Masthead Logo

McGeorge Law Review

Volume 37 | Issue 2

Article 5

1-1-2006

Revoking the License to Phish: Providing Civil Remedies for Victims of Online Fraud

David Ziring

Revoking the License to Phish: Providing Civil Remedies for Victims of Online Fraud

David Ziring

Code Section Affected

Business and Professions Code § 22948 (new).
SB 355 (Murray); 2005 STAT. Ch. 33.

I. INTRODUCTION

When Briella LaCosta followed the instructions in an official-looking e-mail message and entered her eBay username and password, she was unaware of the havoc it would cause.[1] Within a few days of filling out the online forms to which she was directed, over $12,000 in purchases were charged to her credit card.[2] Ms. LaCosta's experience is hardly an anomaly. The number of phishing scams grew an average of twenty-five percent per month between July and October of 2004.[3]

The rise in popularity of online commerce sites has resulted in a parallel growth of a new form of fraud known as phishing.[4] Scammers gain private information from consumers by posing as legitimate businesses and tricking consumers.[5] In 2004, more than 76,000 consumers lost money to this form of fraud.[6]

Typical phishing scams work in the following way: consumers receive e-mails that claim to be from businesses with which the consumers do regular business.[7] The e-mails tell consumers they need to update or validate their account information and direct them to websites that appear to be websites of legitimate businesses.[8] When the consumers log into the websites, the operators of the sites steal their identities and use them to conduct business or perform illegal acts in the consumers' names.[9]

---

1. Joseph Menn, *Thieves Use Many Ways to Obtain Personal Data,* L.A. TIMES, Mar. 19, 2005, at C1.

2. *Id.*

3. ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITIES TRENDS REPORT 1 (Oct. 2004), http://www.antiphishing.org/reports/APWG_Phishing_Activity_Report-Oct2004.pdf (on file with the *McGeorge Law Review*).

4. Menn, *supra* note 1.

5. *See* Ian Austen, *On EBay, E-Mail Phishers Find a Well-Stocked Pond,* N.Y. TIMES, Mar. 7, 2005, at C1 (describing a coin dealer who had a scammer use his account to sell $780,000 in coins that did not exist).

6. SENATE JUDICIARY COMMITTEE, COMMITTEE ANALYSIS OF SB 355, at 4 (Apr. 5, 2005).

7. FTC, HOW NOT TO GET HOOKED BY A 'PHISHING' SCAM 1 (June 2005), http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf (on file with the *McGeorge Law Review*).

8. *Id.*

9. *Id.*

Existing California law prohibits fraud and unlawful business practices, but does not directly address phishing.[10] Chapter 33 provides a civil remedy to consumers and Internet service providers (ISPs) adversely affected by those engaged in phishing.[11] By taking action against fraudulent activities, the new law seeks to rebuild confidence in the security of Internet commerce.[12]

II. EXISTING LAW

A. *California Law*

California law recognizes an action for fraud.[13] A victim of a phishing scam can bring a fraud action against a defendant who intentionally misleads the victim into relying on misrepresentations that result in injury to the victim.[14]

Victims also have some legal recourse under California identity theft law. California defines identity theft as the "unauthorized use of another person's personal identifying information to obtain credit, goods, services, money, or property."[15] Existing law permits individuals to bring actions to establish that they are victims of identity theft.[16] Successfully proving they are the victims of identity theft protects individuals from liability for debts fraudulently incurred in their names.[17]

Finally, existing law permits an attorney general or district attorney to seek injunctive relief and civil penalties for "any unlawful, unfair or fraudulent business act or practice."[18] Individuals may also seek injunctive relief if they suffered an injury and lost money or property as a result of the unlawful business acts or practices.[19]

B. *Other States*

Four other states have recently passed statutes related to phishing and other similar forms of Internet fraud. Arkansas enacted the Consumer Protection

---

10. SENATE FLOOR, BILL ANALYSIS OF SB 355, at 1-2 (May 24, 2005).

11. *Id.*

12. *See id.* at 4 ("[P]hishing is greatly undermining" individuals' "[c]onfidence in the integrity of personal information transmitted via the internet . . . .").

13. CAL. CIV. CODE §§ 1571-74, 1709 (West 1982 & Supp. 2006); *see also* Robinson Helicopter Co., Inc. v. Dana Corp., 34 Cal. 4th 979, 990, 102 P.3d 268, 274 (2004) (listing the elements of fraud as a misrepresentation, knowledge of falsity, intent to defraud, (i.e., intent to induce reliance), justifiable reliance, and resulting damage).

14. *See* SENATE JUDICIARY COMMITTEE, BILL ANALYSIS OF SB 355, at 4 (Mar. 29, 2005) (discussing the elements required to bring a claim for fraud).

