LoJack created a stealth group of car owners who were more likely to report automobile theft and a technology more likely to detect theft and expose chop shops.¹⁴⁶ Although the auto theft sanction was left unchanged, the threshold for commission of auto theft was dramatically enhanced. The question is whether policymakers can establish a proper mechanism to create a stealth group of consumers, randomly distributed throughout the economy. No fraud perpetrator would want to ensnare these stealth consumers in her net, because they would be more likely to report (like the LoJack owners) and more likely to be equipped with the tools, resources, and education to lead authorities into consumer fraud

141. *Id.*

142. Some activists favoring less-restrictive gun laws advocate this position. See, e.g., JOHN R. LOTT, JR., *MORE GUNS, LESS CRIME: UNDERSTANDING CRIME AND GUN-CONTROL LAWS* (1998) (arguing that concealment of firearms produces a deterrent effect). *Contra* Ian Ayres & John J. Donahue III, *Shooting Down the "More Guns, Less Crime" Hypothesis*, 55 *STAN. L. REV.* 1193 (2003) (arguing the opposite). A debate on the merits of gun control arguments, however, is beyond the scope of this Article.

143. Ayres & Levitt, *supra* note 13, at 44.

144. *Id.*

145. This Article contends that it is possible to create an effective legal device in the consumer protection context that relies on the same principles as LoJack, bearing in mind that not every principle carries over to consumer protection and that a similarly astronomical social benefit would be challenging to achieve.

146. *Id.* at 60. Ayres and Levitt noted that auto thieves cleverly adjusted their techniques by quickly abandoning cars after the initial theft, observing them for a period of time to see if LoJack picked them up, and then bringing them into the chop shop. *Id.* at 61. However, further evasive action still raises the cost of committing the auto theft.

“chop shops” (dens of fraud networks or enterprises).¹⁴⁷ In this proposal, these consumers would be more dangerous to engage, because the sanction’s magnitude (*B*) associated with defrauding them would be dramatically greater.

By drastically increasing (*A*) and (*B*) for a randomly distributed, hidden group of consumers,¹⁴⁸ policymakers can significantly raise the threshold for fraud commission without dramatic expense. For example, if policymakers randomly selected one in every fifty adults for special, hidden protection in the form of severe sanctions for an offense against a class member with twice the risk of prosecution, there would be three results: (1) (*B*) should increase; (2) the level of deterrence should rise throughout the economy; and (3) the level of fraud incidence should drop.

If agencies educate this random group about consumer fraud, (*A*) would also increase. The education could focus on understanding hyper-protection status, what activities fall into the category of consumer fraud, and how to maximize information about the perpetrating entity. Agencies could educate through various forms, such as mailings or a secure web delivery system.¹⁴⁹

Agencies could create additional mechanisms for this group. Policymakers could provide the group with whistleblower incentives and create a simpler interface for a streamlined consumer fraud reporting mechanism, such as a unified complaint window that coordinates investigation and enforcement. Further, if organized schemes exist, like a Nigerian 411 scam¹⁵⁰ or identity theft ring,¹⁵¹ these consumers can help lead authorities into the den of thieves. All of these educational mechanisms would further increase (*A*) and transform these consumers into the functional equivalent of high-reporting LoJack consumers.

147. For one illustration, see the identity theft ring described by Robert McMillan, *Six Charged in Case of AOL Identity Theft Ring*, *COMPUTERWORLD* (Sept. 27, 2006), available at <http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9003691>. One entrant into such a den can break up a consumer fraud chop shop like this one.

148. Lawmakers could allay Equal Protection concerns by ensuring that the adults are given status by purely random means for terms of varying, but limited, duration. Further, no class of individuals would be put at a formal disadvantage and the state interest would be quite strong. Also, lawmakers could avoid any Eighth Amendment concerns about disparate punishments for the same essential offense through careful definition of fraud against a protected individual as an entirely different crime.

149. It would, of course, depend on the consumer’s education and preferred means of education delivery, as well as her appetite for participation.

