DePaul University
UNIVERSITY LIBRARIES

DePaul Business and Commercial Law Journal

Volume 13
Issue 4 *Summer 2015: Symposium - Transactional and Insurance Issues in Art and Cultural Property*

Article 5

Apple, Inc. v. Superior Court: Caveat Emptor: The Future of Online Credit Card Transactions

James John Shield Jr.

Apple, Inc. v. Superior Court: Caveat Emptor: The Future of Online Credit Card Transactions

*James John Shield, Jr.**

I. INTRODUCTION

The Internet profoundly affects modern business transactions. The emergence of the Internet marketplace[1] presents lucrative opportunities for businesses and consumers alike. Since businesses have access to a larger potential market, an online seller can receive greater economies of scale, access previously unavailable buyers, and increase the size and scope of its operations, which thereby increases profits and commercial success. Likewise, consumers also receive the benefits of greater competition, which results in lower prices, an increased availability of previously unattainable products, and a wider variety of comparable goods. However, the law pertaining to e-commerce did not develop as rapidly as the Internet market. As such, the boom in e-commerce grew in tandem with the development and prevalence of instances of Internet fraud.[2]

The laws governing e-commerce were developed in response to the surge in Internet crime; however, the laws only applied retroactively after the theft occurred.[3] But in February of 2013, the California Supreme Court issued the unprecedented case of *Apple v. Superior Court*.[4] The court diverged from the body of law protecting consumers from Internet fraud in favor of new standards that preference protecting sellers at the consumers' expense.[5] In short, the court held that California's Song-Beverly Credit Card Act of 1971 (the "Act"),[6] which prevented sellers from requiring or requesting personal infor-

* J.D. Candidate 2015, DePaul University College of Law; B.S. 2012, University of Illinois – Champaign-Urbana.

1. Throughout the comment, "Internet market", "Internet sales", "online sales", and "online transactions" all refer to the transactions occurring on the Internet and are used interchangeably.

2. *See infra* Part II.A.

3. *See infra* Part II.A.1.

4. Apple v. Superior Court, 292 P.3d 883 (Cal. 2013).

5. *See infra* Part IV.

6. CAL. CIV. CODE § 1747 (1971).

mation from consumers during a credit card sale, did not apply to credit card transactions that occurred on the Internet.[7]

This Note will explore the potential legal and policy issues addressed by the *Apple* court. Part II presents the background information necessary to fully understand the impact of the *Apple* decision. Section A discusses the general nature of online transactions, highlighting the growth of e-commerce and credit card fraud and the potential risks confronting both consumers and sellers in an online transaction. Section B details the relevant statutory provisions the *Apple* court interpreted and the pertinent decisions preceding *Apple*. Part III covers the actual subject matter of the *Apple* decision, presenting the facts, procedural history, the majority's holding and reasoning, and the dissent's objections. Part IV analyzes arguments on both sides of the court and attempts to justify the holding due to the policies of caveat emptor, Section A, and judicial discretion, Section B. Finally, Part V contemplates the potential impact that *Apple* will have on e-commerce and Internet fraud. Specifically, Section A explains how consumers are subjected to increased risks of credit card fraud and identity theft, and Section B discusses potential issues that might arise from having separate bodies of law governing traditional and online sales.

II. BACKGROUND

This section provides the pertinent history of online commerce and the policy decisions impacting consumer protection. The first section analyzes the general nature of online transactions, focusing on the rapid expansion of the Internet market and the fraud that inevitably accompanied its growth, the reasons consumers are more vulnerable to fraud on the Internet,[8] and the measures online-sellers can take protect themselves from fraud.[9] The second section examines the body of law preceding the *Apple* decision, analyzing both statutory[10] and case law.[11]

7. *Apple*, 292 P.3d at 883.
8. *See infra* Part II.A.1.
9. *See infra* Part II.A.2.
10. *See infra* Part II.B.1.
11. *See infra* Part II.B.2.

