

Citation (APA): Modic, D., & Anderson, R. (2015). *It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud*. *Ieee Security & Privacy*, 13(5), 99-103. doi:10.1109/MSP.2015.107

It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud

David Modic and Ross Anderson | University of Cambridge Computer Laboratory

© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

In last issue's column, Monica T. Whitty provided an overview of mass-marketing fraud.¹ In this article, we delve deeper into the emotional aftermath of Internet fraud. We empirically show that understanding fraud's emotional consequences is necessary in the fight against fraud. Different affective costs are associated with different types of traditional crime; so, we reasonably assumed that different types and magnitudes of emotional costs would be associated with different types of Internet fraud. Our study analyzed these emotional consequences, ranking the most prevalent fraud types by perceived impact. We specifically hypothesized that

- becoming an Internet fraud victim carries emotional as well as financial costs,
- these financial and emotional costs vary across fraud categories, and
- individual personality traits influence the victims' perceptions of impact.

Effects of Victimization

Despite Internet fraud's hold on the public interest, the probability of becoming a victim is fairly low. Doug Shadel and Karla Pak estimated a 7 percent response rate to Internet fraud,² while David Modic and Steven Lea found that only 17 percent of the general



population responded to scams.³ Cormac Herley argued that some fraud types (such as the Nigerian advance fee fraud) are purposely transparent to glean the most naive individuals, thereby increasing the chances of fleecing eventual responders.⁴ But although Internet fraud's incidence rates are low, its eventual costs are high because of the sheer scale at which these scammers operate.

Ross Anderson and his colleagues estimated direct losses in the hundreds of millions of pounds per year for credit card fraud alone, with the global figure being 20 times as large.⁵ Consumer agency estimates from across the globe

vary wildly.⁶⁻⁸ There's little doubt that being a crime victim has both emotional and financial consequences, but comparably little research has focused on the victims' emotional costs.

Mark Button and his colleagues demonstrated that many hidden emotional costs, such as stress, result from the financial hardship and relationship issues associated with fraud victimization.⁹ Doug Shadel argued that victims' fear of secondary victimization (victim blaming) strongly influences their subsequent decision making.¹⁰ Finally, Whitty and Tom Buchanan reported that victims of romance scams, or "lonely-hearts

Table 1. Participants' incidence rates for the 10 most common online fraud schemes (N = 6,609).

Scheme	Plausible*		Responded		Lost utility	
	n	%	n	%	n	%
Accommodation: an accommodation ad with very reasonable conditions (for example, rent about half the usual amount)	252	3.8	184	2.8	59	0.9
Auction fraud: an auction with a low price for a very desirable item	359	5.4	407	6.2	325	4.9
Boiler room scam: a call from a broker offering you an insider tip on some good value stock	124	1.9	81	1.2	59	0.9
Computer hijack: an email or webpage advertising a free security sweep or antivirus scan	549	8.3	427	6.5	63	1.0
Counterfeit goods: an online store selling genuine goods for a fraction of the usual price	427	6.5	404	6.1	223	3.4
Phishing: an email from a supposed system administrator or bank manager requesting your login details or bank access codes	272	4.1	917	13.9	202	3.1
Lottery scam: an email claiming that you won an online lottery	78	1.2	172	2.6	78	1.2
Advance fee fraud: an email claiming you're about to receive a windfall (for example, inheritance, dormant bank account, free loan, or EU development funds)	66	1.0	146	2.2	57	0.9
Lonely-hearts swindle: contact from an unknown person looking for companionship or fun	108	1.6	248	3.8	99	1.5
Pyramid scheme: an invitation to participate in a get-rich-quick marketing event without any investment on your part	93	1.4	141	2.1	35	0.5
Overall compliance (total across categories)	2,328	35.2	3,127	47.4	1,200	18.3

*Plausible was defined as a score of 4 or higher on a seven-point Likert-type scale where 1 = completely implausible and 7 = extremely plausible.

swindles,” experience heightened sadness and depression.¹¹

Study Participants

Our study was advertised on the BBC Future website (www.bbc.com/future) in October 2014 as part of a psychology of fraud article. Self-selected participants completed an online questionnaire hosted on our local server (<http://goo.gl/ZwakpA>). The data used in this analysis were part of a larger victimization survey. Participants didn't receive monetary compensation, but they could choose to receive an email discussing their individual results, which 2,131 opted to do. Of the initial 10,493 responses, 3,884 were discarded because the participants failed to answer at least 50 percent of the questions. The final sample size was 6,609 responses.