150. See FTC Consumer Alert, *supra* note 8.

151. See McMillan, *supra* note 147.

2. *Embracing and Enhancing Victim-Shifting and Group Protection*

Returning to the original guiding premises for improving consumer protection, there are three perspectives to consider, each of which presents an opportunity to unlock powerful incentives and a chance to landmine the consumer protection field with invisible deterrents. The first perspective is that of the perpetrator, be it a lone swindler in a room with a phone and a bare light bulb or a multinational corporation. The second perspective is that of the individual consumer or the potential victim. The third perspective is that of the consumer group, whether that group is elderly men, low-income car buyers vulnerable to predatory lending, non-English speakers who are afraid to report crime to authorities, or even status-seeking, wealthy socialites.¹⁵²

a. The Perpetrator Perspective

As explored above, raising the detection and prosecution probability (*A*) and dramatically enhancing the sanction's magnitude (*B*) for a specific group creates a bifurcation in the pool of victims from the perpetrator's perspective. For a fraudulent act to be worth initiating, the perpetrator must view the (*EV*) for the protected group as much higher than it was prior to protection. Further, if the perpetrator is forced to commit fraud outside of the target group, she is beyond her usual expertise and, thus, less certain about (*EV*). This also means that she is less certain about (*p*) and the consequences that follow.

For the perpetrator who was not targeting the specific group, the perspective changes as well. If the perpetrator had planned a broadly targeted scheme, the possibility of accidentally victimizing a hyper-protected individual raises the potential magnitude of the sanction (*B*), thus making the perpetrator's threshold for fraud commission higher. If the group is invisible, it has the same effect on the perpetrator.

To review, from the rational perpetrator's perspective, hyper-protection of a visible or invisible group would raise the threshold for

152. Even the wealthy are vulnerable to fraud. They are perhaps especially vulnerable to certain types of fraud—and (*EV*) is high when the victims have money. See, e.g., Alan Feuer & Charlie LeDuff, *Con Man of the Hamptons, In His Own Words*, N.Y. TIMES, Nov. 4, 2000, at B3. A swindler by the name of Christopher Rocancourt spent a summer posing as a member of the Rockefeller clan. *Id.* Through various schemes, he scored nearly \$1 million from his targets. *Id.* Rocancourt stated, "I would not consider myself a criminal—I steal with my mind. . . . If I take things, if that is your definition of a criminal, then I am a criminal." *Id.* The literate and sophisticated are vulnerable to fraud as well. See *Fed. Trade Comm'n v. Standard Educ. Soc'y*, 302 U.S. 112, 117 (1937) (describing how "teachers, doctors, college professors, club women, [and] business men" were all taken in by deceptive encyclopedia sales practices).

fraud commission almost across the board. Deterred fraud has two primary social benefits: the unlawful, inefficient transaction does not occur, and there is no marginal cost of enforcement and punishment.

b. The Consumer Perspective

Policymakers should examine both sides of the transaction to ensure that group protection works. If they rearrange the basic transactional equation from the consumer perspective, they will find that consumers are also seeking an extracted value (EV_C) from the transaction. The consumer will engage in the transaction if the expected value is greater than or equal to the costs. Revisiting Akerlof's work, the consumer has expectations about quality and risk that factor into the price that she is willing to pay.¹⁵³ This subsection examines the power of the consumer in light of the group protection approach—specifically, from the standpoint that consumers will face different values in the variables of their transaction equation, depending on the circumstance.

The basic economic decision function for fraud-evading consumers is as follows:

$$EV_C > QL * RK$$

In this equation, (QL) represents the consumer's quality expectation for goods, services, or opportunities offered. (RK) represents the risk that fraud (or any unknown factor) will negatively impact the quality of those goods, services, or opportunities.¹⁵⁴ Ultimately, nearly every routine transaction and wild scheme can be viewed through the lens of this simple equation. Start with Akerlof's Nobel Prize-winning theory of used automobiles. Sometimes used cars will not sell, because the consumer without mechanical inclinations places a high value on (RK). The consumer who understands mechanics will have more certainty around (RK) and more confidence about the proper price. Thus, she is less likely to wind up with a lemon than the less-informed consumer with a poor understanding of (RK).¹⁵⁵

From the consumer perspective, education is a key instrument for affecting (RK) and ensuring that only legitimate transactions occur. Educating a group or providing them with resources for complaints makes them harder targets. Not only will they understand and cor-

153. Akerlof, *supra* note 5, at 488.

154. (RK) will always have some value, as no transaction is truly risk-free.