A. *The Nature of Online Transactions and Internet Fraud*

E-commerce rapidly started to expand in the early-2000s in tandem with consumer deception and fraud.[12] In 2000, "online retails were $8.686 billion, an increase of 67.1% from the Fourth Quarter of 1999."[13] Within just one year, e-commerce sales reached $25.8 billion: a 297% increase.[14] The online market's exponential pattern of growth persisted through the decade and became an integral part of the U.S. economy.[15] The most recent e-commerce statistics indicate that online sales were a highly lucrative market: U.S. manufactures reported $2.7 trillion sales, 49.3% of all shipments; merchant wholesalers repotted e-commerce sales of $1.6 trillion, 24.3% of all sales; services industries captured $346 billion, 3% of total revenues; and retailers reported $194 billion, 4.7% of total sales.[16] In just over ten years, e-commerce grew from $8.686 billion annually,[17] to $4.84 trillion annually,[18] a 55721.85% increase. However, the boom in e-commerce created fertile grounds for criminals to exploit consumers and commit credit card fraud and identity theft.[19]

New forms of consumer fraud inherently develop simultaneously with technological advancements because "fraud operators are always among the first to appreciate the potential of a new technology to exploit and deceive consumers."[20] In 1997, less than one thousand Internet fraud complaints were filed with the Federal Trade Commission ("FTC") yearly; however, the number of annual complaints increased to over 25,000 just three years later in 2000.[21] In 2012, the annual reported consumer complaints were 289,874 with an estimated dollar loss of $524,441,110, an 8.3% increase from 2011.[22] Consumer

12. *See On-Line Fraud and Crime: Are Consumers Safe?: Hearing before the Subcomm. on Commerce, Trade & Consumer Protection of the H. Comm. on Energy & Commerce*, 107th Cong. 26-27 (May 23, 2001) [hereinafter *Hearing*] (statement of Eileen Harrington, Assoc. Dir. of Mktg. Practices, Bureau of Competition, FTC).

13. *Id.*

14. *Id.*

15. *See 2011 E-stats*, U.S. CENSUS BUREAU 1 (May 23, 2013), *available at* http://www.census.gov/econ/estats/2011reportfinal.pdf.

16. *Id.* at 2.

17. *Hearing*, *supra* note 12, at 26-27.

18. Total from figures in *2011 E-stats*, *supra* note 15, at 1-2.

19. *See Hearing*, *supra* note 12, at 26-27.

20. *Id.* at 26. The FTC recapped the problems surrounding technology innovation, fraud, and commerce. "Long-distance telemarketing attracted con artists when it was introduced in the 1970's. They swarmed to pay-per-call technology when it became available in the late 1980's. Internet technology is the latest draw for opportunity predators who specialize in fraud." *Id.*

21. *Id.*

22. *2012 Internet Crime Report*, INTERNET CRIME COMPLAINT CENTER, 4 (2012), *available at* http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf.

fraud has thrived on the Internet for a variety of reasons, which presents the FTC and other government agencies with

> a host of novel challenges . . . to combat fraud and deception online. Traditional scams - such as pyramid schemes and false product claims - thrive on the Internet. Moreover, the architecture of the Internet itself has given rise to new high-tech scams that were not possible before development of the Internet. Both traditional scams and more innovative ones exploit the global reach and instantaneous speed of the Internet. In addition, the Internet enables con artists to cloak themselves in anonymity, which makes it necessary for law enforcement authorities to act much more quickly to proactively detect emerging deceptive schemes before the perpetrators disappear.[23] And because the Internet transcends national boundaries, law enforcement authorities must be more creative and cooperative to successfully combat online fraud.[24]

Thus, as Internet fraud becomes more high-tech and the size and scope of the fraud expands with the increasing global market, the effective remedies for detecting the fraud must adapt just as quickly; however, consumer safeguards presently lack the ability to act proactively – as opposed to retroactively – to detect and combat Internet fraud.[25] While fraud occurring on the Internet and in a traditional "brick and mortar" business share similar characteristics, the Internet adds a dimension of complexity and risk that warrants more proactive consumer protection.[26]