In the analyzed sample, gender was unevenly distributed, with 71 percent males ($n = 4,588$) and 29 percent females ($n = 1,840$); 3 percent ($n = 181$) didn't respond to this question. Our respondents were generally older, with 23 percent ($n = 1,499$) aged 41 to 50 years old and 22 percent ($n = 1,476$) aged 51 to 60 years old. Most were college graduates: 36 percent ($n = 2,332$) had a bachelor's degree or similar, 30 percent ($n = 1,949$) a master's or professional degree, and 10 percent ($n = 636$) a doctoral degree. Most participants were married (57 percent, $n = 3,692$), and a few (3 percent, $n = 214$) were unemployed or casual workers. Regarding computer and technological expertise, participants reported a mean skill level of 4.41 (standard deviation [SD] = 0.86) on a six-point Likert-type scale where 1 = inexperienced and 6 = expert.

Study Design

We performed a series of correlations, multinomial regression analyses, and analyses of variance (ANOVAs) on the data to establish the financial and emotional impacts of scam compliance.

Dependent Variables

We measured two dependent variables (DVs): emotional and financial impact. Emotional impact represented the participants' self-reported strength of perceived affective consequences across Internet fraud categories, whereas financial impact characterized the participants' self-reported financial loss as a consequence of victimization. Participants were instructed to “Think of the situation you specified above that had the biggest significance to you. Please tell us what impact it left on you. Please answer

on a scale of 1 to 10, where 1 means that the aftermath left no impression at all and 10 means it had a very high impact.” They were then asked, “In terms of money you had at the time, how big was the financial impact on your budget?” and “Emotionally, how strongly did being conned impact you?”

Independent Variables

We also analyzed three sets of independent variables (IVs). The first IV, schemes, represented the participants’ self-reported scam compliance with the 10 most common online fraud schemes: accommodation, auction fraud, boiler room fraud, computer hijack, counterfeit goods, phishing, lottery scams, advance fee fraud, lonely-hearts swindles, and pyramid schemes.^{3,6,7} For each scheme, participants rated their compliance as 0 (no compliance), 1 (found the scheme plausible), 2 (responded to the scheme), or 3 (lost utility to the scheme). We define utility as an economist would: a measurable good that an individual might gain or lose in a given exchange, for example, money, happiness, hope, or free time. These scam compliance stages were established in previous research.^{3,12}

Results

Our analyses of the survey data revealed the following incidence rates and emotional and financial impacts.

Incidence Rates

Approximately 35 percent of the participants found at least one scheme plausible; computer hijack was considered the most plausible at 8 percent, followed by counterfeit goods at 6 percent. Phishing scams had the highest response rate at 13 percent of participants. The most successful type of fraud in terms of loss of utility was auction fraud at 5 percent of participants. Table 1 details the incidence rates for each fraud scheme.

Table 2. Financial and emotional impact interactions and ranking across fraud categories in self-reported victims (n = 1,366).

Scheme	Financial effect [†]	Emotional effect [†]
Accommodation	1.152***	0.725*
Auction fraud	-0.65***	-1.18***
Boiler room scam	1.507***	0.114
Computer hijack	-0.117	0.393
Counterfeit goods	-0.593**	-1.263***
Phishing	-0.554**	-0.261
Lottery scam	-1.307***	-1.914***
Advance fee fraud	0.94*	1.314*
Lonely-hearts swindle	0.824***	1.435***
Pyramid scheme	1.807***	0.480

Significance is indicated as follows: * $p < 0.10$, ** $p < 0.05$, and *** $p < 0.001$.