155. An entire cottage industry has emerged to address (RK) in the used automobile sector. See Carfax.com, Vehicle History Reports, <http://www.carfax.com> (last visited July 10, 2007). See also Jeanne Wright, *Unlocking the Secrets of Your Car's Past*, L.A. TIMES, Nov. 28, 2001, at G1.

rectly value (*RK*), but they will also be more likely to report a scammer. The latter point is especially powerful: policymakers should filter the fraud perpetrators toward individual consumers who are able to accurately assess (*RK*). These educated consumers are able to disengage from the transaction or report the scam to the authorities.¹⁵⁶

To illustrate, there are innumerable ways in which policymakers can engage the consumer perspective and decrease (*RK*). If the consumer is aware of severe penalties for fraud perpetration, her (*RK*) is decreased. For example, if auto repair shops were threatened with permanent closure for first-offense fraudulent activities, consumers aware of such a sanction would have severely decreased (*RK*), because they would assume that auto repair shops are legitimate. Increased consumer education can also reduce (*RK*). Most importantly, putting a consumer in a protected group should reduce (*RK*) for that group and ultimately for the public at large, once the incidence of fraud diminishes.

Further, if policymakers provide hyper-protected consumers more effective and direct means for civil cost recovery, policymakers can use the consumer perspective and incentive structure to significantly enhance the group protection approach. This proves true whether individuals receive the recovery through prosecuting agencies or enhanced damages. The group approach engages the individual consumer, and the individual consumer's perspective can reinforce the group approach.

c. The Group Perspective

Below, Part IV selects a specific, hyper-protected group for purposes of illustration.¹⁵⁷ It is helpful, however, to first delineate the criteria used to select that group. The selected group should be especially vulnerable. That vulnerability could be economic or it could relate to the group's reticence to report fraud. It should be a group that would benefit the most from protection.¹⁵⁸ The group must also be

156. Education schemes should be artfully targeted and designed in the spirit of the "Best Practices" approach, as applied to anti-tobacco education for youth. See Colleen E. Medill, *Transforming the Role of the Social Security Administration*, 92 CORNELL L. REV. 323, 350–54 (2007). Thank you to Susan Morse for directing me to this example.

157. See *infra* notes 163–201 and accompanying text.

158. One could argue that protecting the public from big-ticket scams that target individuals with more money would maximize net utility because of the sheer size of the fraud involved. Alternatively, one could argue that protection of consumers with lower-income from smaller scams would maximize net utility, because the marginal loss from a scam is more significant to the lower-income individual. Again, this is a question of distributive justice. See RAWLS, *supra* note 133.

readily identifiable to policymakers and law enforcement. Finally, the group must have clearly definable features—the more easily definable, the more efficient the enforcement.

There are numerous examples of this type of definitional protection in criminal law. For example, crimes against the elderly will occasionally carry an extra sanction.¹⁵⁹ The same holds true for crimes against law enforcement officials. Members of Congress are also a protected class. A random assault on a law professor eating a hot dog in Central Park is a state offense.¹⁶⁰ However, a random assault on a member-elect of Congress eating a hot dog in Central Park is a federal offense.¹⁶¹

The group must be easily identifiable, large enough to be significant, and broadly distributed throughout the general population. If policymakers provide hyper-protection to members of the group, they want them to serve, to some degree, as an invisible deterrent. That is, they want consumers embedded broadly within the population to serve as highly undesirable targets for the potential fraud perpetrator in a wide number of circumstances.

Policymakers must be mindful of resources, however, if they want group protection to be credible. For example, protecting the entire fifty-and-over populations through a dramatic increase in (*B*) would be incredibly costly and difficult to enforce evenly. Thus, at some point, the exception swallows the proverbial whole.

Addressing the group perspective requires a unique understanding of the group's characteristics. What makes a group vulnerable? To what types of schemes does a group fall prey? Answering these questions enables the group not only to receive customized, external protection through a surge in (*B*), but also to receive less-expensive, customized outreach and education that increases (*A*). Here, by impacting (*A*) through the lens of the group, policymakers make both the group and the individual members of the group floating throughout the economy more dangerous targets for scammers and swindlers.

Selecting the proper group is critical, and understanding that group's perspective is necessary. Protecting the group requires a strong understanding of its perspective and the scammer's perception of that group's perspective. If the group selected for primary protection is fabricated (for example, a randomly-selected group), the insti-

159. See 18 U.S.C. § 2326 (2000).

160. See N.Y. PENAL LAW § 120.10 (McKinney 2004). Perhaps Congress should revisit the issue of law professor protection.

161. See 18 U.S.C. § 351 (2000) (elevating assault, kidnapping, and other crimes against members of Congress and members-elect to a federal offense).

tutional framework that supports protection will be critical. Put simply, for the systemic approach to work, policymakers must address the selected group's perspective.