1. Consumer Vulnerability to Internet Credit Card and Identity Theft

Credit card fraud, which "is the use of another person's credit card or credit card information for the purpose of stealing," exceeded $3.2 billion in 2007.[27] Similarly related to credit card theft is identity theft – "the use by a thief, unbeknownst to his victim, of the victim's name, social security number or other personal identifying information, to open accounts and rack up huge debts for goods and service."[28] Consumers face an increased risk of both credit card fraud and identity theft on the Internet because online purchases require consumers to

23. *Id.*

24. *Hearing*, *supra* note 12, at 26-27.

25. *Id.* at 31.

26. *Id.* at 5-6.

27. Lydia Segal, *Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem*, 16 FORDHAM J. CORP. & FIN. L. 743, 747 (2011) (citing Reed Richardson, *Are You Compliant, Small Business Online Community*, BANK OF AM. (Apr. 17, 2008, 8:41 AM), https://smallbusinessonlinecommunity.bankofamerica.com/community/managing-your-finances/merchant-services/blog/2008/04/17/are-you-compliant).

28. *Hearing*, *supra* note 12, at 24.

produce their credit card number and personal information to an unknown source with the hope this information will not be reproduced, copied, or stolen. Since online purchasers do not have "an opportunity to meet and see online merchants in person, consumers are rightfully concerned with security and fraud potential when purchasing merchandise over the Internet."[29]

Frequently, online sellers do not provide consumers adequate means to contact them; some sellers omit telephone numbers and office locations and choose only to give consumers email addresses.[30] Even when the seller offers a telephone number and address, consumers never physically see the location and, therefore, cannot be certain that the seller is who they claim to be.[31] Because online transactions involve an inherent risk that the seller is not who it claims to be, consumer protection legislation has historically protected consumers.[32] Accordingly, legislatures generally determine that

> [l]aws should not place the risk of fraud or error losses from online transactions on consumers, but on the providers and online merchants who profit from the use of the technology . . . [because] shift[ing] the risk of fraud on consumers create[s] a moral hazard and will produce economically inefficient outcomes.[33]

Congress consistently recognizes the inherent problems with online identity theft and credit card fraud, but its legislation targets the criminal activity after the fact, rather than providing proactive measures to protect consumers.[34] The Computer Fraud and Abuse Act of 1986 ("CFAA") created civil and criminal penalties for unauthorized access to financial institutions' or the federal governments' digital data.[35] The Cyber-Security Enhancement Act of 2002 ("CSEA")[36] criminalized computer hacking and strengthened the CFAA's penalties.[37] The Identity Theft and Assumption Deterrence Act of 1998 ("ITADA") imposed criminal sanctions for identity theft and required the FTC to

---

29. Watchara Neitivanich, *Mechanisms for the Protection of Online Consumers; A Comparative Analysis of the U.S. E-Sign Act and Thai E-Transactions Act*, 10 ANN. SURV. INT'L. & COMP. L. 103, 103 (2004); *see generally, e.g.*, Thomas Fedorek, *Computers + Connectivity = New Opportunities for Criminals and Dilemmas for Investigators*, 76-Feb N.Y. ST. B.J. 10 (2004) (detailing the general nature of Internet fraud and its impact on both consumers and businesses).

30. Neitivanich, *supra* note 29, at 103.

31. *Id.*

32. *The Role of Certification Authorities in Consumer Transactions*, INTERNET LAW AND POL'Y FORUM (Apr. 14, 1997), http:// www.ilpf.org/groups/ca/exec.htm.

33. Neitivanch, *supra* note 28, at 108.

34. Segal, *supra* note 27, at 752-53.

35. 18 U.S.C. § 1030 (2005).

36. Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2156 (2002).