15. CAL. CIV. CODE § 1798.92(b) (West Supp. 2006).

16. *Id.* § 1798.93.

17. *Id.*

18. CAL. BUS. & PROF. CODE §§ 17200, 17204 (West 1997 & Supp. 2006).

19. *Id.* § 17204.

Against Computer Spyware Act, which criminalizes the installation of spyware and the collection of personally-identifiable information.[20] The Arkansas Attorney General enforces the Act.[21] Hawaii created an anti-phishing taskforce to examine options for preventing electronic commerce-based crimes in Hawaii.[22] A new Texas law permits ISPs, website owners, and trademark owners who are adversely affected by phishing scams, as well as the Texas Attorney General, to bring suit against a scammer for the greater of actual damages or $100,000.[23] Finally, Virginia has made it a felony for any person other than a law-enforcement officer to use a computer to obtain any personally-identifying information by trickery or deception.[24]

C. *Federal Law*

A proposed addition to the CAN-SPAM Act,[25] called the Anti-Phishing Act of 2005, would criminalize Internet scams that fraudulently obtain personal information by posing as legitimate online businesses.[26] This addition would impose fines and imprisonment of up to five years on a person who creates a website that represents itself as a trusted online corporation and uses that website to solicit means of identification from any other person.[27] The Act would also impose fines and imprisonment on a person who sends an e-mail message that falsely identifies itself as being sent by a legitimate business to solicit identifying information from any other person.[28] As of July of 2006, the bill had not been enacted.

III. CHAPTER 33

Chapter 33 makes it unlawful for any person to induce another person to provide identifying information by misleading that person into believing that the person is providing the information to a known and trusted online business.[29] The new law allows several different classes of plaintiffs to bring a civil action

---

20. ARK. CODE ANN. §§ 4-111-101 to 4-111-105 (West Supp. 2005).

21. *Id.*

22. HAW. REV. STAT. § 803, PT. IV NOTE (Supp. 2006).

23. TEX. BUS. & COM. CODE ANN. § 48.004 (Vernon Supp. 2005).

24. VA. CODE ANN. §§ 18.2-152.5:1 (West Supp. 2005).

25. FTC, THE CAN-SPAM ACT: REQUIREMENTS FOR COMMERCIAL EMAILERS, http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.pdf (last visited Oct. 23, 2005) (on file with the *McGeorge Law Review)* ("The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.").

26. S. 472, 109th Cong. (2005).

27. *Id.*

28. *Id.*

29. CAL. BUS. & PROF. CODE § 22948 (enacted by Chapter 33).

against individuals who violate Chapter 33. They include ISPs, owners of trademarks being infringed, individuals adversely affected by a phishing scam, and attorney generals and district attorneys.[30]

Remedies that can be awarded depend on the class of plaintiff.[31] An ISP or trademark holder may be awarded the greater of the actual damages the fraudulent activity caused or $500,000.[32] An individual who has been harmed by a violation of the statute may seek an injunction preventing future violations and recover the greater of three times the actual damages or $5,000 per violation.[33] An attorney general or district attorney may also bring an action to enjoin further violations of the statute and may recover a civil penalty of up to $2,500 per violation.[34]

In addition to the remedies available to plaintiffs, Chapter 33 allows a court, at its discretion, to increase the recoverable damages to an amount up to three times the damages that could otherwise be awarded if the defendant has engaged in a pattern or practice of violating the statute.[35] A court may also award costs and reasonable attorneys' fees to a prevailing plaintiff.[36]

IV. ANALYSIS OF CHAPTER 33

The continued growth of the California economy depends in no small part upon Internet commerce and communications.[37] Consumer confidence in online commerce must be maintained and strengthened for this growth to continue.[38] Supporters of Chapter 33 believe one of the best ways to protect consumers from Internet fraud requires both educating them with the information they need to protect themselves and creating strong laws such as Chapter 33 that are zealously enforced to combat phishing.[39]

Chapter 33 covers behavior that was already treated as a fraudulent and illegal business practice.[40] The major change it makes to the law is in the classes

---

30. *Id.* § 22948.3.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *See* Letter from Roger Cochetti, Group Dir., U.S. Pub. Pol'y, Computing Tech. Indus. Ass'n., to Senator Joe Dunn, Cal. State Senate (Mar. 30, 2005) [hereinafter CompTIA Position Letter] (on file with the *McGeorge Law Review*) (stressing the importance of the Internet to California's economy).

38. *See* Letter from Jim Hawley, Cal. Dir. & Gen. Couns., TechNet, to Senator Joe Dunn, Cal. State Senate (Mar. 30, 2005) [hereinafter TechNet Position Letter] (on file with the *McGeorge Law Review*) (discussing the importance of trust in online commerce).