3. *Projecting the Impact*

Having assessed the group's perspectives, this subsection briefly assesses the potential impact from selecting the right groups for hyperprotection. Returning to the fraud equation, increasing (*A*) by expanding the size of the federal and state enforcement regimes across the board would be quite expensive. Incremental and generalized education outreach programs would fall into the same category. Ultimately, expanding (*A*) through the detection system and the nature and shape of (*B*)¹⁶² across the board would have a proportionate deterrent effect, but could potentially over-allocate resources to the problem.

Instead, if policymakers concentrate their resources on one group, consumers will benefit from the cascading effect of deterrence. Fraud becomes a more difficult game when a vulnerable group is either taken out of the equation or distributed throughout the population. Perpetrators are forced to take their acts to unfamiliar territories and to consumers with a better understanding of how to report—or, at least a higher likelihood of doing so. If policymakers further concentrate their resources on administering a plan to protect a randomly selected, concealed group of consumers, they can focus their education and enforcement efforts on that smaller group. If the sanctions are severe enough, the general level of deterrence should soar.

IV. WHOM TO PROTECT?

In this Part, Section A explores the challenges of setting criteria for group selection,¹⁶³ and Section B applies those criteria to the available data.¹⁶⁴ Section C revisits the establishment of a randomly selected group (with the invisible deterrent) within this context.¹⁶⁵ Finally, Section D explores the power of combining these two approaches.¹⁶⁶

162. In 2004, the annual cost of federal imprisonment in 2004 was \$23,000. *Costs of Incarceration and Supervision*, 36 THE THIRD BRANCH 5 (May 2004), <http://www.uscourts.gov/ttb/may04/ttb/costs/index.html>.

163. See *infra* notes 167–168 and accompanying text.

164. See *infra* notes 169–194 and accompanying text.

165. See *infra* notes 195–200 and accompanying text.

166. See *infra* note 201 and accompanying text.

A. *The Criteria for the Defined Group*

In order for hyper-protection to be efficient, the group must not be so large that it swallows the whole. The group should, however, have a membership that circulates throughout the population so that scammers would fear accidentally ensnaring them in a scheme. The group should be truly vulnerable; members should be easier to deceive or strong-arm, less likely to know that they have been defrauded, and less likely to report fraud. If policymakers want to deter fraud, they need to go to the location of the fraud.

Finally, the group should be comprised of individuals that we normatively deem socially worthy of extra protection.¹⁶⁷ This part of the group selection process, however, should be wholly confined to a choice within the identified set of groups. Political considerations may enter at this phase, but policymakers should view such considerations with some concern. Interested parties will clamor for the broadest protections possible for their constituencies, which may have a bearing on efficiency and effectiveness. This Article assumes that, if the group is properly selected, notions of distributive justice should be applied.¹⁶⁸ But, again, such notions should be secondary to the goals of minimizing fraud incidence and maximizing utility for the whole.

B. *Selecting the Defined Group*

When thinking about definability, ethnicity, gender, and age are readily recognizable places to draw lines.¹⁶⁹ Which group or cross-section of these groups would be most vulnerable and least likely to report crime? In 2004, the FTC conducted an extensive survey to determine who was most likely to be victimized by fraud and who was most likely to complain about fraud.¹⁷⁰ This survey provided “the first systematic look in the last decade at the problem of consumer fraud.”¹⁷¹ The data provide some basis for drawing conclusions about victimization and the likelihood of consumer reporting by group.¹⁷²

167. See generally Mikos, *supra* note 126.

168. See RAWLS, *supra* note 133, at 303.

169. Also, such definitions and divisions of these groups have been put to use by both the U.S. Census and the FTC.

170. KEITH B. ANDERSON, CONSUMER FRAUD IN THE UNITED STATES: AN FTC SURVEY ES-1 (2004), available at <http://www.ftc.gov/reports/consumerfraud/040805confraudrpt.pdf>.

171. *Id.* at 115.