37. *Id.* § 225(g).

establish a method to record consumers' complaints.[38] Congress also "passed several laws to protect consumers from unauthorized credit card charges and losses tied to identity theft."[39] The "Truth in Lending Act,[40] ("TILA"), Regulation Z,[41] and the Fair Credit and Billing Act[42] ("FCBA") limit consumer liability for unauthorized charges . . ." and the Identity Theft Enforcement and Restitution Act of 2008 ("ITERA") allows victims of credit card fraud and identity theft to "seek restitution for money spent restoring their credit and fixing other associated harms."[43] While both federal and state legislatures addressed the problems of Internet fraud, the laws were ineffective in protecting consumers since the fraud must occur before the consumers can seek relief under these laws. Consumers are at risk every time they use their credit card online, more so than ever, because Internet credit card fraud and identity theft are increasing every year and the current law fails to afford proactive means of protection.

2. Seller's Susceptibility to Fraudulent Transactions

Online transactions are a "double-edged sword" for both buyers and sellers. Because neither party to the transaction can readably identify the other, both are at risk of fraudulent misrepresentation.[44] If a seller suspects fraud in a traditional "brick and mortar" business it can request a valid form of identification (driver's license or state identification card) to verify the consumer's identity. But, the inherent nature of Internet transactions completely eliminated the personal component of a traditional sale. Thus, when a consumer's credit card information is stolen and used to purchase goods from a seller, both parties suffer. Accordingly, sellers identified the growing instances of credit card fraud[45] and sought measures to protect themselves from fraudulent transactions.

One of the most common policies sellers implement to address the issue of Internet credit card fraud are verification systems that ascertain the identity of the purchaser. For example, there is a patented method available that can obtain "credit card information relating to the transaction from the consumer, and . . . [verify] the credit card based upon a variety of parameters . . . [that] are weighted so as to

38. 18 U.S.C. § 1028 (2005).
39. Segal, *supra* note 27, at 753-54.
40. 15 U.S.C. § 1601 (2006).
41. 12 C.F.R. § 226.1 (2014).
42. 15 U.S.C. § 1601.
43. Segal, *supra* note 27, at 752.
44. For example, both parties can assert a false identity.
45. *See supra* Part I.A.

provide a merchant with a quantifiable indication whether the credit card transaction is fraudulent."[46] After the customer purchases an online product the merchant sends the credit card information to a third-party verifier, who checks the history and consistency of the credit card user's purchases.[47] These systems provide sellers with a reliable and discrete method to verify the purchaser's identity. First, the credit card user's purchase history can be ascertained though previous credit card purchases and then a consistency check determines if the present sale conforms to the consumer's purchase history.[48] Next, the purchase information is imputed into an automated verification system that determines whether or not the information given during the sale[49] matches the information on the card.[50] Finally, the system verifies whether the credit card user's Internet address matches the Internet Protocol ("IP") address of the consumer's previous purchases.[51] Thus, online sellers presently possess unobtrusive and effective means that can determine and ensure a consumer's identity, thereby protecting them from potential fraud.

Due to the nature of the online transaction, and the accompanying potential for fraud, sellers were the first to move to prevent credit card fraud/identity theft. This is because online sellers possess the means to protect themselves from fraudulent transactions. Sellers have access to verification systems that proactively detect fraud, whereas consumers, who lack access to these systems, must entirely trust online sellers with their credit card and personal information.

46. U.S. Patent No. 6,029,154 (filed July 28, 1997). The abstract of the Patent provides a method and system for detecting fraud in a credit card transaction between consumer and a merchant over the Internet. The method and system comprises obtaining credit card information relating to the transaction from the consumer; and verifying the credit card information based upon a variety of parameters. The variety of parameters are weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent. In so doing, an integrated verification system is provided which allows a merchant, or the like, to accurately and efficiently determine the validity of a transaction over the Internet.

Id.

47. *Id.* at col. 2 l. 25.

48. *Id.* at col. 2 l. 66 & col. 3 l. 1.

49. Specifically, information that is essential to the purchase, such as delivery address.

50. *See* U.S. Patent No. 6,029,154 col. 3.