39. *See* Letter from Robyn Holst, Cal. Gov't Aff. Dir., Microsoft, to Senator Joe Dunn, Cal. State Senate (Mar. 29, 2005) [hereinafter Microsoft Position Letter] (on file with the *McGeorge Law Review*) (discussing Microsoft's strategy to comabt phishing).

40. *See* CAL. BUS. & PROF. CODE § 22948.2 (West 2006).

of plaintiffs who may bring suits and the amount of damages that may be awarded.[41] By allowing victims to collect up to $1.5 million,[42] it may create the type of tough law that industry groups believe is necessary to prevent phishing scams.[43] In addition, the state budgetary impact of Chapter 33 is likely to be minimal, as awards for attorneys' fees may potentially offset any state costs.[44]

One area of concern is whether the problem of phishing can be addressed at the state level or whether, as a problem of interstate commerce, federal legislation must address it.[45] Similarly, one of the challenges facing anyone who attempts to combat phishing is the multinational nature of the scams.[46] Only twenty-six percent of phishing sites originated in the United States[47] and the number of phishing sites in China has nearly overtaken the number in the United States.[48] Often, technical solutions, such as selectively blocking data from foreign networks, are required to deal with scams originating outside of the United States.[49] Supporters believe, however, that Chapter 33, in addition to other state and federal laws, will work especially well "as a potent arrow in the quiver of Californian consumers . . . to combat phishing."[50]

While its use in identity theft is growing, phishing is only one method by which consumer information is criminally obtained.[51] Existing California and federal laws cover many of the more traditional methods of illegally acquiring personal information, such as stealing credit card applications and pick-pocketing.[52] But, as with dealing with other forms of identity theft, the most powerful way to protect consumers from phishing scams is to educate them, making it less likely the fraud will deceive them.[53]

---

41. *Id.* § 22948.3.

42. *See* CompTIA Position Letter, *supra* note 37 (calculating maximum damages of $500,000, which the court may triple when a pattern of behavior has been established).

43. *See, e.g.,* Microsoft Position Letter, *supra* note 39 (providing support for Chapter 33).

44. SENATE FLOOR, BILL ANALYSIS OF SB 355, at 3-4 (May 24, 2005).

45. CompTIA Position Letter, *supra* note 37.

46. *See* ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT, (Apr. 2005), http://www.antiphishing.org/reports/APWG_Phishing_Activity_Report_April_2005.pdf (on file with the *McGeorge Law Review*) (stating that in April 2005, sixty-eight countries hosted phishing sites).

47. *Id.*

48. *Id.*

49. *See, e.g.,* Scott Granneman, *Blocking Chinese IP Addresses*, REGISTER, Aug. 31, 2005, http://www.theregister.co.uk/2005/08/31/blocking_chinese_ip_addresses (on file with the *McGeorge Law Review*) (discussing the advantages and disadvantages of blocking all data from China and other countries).

50. CompTIA Position Letter, *supra* note 37.

51. *See* Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 663-64 (stating that traditional methods of obtaining information, such as stealing pre-approved credit card applications and gathering receipts and information from dumpsters, are being replaced modernly by more sophisticated scams, often using the Internet).

52. *See* 18 U.S.C. § 1708 (West 2005) (criminalizing theft of United States mail); *In re* George B., 228 Cal. App. 3d 1088, 1095, 279 Cal. Rptr. 388, 392 (1991) (Sparks, J., dissenting) (stating, in part, that the purpose of the grand theft statute is to protect persons from pickpocketing and other offenses that physically endanger the victim).

53. *See* News Release, Debra W. Yang, U.S. Att'y, Cent. Dist. of Cal., 'Stop Identity Theft Now'

V. CONCLUSION

Chapter 33's supporters believe it is an excellent tool in preventing phishing scams.[54] By making a remedy available to the victims of these scams, Chapter 33 acts not only to dissuade potential scammers, but also to strengthen and rebuild consumer confidence and trust in online commerce.[55] In combination with efforts to better educate online consumers and solutions the computer industry is developing, phishing may well be a problem with a solution in sight.[56]

Educational Video Program Unveiled By Justice Department Officials in Los Angeles, Feb. 26, 2003, http://www.usdoj.gov/ust/r16/pdfdocs/StopIDtheft_program.pdf (on file with the *McGeorge Law Review*) (describing a course provided by the United States Department of Justice to educate the public about identity theft threats).

54. Microsoft Position Letter, *supra* note 39.

55. TechNet Position Letter, *supra* note 38.

56. Microsoft Position Letter, *supra* note 39.

* * *