172. Decision theorists have performed a considerable amount of research illustrating differences in rational behavior by group, and policymakers can also draw upon this data. For a survey of such studies, see Gregory Mitchell, *Why Law and Economics' Perfect Rationality Should not be Traded for Behavioral Law and Economics' Equal Incompetence*, 91 GEO. L.J. 67, 139–60 (summarizing research on the differences in rational behavior by sex, cognitive disposition, cul-

1. *Victimization by Group*

According to the survey, among racial and ethnic minorities, the population most victimized by consumer fraud is, by far, Native Americans and Alaskan Natives.¹⁷³ Over 33% of this group had been victims of fraud in the year prior to the survey.¹⁷⁴ African Americans were next at 17.1%, followed by Hispanics at 14.3%. Over 6% of non-Hispanic whites were victimized.¹⁷⁵ Although Native Americans and Alaska Natives are certainly worthy of protection (especially given how far they seem to stand out from other groups), their population distribution may be too geographically concentrated. In other words, they may not circulate broadly enough in the population to meet this plan's needs.

Curiously, despite the above-mentioned SCAMS Act's mission,¹⁷⁶ the elderly do not appear to be the group in need of the most protection.¹⁷⁷ In fact, only 4.7% of the population over the age of sixty-five reported to the FTC that they had experienced fraud in the past year.¹⁷⁸ In comparison, individuals between the ages of twenty-five and forty-four were victimized at over twice the rate of those over age sixty-five, with 11.1% of the group reporting a fraud encounter in this survey.¹⁷⁹ Accordingly, it is important to look at victimization in conjunction with propensity to complain in order to select the appropriate group.

2. *Propensity to Complain by Group*

Several noteworthy points emerge when examining which groups are most likely to complain. Overall, when consumers complained, 53.7% of the time they complained to the seller or manufacturer and 18.6% of the time to their credit card company.¹⁸⁰ Only 8.4% of con-

tural background, and developmental differences). While this Article argues that consumer groups should, in part, be chosen for protection by certain very distinguishable behavioral differences, it argues for a generalist approach toward deterrence of fraud and unfair and deceptive trade practices. Policymakers can broadly enhance deterrence with blunter tools. Choosing the right micro-groups for protection to enhance that deterrence requires a keen understanding of the group's attributes. The two approaches can reside under the same roof, according to Mitchell's main argument.

173. ANDERSON, *supra* note 170, at ES-4.

174. *Id.*

175. *Id.*

176. The SCAMS Act may have had some limited effect on telemarketing.

177. It is difficult to know whether this population is less likely to admit that they have been defrauded, but the differential between this group and the younger group is substantial.

178. ANDERSON, *supra* note 170, at ES-6.

179. *Id.*

180. *Id.*

sumers complained to an official source—"a local, state, or federal government agency or better business bureau."¹⁸¹ This has practical implications. Is official source reporting low because of actual resolution from these sources? Is official source reporting low because of the enforcement diffusion and confusion described earlier? Is official source reporting low, because consumers lack education? As policy-makers select a group, they must consider whether the interface between the official source and the consumer is adequate. In the universe of those who complain, women are more likely to complain "when they believed they had been defrauded."¹⁸² While 74.5% of women complained, the complaint rate for men was 10% lower.¹⁸³

Younger consumers are also more likely to complain. Only 55.4% of consumers between the ages of fifty-five and sixty-four complained of fraud, while 75% of consumers below the age of thirty-five complained.¹⁸⁴ The survey made several other important findings: (1) those with more education are more likely to complain than those with less; (2) those with higher incomes are more likely to complain than those with lower incomes; and (3) people who pay with credit cards are more likely to complain than those who pay with money orders.¹⁸⁵

Regarding racial and ethnic classification,¹⁸⁶ African Americans were least likely to complain, at a rate of 55.7%, followed by Native Americans or Alaska Natives at 64.7%. Somewhat surprisingly, 70.8% of Hispanics complained, a rate nearly equal to that of non-Hispanic whites (72.1%).¹⁸⁷ This is inapposite to the findings of the October 2004 Law Enforcement Workshop and Hispanic Outreach forum, which concluded, "Hispanics may *under-report fraud* due to cultural issues or fear of reporting."¹⁸⁸ This survey leaves policymakers with a clearer picture of who feels empowered to complain about fraud and who does not. They should use the power of complaining

181. *Id.* at ES-6-7.

182. *Id.* at ES-7.

183. *Id.*

184. ANDERSON, *supra* note 170, at ES-7.

185. *Id.* at 86-87.