51. *Id.* at col. 3 l. 14.

B. *Legal Realm Prior to Apple*

1. Statutory Law

The California legislature enacted the Song-Beverly Credit Card Act of 1971 to govern the issuance and use of credit cards.[52] The legislature modeled the Act on Federal TILA; with the purpose of extending consumer protection from credit card fraud on the state level.[53] The Act prohibits the recording of personal identification information as a request, or requirement, in a credit card transaction.[54] Personal identification information "means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."[55] The Act explicitly provides exceptions[56] to transactions that involve contractual obligations, it permits pay-at-the-pump gas stations to require the ZIP code linked to the card,[57] and enumerates when the seller is required to record the credit card information under federal or state law.[58] Personal information may also be recorded if it is incidental to complete the individual transaction, such as

52. CAL. CIV. CODE § 1747 (1971).

53. *See id.* § 1747.01.

54. Section 1747.08(a) provides:

> [e]xcept as provided in subdivision (c) no person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall do any of the following . . . (2) [r]equest, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise.

Id. § 1747.08(a) (1971) (effective Oct. 9, 2011).

55. *Id.* § 1747.08(b).

56. While section 1747.08(c) provides three subsections of exceptions, only section 1747.08(c)(3) is relevant for this note. Subsection (c)(1) applies when "the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or other similar occurrences." *Id.* § 1747.08(c)(1). The subsection (c)(2) exception relates to "cash advance transaction." CAL. CIV. CODE § 1747.08(c)(2).

57. The *Apple* court found section (c)(3)(B) to be the most significant exception that precluded extending the Act to online transactions because it was added with the 2011 Amendment. *See* Apple Inc. v. Superior Court, 292 P.3d 883, 893 (Cal. 2013).

58. *See* § 1747.08(c)(3). In pertinent part, section 1747.08(c)(3) provides that the Song-Beverly Act does not apply if any the following applies:

> (A) The person, firm, partnership, association, or corporation accepting the credit card is contractually obliged to provide personal identification information in order to complete the credit card transaction. (B) The person, firm, partnership, association, or corporation accepting the credit card in a sales transaction at a retail motor fuel dispenser or retail motor fuel payment island automated cashier uses the ZIP code information solely for prevention of fraud, theft, or identity theft. (C) The person, firm, partnership, association, or corporation accepting the credit card is obligated to collect and record the personal identification information by federal or state law or regulation.

Id.

when the information is necessary to deliver, service, or install the purchased goods and services.[59]

The final exception in subsection (d), which created the issue in *Apple*, permits a seller to require consumers "to provide reasonable forms of positive identification, which may include a driver's license or a California State identification, or . . . another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise."[60] Finally, the Act provides civil and criminal penalties for violators.[61] In short, the Act protects consumers by prohibiting sellers from requesting or requiring personal information from consumers in the course of a credit card transaction that could be used for fraud and identity theft.

The expansion of the e-commerce market has forever changed the credit card transaction and transformed the implications of the Song-Beverly Act. Since the Act was originally legislated in 1971, and was never specifically amended to include e-commerce credit card transactions, the *Apple* court needed to determine whether or not the Act's protections extended to online sales.

2. Case Law

Technological advancements lead to unforeseen circumstances and, therefore, legislation enacted prior to these advancements places a burden on the courts to determine whether or not the legislature intended a specific law to apply to in general to all situations, or only those comprehended at the time when the law was enacted. The Song-Beverly Act's plain language is unambiguous when considering traditional "brick and mortar" transactions; however, the e-commerce explosion has presents the courts with more difficult situations to interpret.

---

59. *See id.* § 1747.08(c)(4).

60. *Id.* § 1747.08(d). The full text of this subsections provides that the Song-Beverly Act does not prohibit any person firm, partnership, association, or corporation from requiring the cardholder, as a condition to accepting the credit card as payment in full or in part for goods or services, to provide reasonable forms of positive identification, which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise. If the cardholder pays for the transaction with a credit card number and does not make the credit card available upon request to verify the number, the cardholder's driver's license number or identification card number may be recorded on the credit card transaction or otherwise.