[†] These coefficients show the magnitude of differences across different fraud types as compared with the reference category, which was scam compliance with other fraud types not contained in the measured categories.

Emotional and Financial Impact

In the following analysis, we focus on only those respondents who lost utility to Internet fraud ($n = 1,366$). Table 1 shows the number of participants who lost utility to the schemes we specifically analyzed ($n = 1,200$). The 166-participant discrepancy between the two samples is due to some participants losing utility to scams other than the ones we measured.

We first tested the DVs for suitability of use in the general linear model. The financial variable was positively skewed (mean = 2.63, SD = 2.26), and the emotional variable was negatively skewed (mean = 5.14, SD = 2.83). Although Shapiro-Wilk and Kolmogorov-Smirnov tests showed these data to be nonnormal, the relatively large sample size counterbalanced this; group-size discrepancies were similarly counterbalanced.

We performed a 2×1 ANOVA for impact (financial and emotional) and schemes (converted into a single categorical variable). The main effect of impact was statistically significant (financial: $F(30, 1,339) =$

13.113, $p < 0.001$; and emotional: $F(30, 1,339) = 12.884$, $p < 0.001$); that is, our fraud victims perceived significant financial and emotional impacts. The observed power of the main effect was 1.00, and the effect sizes were 0.097 (financial) and 0.096 (emotional). Most impact \times scheme interactions were statistically significant (see Table 2).

Discussion

Confirming our hypothesis, we found that our participants perceived significant financial and emotional impacts across the studied fraud types. Although some previous evidence existed for the emotional impact of victimization,^{9,11} our analysis quantitatively confirmed those more qualitative findings.

Furthermore, financial and emotional costs varied across fraud types. Financially, the results were somewhat cut and dried: boiler room fraud had the highest reported financial loss, closely followed by pyramid schemes and accommodation fraud (see Figure 1 for the full rankings). Although some fraud types have potentially high return rates—lottery scams, for example—they have

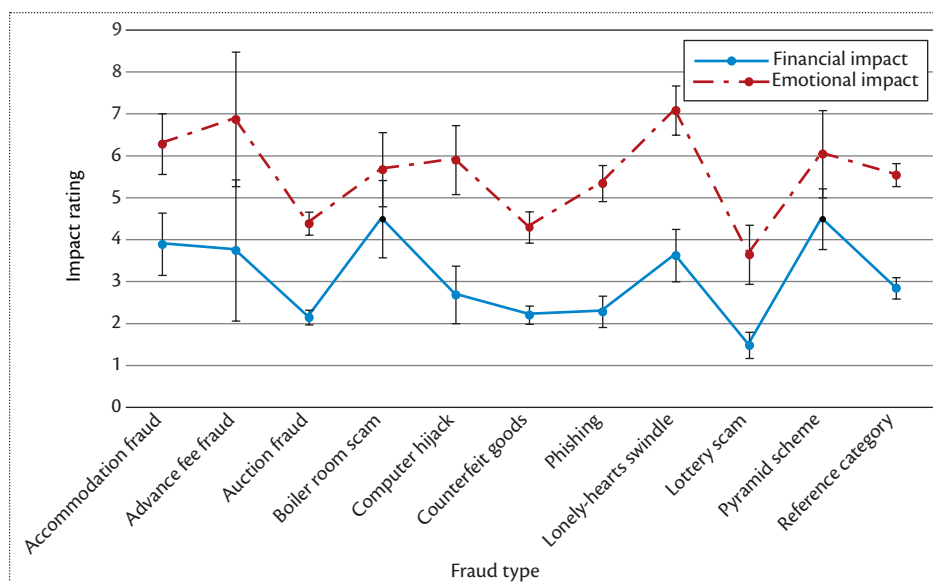


Figure 1. The participants' average reported impact for each fraud category. Boiler room fraud had the highest reported financial loss, closely followed by pyramid schemes and accommodation fraud.

such low incidence and plausibility rates that almost no one complies with them anymore.