186. The constitutionality of such a race-based or ethnicity-based approach is a subject beyond the scope of this Article. If necessary or more effective, other classifications can be devised to achieve the desired result. Simple emphasis on education and outreach to these groups would not be suspect. Note that the groups selected in this Article are driven mostly by FTC data collection around defined groups. More data could be collected to identify less constitutionally challenging groups.

187. ANDERSON, *supra* note 170, at 87. However, the reporting levels of unauthorized Hispanic aliens is unaddressed in the survey. See Kittrick, *supra* note 67.

188. HISPANIC OUTREACH FORUM, *supra* note 66, at iii (emphasis in original).

consumers by shifting the fraud target away from those who remain quiet to those who do not.

3. *Selecting the Best Group with an Externally Identifiable Constituency*

Whatever its characteristics, policymakers should protect a vulnerable, broadly distributed group. Native Americans and Alaskan Natives are the most likely to be defrauded.¹⁸⁹ But the group is too small (between 0.8% and 1.5% of the 2000 population)¹⁹⁰ and too geographically concentrated (nearly 36% of the group population lives in American Indian reservations or Alaska Native villages)¹⁹¹ to serve this plan's overarching purposes. The small size and limited geographic reach of this population would prevent it from serving as the best candidate for spreading deterrence.¹⁹²

Similarly, women are more likely to complain than men. Do policymakers want to shift fraud away from men? African Americans report that they have been defrauded at a higher rate, but are less likely to report fraud. Would African American men be an appropriate group? Would African American men between the ages of twenty-five and forty-four? Would African Americans below a certain income level? Would these groups be appropriately geographically dispersed? Would income level categorization be clear enough for law enforcement to readily recognize? For example, would an individual claiming poverty level status have to report a crime with their tax return or pay stubs in hand, or even their children's birth certificates? Would that dampen the effect of the program?

These are the types of questions that policymakers should wrestle with in their decision to select such a group, albeit with inevitable clamoring for protected status from special interest groups. The group ultimately selected does not matter, however, if the desired effect can be created. Here, if policymakers selected African American males living below the poverty line, they would have a group of approximately four million individuals.¹⁹³

189. See *supra* note 173 and accompanying text.

190. STELLA U. OGUNWOLE, *WE THE PEOPLE: AMERICAN INDIANS AND ALASKA NATIVES IN THE UNITED STATES, CENSUS 2000 SPECIAL REPORTS 2* (2006), available at <http://www.census.gov/population/www/socdemo/race/censr-28.pdf>.

191. *Id.* at 14.

192. This is not to say, however, that the Bureau of Indian Affairs (BIA) and the FTC should not make this enforcement effort a priority.

193. There are nearly 16.8 million African American males in the United States. U.S. CENSUS BUREAU, *THE BLACK POPULATION IN THE UNITED STATES: MARCH 2004, POPULATION BY REGION, SEX, RACE AND HISPANIC ORIGIN, WITH PERCENT DISTRIBUTION BY RACE AND*

Policymakers should be concerned with regional distribution (54% of African Americans live in the South).¹⁹⁴ Nonetheless, if agencies hyper-protected this group by elevating (*B*), educating them (elevating (*A*)), and providing group members with one, unified complaint window for routing fraud complaints and incentives for the consumer to report through enhanced civil recovery, they might see a significant impact on the consumer landscape.

In response, scammers would shift toward targeting women, non-African Americans, or those above the poverty line, all of whom are more likely to report and may be more able to absorb fraud. Further, those scammers who operate from a distance or engage in mass corporate fraud would regret ensnaring the hyper-protected, super-educated members of this group. This would enhance deterrence and make fraud commission more difficult. In other words, the (*EV*) threshold would be much higher.

Even if policymakers carefully chose one of these groups, there would always be a way for some scammers to avoid the group (possibly through visible or demographic characteristics) or to fashion scams for other groups. That is why selection of a group with an externally identifiable consistency should be combined with constructing a permanent, hyper-protected, randomly selected group of consumers.

C. *Creating a Randomly Selected Group*

Choosing an externally identifiable group can be effective, but is certainly not a panacea. As the concept of novel fraud¹⁹⁵ indicates, fraud perpetrators are innovative and may find means to circumvent groups with visible characteristics. This is where a LoJack-type initiative may be helpful. Instead of simply protecting an identifiable, avoidable group, policymakers could create a random, hidden group to protect as well. The size of the group must be small enough to be affordable with regards to education and maintenance. The size would also need to be manageable enough that the enhanced punishments associated with tampering with this random group would not become cost-prohibitive.