Id.

61. *See id.* § 1747.08(e)-(f).

Florez et al. v. Linens 'N Things, Inc. was the first case to analyze the Act in light of the e-commerce boom.[62] The *Florez* court held the seller violated section 1747.08 because it requested the consumer's telephone number before completing the credit card purchase.[63] The court found a telephone number is personal information under the Song-Beverly Act and, since the seller "requested" it to complete the online credit card sale, the Song-Beverly Act prohibited the practice.[64]

In *Archer v. United Rentals, Inc.*, the Second Appellate District held that the legislative purpose of the Song-Beverly Act is to protect "the personal privacy of an individual in his or her personal identification information during a transaction involving the credit card issued for consumer purposes."[65] The court reasoned that section 1747.08 applies to *all* consumer credit purposes without regard to the actual purpose for which the credit card was used.[66] Therefore, the court did not draw a distinction between "brick-and-mortar" credit card transactions and Internet sales even though the e-commerce existed in 2003.

The Central District Court of California re-affirmed *Archer* in *Rothman v. Gen. Nutrition Corp.*, by stating that "a violation [of section 1747.08(a)] only occurs if the personal information is written down or recorded in some way."[67] Hence, the court essentially decided that a credit card transaction was a credit card transaction for the purposes of the Song-Beverly Act irrespective of the sale's form. The implication of this holding is the Act applies regardless of *form*: the Act protects consumers regardless of the structure of the sale.[68]

Then, in *Pineda v. Williams-Sonoma Stores, Inc.*, the California Supreme Court held that requesting or requiring a ZIP code constitutes personal identification information within the meaning of section 1747.08 and a retailer cannot request said information.[69] Specifically, the court found that the legislature intended for the word "address" to

62. 133 Cal. Rptr. 2d 465 (Cal. Ct. App. 2003).

63. *Id.* at 470-71.

64. *See id.*

65. 126 Cal. Rptr. 3d 118, 132 (Cal. Ct. App. 2011).

66. *Id.* at 130-31 (emphasis added). It is important to emphasize that here that just two years before the *Apple* decision the court held that the Song-Beverly Act applied to *all* credit card transactions irrespective of the sale's form.

67. No. CV 11-03617 SJO (RZx), 2011 WL 6940490, at *11 (C.D. Cal. Nov. 17, 2011).

68. By stating the Song-Beverly Act applies to all consumer transactions, regardless of its form, explicitly means the structure of the sale is irrelevant to the statute's application. E-commerce is the *form* of a credit card transaction and, therefore, it would seems that the Song-Beverly Act should afford consumers its protection during online transactions.

69. 246 P.3d 612, 620 (Cal. 2011).

be construed as not only a complete address, but rather *any* components of a consumer's address.[70]

Following the court's decision in *Pineda*, the Fourth Appellate District decided in *Alveraez v. Brookstone Co, Inc.* that Supreme Court's interpretation of section 1747.08, in *Pineda*, is not "limited in any way based on how (or whether) a retailer subsequently uses ZIP code information requested from a credit card customer and then recorded during a transaction."[71] "Section 1747.08 generally prohibits businesses from requesting 'personal identification information' during credit card transactions and then recording that information."[72] Hence, the aforementioned courts determined that the Song-Beverly protections apply to both Internet credit card sales and "brick-and-mortar" transactions. The *Apple* court subsequently diverged from this precedent and laid an unprecedented decision.