Interestingly, although pyramid schemes seem transparent to most people (especially after the Bernie Madoff case), our respondents ranked them as the second highest financial impact category. Very few individuals fall for pyramid schemes (half of a percentage in our sample), but those who do feel a comparatively high financial sting. These findings suggest that we should pay more attention to pyramid schemes in addition to the more elaborate Internet frauds typically studied.

Participants reported the highest emotional impact for romance scams. We expected that categories eliciting sadness as an aftermath would have the highest ranking. But advance fee fraud ranked as the second highest emotional impact category, closely followed by accommodation scams. In advance fee fraud, scammers work hard to establish a relationship with potential victims¹³—making the eventual betrayal similar to that of a romance scam. In accommodation fraud, the respondents reported either renting a nonexistent property

or buying a property for which the deal didn't go through. In both cases, the emotional impact might stem from a loss of security.

Attitudes toward financial loss differ according to an individual's wealth. Simply put, a millionaire who loses the equivalent of US\$100 will be less emotionally affected than an unemployed person who loses the same amount. However, both will have lost some personal utility. Millionaires who lose many times their monthly income to fraud will experience similar emotional and financial impact as less wealthy individuals. Therefore, we recorded the participants' perceptions of impact relative to their monthly income at the time of victimization. Financial impact depends on personal utility and emotional impact is subjective by default, so focusing on individual perceptions allows easier cross-referencing of the two categories.

Interestingly, some individuals didn't find certain scams plausible yet still responded to them, perhaps because they had unrealistically positive expectations of resolution of events (optimism bias)^{14,15} or false illusions of control.^{16,17}

However, exploring these phenomena's effect on scam compliance is beyond this article's scope.

Internet fraud's emotional impact is a major component of victimization and felt as strongly as the financial impacts. We suggest that policymakers and other interested parties consider both elements when crafting policies to deter fraud and manage its aftermath. Furthermore, as Figure 1 shows, the participants consistently reported emotional impact as more severe than financial impact across all fraud types. Even after we reanalyzed our results while controlling for the emotional impact of a financial loss (versus the emotional impact of being scammed), the emotional aspect remained an important component of a scam's aftermath. However, the strong correlation between monetary and emotional losses aligns with Stephen Lea and Paul Webley's research showing that possession or dispossession of money elicits a strong emotional response,¹⁸ as well as with Ben Seymour and his colleagues' finding that financial losses activate the brain's pain receptors.¹⁹

Two practical approaches to combat fraud are minimizing the impact of affective states on decisions to engage with scammers and alleviating the stress and anguish of fraud's aftermath. For example, individuals might correspond with scammers in the mistaken belief that the scam payoff is the only way to ensure a comfortable existence. We can counteract such beliefs by demonstrating that victims rarely experience favorable outcomes and by dismantling the scammers' reassurances one by one. To alleviate stress and anguish, numerous therapeutic techniques can be used to disperse stress and negative emotional states. For example, reframing^{20,21} can help victims see losing

money as the “fee” for learning how not to fall for fraud, or having a broken heart as a valuable lesson in reading people and understanding their own relationship expectations.

After a scam, it might be “all over but the crying,” but there are still ways to minimize the length and strength of its impact. ■

Acknowledgments

This work was supported by the Engineering and Physical Sciences Research Council (grant RG 73897 to David Modic), whom we wish to thank. We also thank King’s College for enabling this line of research.