HISPANIC ORIGIN, <http://www.census.gov/population/socdemo/race/black/ppl-186/tab20.pdf> [hereinafter THE BLACK POPULATION STATISTICS]. Of this population, 24.5% are living below the poverty line—giving us a rough estimate of four million in our protected group. U.S. CENSUS BUREAU, THE BLACK POPULATION IN THE UNITED STATES: MARCH 2004, POVERTY STATUS OF FAMILIES IN 2003 BY TYPE, FOR BLACK ALONE AND WHITE ALONE, NOT HISPANIC FAMILIES: MARCH 2004, <http://www.census.gov/population/socdemo/race/black/ppl-186/tab17.pdf>.

194. U.S. CENSUS BUREAU, THE BLACK POPULATION STATISTICS, *supra* note 193.

195. See generally Buell, *supra* note 10.

Policymakers could choose consumers through a random selection mechanism. These consumers would be granted access to an all-purpose complaint window, like a toll free number. They would receive special education through the mail or by other means. In addition to receiving protection through enhanced (B), policymakers might choose to give them personal incentives to be activists within the system. Additionally, policymakers could initiate a massive public education initiative about random protective status to change the behavior of the lone scammer and major fraudulent enterprises repeatedly interfacing with the public.

Just as the putative automobile thief was unable to detect whether an automobile had LoJack,¹⁹⁶ a fraud perpetrator must never be able to tell in advance whether she is targeting a consumer with an enhanced invisible deterrent.¹⁹⁷ An invisible deterrent attached to specific individuals should protect the general population in substantially the same manner as that of invisible devices attached to cars. LoJack prevents the completion of auto theft through concealment and an increase in (A).¹⁹⁸ Similarly, an enhanced invisible deterrent attached to a random set of consumers prevents the completion of theft and increases (A).

The enhanced invisible consumer approach, however, like many conceptual devices, has some flaws. The existence of randomly protected consumers would not shift fraud attempts toward those more likely to report it. With this approach alone, fraud would likely be directed at the same populations. Even within the vulnerable populations, those given enhanced invisible deterrent status might be unable or unwilling to avail themselves of the privileges assigned to them. For instance, the elderly might not understand the implications of their status or how to exercise their rights. Groups with immigration enforcement concerns or fear of authority may be too attenuated from the system to obtain such a status. Even if protected status could be logistically assigned within these groups, they may be reluctant to exercise it. The administration of such a program and the level of public education associated with it, while not inconceivable, is somewhat foreboding.

Nonetheless, the enhanced, invisible, randomly assigned deterrent approach should not be dismissed as mere high concept, because it

196. See *supra* notes 135–144 and accompanying text.

197. The penalty for disclosing protected status to a merchant should be loss of that status, at a minimum. This would prevent consumers from abusing or unfairly leveraging their status. A system of rules and logistics would obviously need to be designed to enforce this.

198. See *supra* note 143 and accompanying text.

may spur more thinking¹⁹⁹ and could ultimately be part of a comprehensive new approach to consumer protection in the United States. Ayres and Levitt found that, in the cities where automobile LoJack was introduced, “auto thefts per capita decline[d] by . . . 17.4 percent . . . [with] little apparent change in non-LoJack cities.”²⁰⁰ A similar result in the consumer fraud arena would be a significant achievement.

Although the analogy between physically protecting automobiles and legally protecting people is not perfect (for example, the human factor is more influential in the consumer fraud context), it is worth pursuing. As a practical matter, policymakers can offer this concept as a state or local pilot program. The effectiveness of the program could be measured in a controlled environment and adjusted accordingly. As explained below, however, the best approach would be to combine the hyper-protected, defined group approach with the randomly selected, enhanced invisible deterrent approach.

D. The Power of a Combined Approach

Combining the enhanced invisible deterrent approach with a defined group approach would enable society to concentrate limited resources on the consumer fraud problem. The combined approach does not require significant incremental enforcement mechanisms. Instead, it provides a front door to interface with our current consumer protection regime. The complaint window will guide the specially protected consumer through the process. Resources must be allocated toward education and administration, but this requires channeling incremental resources targeted for new enforcement initiatives.