III. SUBJECT OPINION

In *Apple,* Plaintiff attempted to purchase downloadable material from Apple Inc.'s ("Apple") Internet store that only sold downloadable products.[73] Plaintiff claimed Defendant "requested or required him to provide his address and telephone number as a condition of accepting his credit card as payment" for the download purchase on iTunes.[74] Plaintiff sued Apple on behalf of himself and a putative class of similarly situated individuals.[75] Plaintiff alleged Apple violated the Song-Beverly Act by recording each customer's personal information even though Apple was not contractually or legally obligated to collect a customer's telephone number or address to complete credit card transaction and Apple did not require a customer's telephone number or address for any special purpose incidental, but related, to the individual credit card transaction.[76] In the alternative, Plaintiff asserted that even if the billing address was necessary to validate the downloadable content transaction, there was no need for requiring Plaintiff's phone number because it was not necessary for Apple to have this information to complete the transaction.[77]

---

70. *Id.* Furthermore, the court held that its statutory interpretation could apply retrospectively and afford the Plaintiff relief. *Id.*

71. 135 Cal. Rptr. 3d 777, 783 n.9 (Cal. Ct. App. 2011).

72. *Id.* at 781.

73. Apple Inc. v. Super. Ct., 292 P.3d 883, 885 (Cal. 2013).

74. *Id.* at 884.

75. *Id.* at 885.

76. *Id.* at 890. The downloadable content was instantaneously transferred to the consumer, which means that there was no purpose for an address for shipping or delivery purposes.

77. *Id.*

At trial, Apple moved to dismiss these complaints by filing a demurrer, but the trial court denied it because the Song-Beverly Act "is silent on exempting online credit card transactions" and does not completely exempt online credit card transactions for the Act's reach.[78] However, Apple promptly filed a writ of mandate seeking review of the order, but the California Court of Appeals summarily denied.[79] The California Supreme Court decided to hear Apple's case for the purposes of determining whether section 1747.08 is violated when an online retailer requests and records a consumer's home address, phone number, and email address as a condition to accepting a credit card as payment for a downloadable product.[80]

A. *The Majority*

Ultimately, the California Supreme Court decided that online retailers were permitted to require a customer's home address and phone number as a condition to accepting a credit card as payment for electronically downloadable products because the California legislature could not foresee the Internet market and, therefore, did not intend for section 1747.08 to govern Internet transactions.[81] Because downloadable content did not exist and was not anticipated when the statute was enacted, the court reasoned that the legislature did not intend to apply the Song-Beverly Act in situations where a "standard mechanism"[82] of verification was not possible.[83] Since photographic identification was unavailable during an online transaction, there was no privacy intrusion in requiring personal information because sellers were entitled to protect themselves from potential credit card fraud.[84]

Furthermore, the court decided that since the California legislature's 2011 amendment to the Song-Beverly Act permitted "pay-at-the-pump" gas stations to require the consumer's ZIP code as a condition of the purchase because "no employee or other seller is present" during the sale[85] that Internet sales, where no employee is physically present during the transaction, permits the seller to require more intrusive personal information.[86] However, the court neglected to address whether or not sellers may use a consumer's IP address and

78. *Apple*, 292 P.3d at 885.
79. *Id.*
80. *Id.* at 884.
81. *Id.* at 889.
82. E.g., physical verification of a photo I.D.
83. *Apple*, 292 P.3d at 888-889.
84. *Id.* at 889.
85. *Id.* at 890.
86. *Id.* at 892.

credit card history to verify the purchaser's identity rather than more intrusive means.

Additionally, the court held that the California Online Privacy Protection Act of 2003 ("COPPA") indicated that the legislature knew how to make its e-commerce policy explicit.[87] As such, since it neglected to address online transaction directly, the legislature did not want the Song-Beverly Act to apply to online transactions and, thus, narrowly restricted the language to preclude an application to Internet transactions.[88] Said in another way, because the legislature did not address online credit card transactions, the court determined the legislature did not want the Song-Beverly Act to apply to online sales.[89] The court found COPPA permitted online transactions to "go above and beyond the requirements of Section 1747.08," and, therefore, concluded that the Song-Beverly Act only applied to traditional "brick and mortar" sales, not online transactions.[90] Since retailers must "conspicuously post" third-party disclosure privacy policies regarding the personal identity information they collect and disclose, the court found the privacy intrusion irrelevant because a consumer could decline to accept the policy.[91] Hence, the court reasoned that an online seller was permitted to require personal information since a consumer, if "not satisfied with the policy of a particular retailer," can decline to purchase a product from the seller.[92] Therefore, an online seller is permitted to require personal information from buyers in an e-commerce transaction.