References

1. M.T. Whitty, “Mass-Marketing Fraud: A Growing Concern,” *IEEE Security & Privacy*, vol. 13, no. 4, 2015, pp. 84–87.
2. D.P. Shadel and K.B.S. Pak, *The Psychology of Consumer Fraud*, Stanford Center on Longevity, 2007.
3. D. Modic and S.E.G. Lea, “Scam Compliance and the Psychology of Persuasion,” *Social Sciences Research Network*, 2013; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2364464.
4. C. Herley, “Why Do Nigerian Scammers Say They Are from Nigeria?,” 2012; <http://research.microsoft.com/pubs/167719/WhyFromNigeria.pdf>.
5. R. Anderson et al., “Measuring the Cost of Cybercrime,” *Proc. 11th Ann. Workshop Economics of Information Security (WEIS 12)*, 2012; http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.
6. P. Fischer, S. Lea, and K. Evans, *The Psychology of Scams: Provoking and Committing Errors of Judgment. Research for the Office of Fair Trading*, Univ. Exeter, 2009.
7. *Fraud Trends January–June 2009*, National Consumer League Fraud Center, 2009.
8. *Financial Fraud and Fraud Susceptibility in the United States: Research Report from a 2012 National Survey*, FINRA Investor Education Foundation, Stanford Center on Longevity, 2013; <http://fraudresearchcenter.org/2013/09/financial-fraud-and-fraud-susceptibility-in-the-united-states-research-report-from-a-2012-national-survey>.
9. M. Button, C. Lewis, and J. Tapley, “Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families,” *Security J*, vol. 27, no. 1, 2014, pp. 36–54.
10. D.P. Shadel, *Outsmarting the Scam Artists: How to Protect Yourself from the Most Clever Cons*, John Wiley & Sons, 2012.
11. M.T. Whitty and T. Buchanan, *The Psychology of the Online Dating Romance Scam. A Report for the ESRC*, Univ. Leicester, 2012.
12. D. Modic, *Willing to Be Scammed: How Self-Control Impacts Internet Scam Compliance*, School of Psychology, Univ. Exeter, 2013.
13. W.L. Cukier, E.J. Nesselroth, and S. Cody, “Genre, Narrative and the ‘Nigerian Letter’ in Electronic Mail,” *40th Annual Hawaii Int’l Conf. System Sciences (HICSS 07)*, 2007, p. 70.
14. T. Sharot et al., “Neural Mechanisms Mediating Optimism Bias,” *Nature*, vol. 450, no. 7166, 2007, pp. 102–105.
15. N.D. Weinstein, “Unrealistic Optimism about Future Life Events,” *J. Personality and Social Psychology*, vol. 39, no. 5, 1980, pp. 806–820.
16. E.J. Langer, “The Illusion of Control,” *J. Personality and Social Psychology*, vol. 32, no. 2, 1975, pp. 311–328.
17. F. Martinez, J.-F. Bonnefon, and J. Hoskens, “Active Involvement, Not Illusory Control, Increases Risk Taking in a Gambling Game,” *Q. J. Experimental Psychology*, vol. 62, no. 6, 2009, pp. 1063–1071.
18. S.E.G. Lea and P. Webley, “Money as Tool, Money as Drug: The Biological Psychology of a Strong Incentive,” *Behavioral and Brain Sciences*, vol. 29, no. 2, 2006, pp. 161–209.
19. B. Seymour et al., “Differential Encoding of Losses and Gains in the Human Striatum,” *J. Neuroscience*, vol. 27, no. 18, 2007, pp. 4826–4831.
20. M.S. Robbins et al., “The Immediate Effect of Reframing on Client Attitude in Family Therapy,” *J. Family Psychology*, vol. 10, no. 1, 1996, pp. 28–34.
21. T.E. Nelson and Z.M. Oxley, “Issue Framing Effects on Belief Importance and Opinion,” *J. Politics*, vol. 61, no. 4, 1999, pp. 1040–1067.

David Modic is a research associate in the University of Cambridge Computer Laboratory and King’s College. Contact him at david.modic@cl.cam.ac.uk.

Ross Anderson is a professor of security engineering in the University of Cambridge Computer Laboratory. Contact him at ross.anderson@cl.cam.ac.uk.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

IEEE SECURITY & PRIVACY

Letters for the editor? Please email your comments or feedback to editor Christine Anthony (canthony@computer.org). All letters will be edited for brevity, clarity, and language.