As a combined incremental effort, the two approaches would raise (A) on two fronts: shifting fraud toward those likely to report it and

199. Politically or logistically challenging proposals are often met with strong reactions. A case study is Anne Alstott and Bruce Ackerman's proposal to solve economic inequality in the United States by granting every citizen upon graduation of high school a cash amount of \$80,000—first for educational use, then for other means after age twenty-one. BRUCE ACKERMAN & ANNE ALSTOTT, *THE STAKEHOLDER SOCIETY* 1–5 (1999). The proposal met with blistering criticism from some quarters. See, e.g., James K. Galbraith, *Raised on Robbery*, 18 *YALE L. & POL'Y REV.* 387, 388 (2000) (book review). Yet the book has spurred thought and reaction, even on a practical level (such as the development of the UK Child Trust Fund program, which partially rests on Alstott and Ackerman's work). See Rajiv Prabhakar, *Attitudes Toward the Child Trust Fund, What do Parents Think?*, 6–7, 22 (CSD Working Paper No. 06-10, 2006), available at <http://gwbweb.wustl.edu/csd/Publications/2006/WP06-10.pdf>; Dominick Maxwell, *Child Trust Funds in England*, Inst. for Pub. Policy Research (Mar 1, 2006), <http://www.ippr.org/articles/?id=2029&tID=93&pID=2029>. Thus, even broad theoretical strokes and audacious policy proposals can stir practical impact quite quickly.

200. Ayres & Levitt, *supra* note 13, at 53.

creating an atmosphere of enhanced deterrence in the general population. (*B*) would also rise, not only for perpetrators targeting the specifically defined group, but also for groups that are adjacent to that group. The enhanced invisible deterrent would also boost (*B*) throughout the economy. Taken together, the threshold for commission of consumer fraud will increase through a combination of defined and random group approaches. One concern about this approach is that enterprises and individuals engaging in legitimate activity may have to take extra precautions or may balk at targeting certain markets for their goods and services because of heightened protection for a group. These compliance costs will not be trivial in an environment with heightened protection.²⁰¹ The benefits of increased protection, however, will outweigh the costs of compliance.

V. CONCLUSION

Consumer protection has been a difficult, perpetual challenge for U.S. policymakers and institutions. Fraud continues to evolve. Perpetrators hone in on those who are weak and unlikely to report. Resources devoted to the problem are limited and usually target specific *post hoc* schemes.

To respond, policymakers should seek mechanisms that leverage current human behavior at minimal incremental cost to achieve the maximum effect upon the consumer fraud problem. Selecting a specific group for protection, if artfully done, has cascading effects on the incentives of perpetrators, consumers, and collective groups. It shifts incentives and leverages preexisting behavior patterns to elevate the risk and, therefore, the threshold for fraud commission. If policymakers select a random group for protection, they will have a strong first-order effect. For the perpetrator, commission becomes riskier through this lower-cost initiative. If selection of an invisible, random group for protection can do for consumer protection what LoJack did for automobile theft, the effect will be enormous.

Further, there may be other applications for the stealth, random assignment of special status. Policymakers would want to unlock the power of the citizenry in transactions that are often hidden from sight and in situations where enforcement can be excessively expensive. Imagine that a state or locality randomly conferred a concealed special status on residential properties. In other words, burglary of these

201. For example, although the Sarbanes-Oxley Act of 2002 was intended to protect investors, it has imposed significant compliance costs. See Guhan Subramanian, *Fixing Freezeouts*, 115 *YALE L.J.* 2, 6 & n.16 (2005) (and sources cited therein).

residential properties would result in severe sanctions. Would this result in an efficient reduction in the overall burglary rate? Consider the case of a college dealing with a plague of cheating scandals. If the college selected a random, concealed group of students, charged them with the responsibility of reporting academic dishonesty, and conditioned a full tuition waiver on whether they meet their reporting obligations, would it work? Would we want to live in such a society? If policymakers use invisible deterrent status to protect some individuals, would it be effective? Would it be too Orwellian? Should we limit our application of randomness to the protection of specific property and victims? In the consumer fraud context, implementing one or both of these approaches should, at the very least, help policymakers understand how fraud perpetrators will react to changes in their incentive structure and could help protect a vulnerable group. At most, it could provide a powerful weapon for reducing a pervasive economic and social plague.