Based on

> section 1747.08's text, purpose, and history [the court was] unable to find the clarity of legislative intent or consistency with the statutory scheme necessary to conclude that the Legislature in 1990 intended to bring the enormous yet unforeseen advent of online commerce involving electronically downloadable products – and the novel challenges for privacy protect and fraud prevention that such commerce presents – within the coverage of the Credit Card Act.[93]

However, the majority casted doubt on its own decision by stating "the Legislature may wish to revisit the issue of consumer privacy and fraud prevention in online credit card transactions,"[94] indicating the

87. *Id.* at 894.
88. *Apple*, 292 P.3d at 894.
89. *Id.*
90. *Id.*
91. *Id.* at 895.
92. *Id.*
93. *Apple*, 292 P.3d at 896.
94. *Id.* at 896.

court believed the protections of the Song-Beverly Act probably should apply to online transaction.

Ironically, after refusing to grant consumers online protection from credit card fraud, the court casted no doubt on the claim that "protecting consumer privacy in online transactions is an important policy goal, nor [did it] suggest that combating fraud is as important or more important than protecting privacy. [The court] express[ed] no view on this significant issue of public policy."[95] Hence, the court illusorily claimed to be exercising judicial restraint by not dictating public policy. Yet, the court's holding explicitly created the policy that consumers have no privacy protection from online sellers extracting personal, and private, information. Because "[t]here [was] no doubt that retail commerce [had] changed dramatically since section 1747.08 was enacted . . . the idea of computerized transaction involving the sale and purchase of virtual products was beyond any legislator's imagination" the court refused to extend the Song-Beverly protections to online sales.[96] However, the dissent adamantly opposed the majority's decision for a variety of reasons.

B. *The Dissent*

Justice Kennard dissented because "California statutory law prohibits retail sellers from recording the personal identification information, such as home addresses and telephone numbers, of their credit-card-using consumers" because the legislature wanted to protect consumer privacy.[97] Because "[t]he statue does not *exempt* online sales of downloadable products . . . , and on its face the statute applies to sales conducted over the Internet just as it does to sales conducted face-to-face or by mail or telephone," Justice Kennard concluded the Song-Beverly Act should apply to online transactions.[98] Justice Kennard believed the majority's holding "leav[es] Internet retailers free to demand personal identification information from their credit-card-using customers and to resell that information to others."[99] Hence, contrary to the purpose of the Song-Beverly Act to protect consumers from fraud and identity theft, "[t]he majority's decision [was] a major win for [online] sellers, but a major loss for consumers, who in their online

95. *Id.*

96. *Id.*

97. *Id.* at 896 (Kennard, J., dissenting).

98. *Id.* at 896-97 (emphasis added).

99. *Apple*, 292 P.3d at 897 (Kennard, J., dissenting).

activities already face an ever-increasing encroachment upon their privacy."[100]

Justice Kennard argued that the "statute means just what it says and contains no exemption, expressed or implied, for online sales of downloadable products."[101] Thus, courts should presume "that the plain language of the statue express[ed] congressional intent [and, thus,] is rebutted only in 'rare and exception circumstances.'"[102] Because the statue applies to any "person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business,"[103] this statute applies to Apple because it fulfills these criteria and therefore Apple should abide by the Song-Beverly Act.[104] The statute "prohibits sellers from recording . . . credit-card-using customers' 'personal identification information'" and applies to *any seller* that accepts credit cards for to complete the transaction.[105] Therefore, Apple fulfills the statutory requirement by being a corporation that accepts credit card as a form of payment and, accordingly, cannot require personal information to complete the transaction.

Justice Kennard also analogized the impersonal nature of mail and telephone transactions, both non-face-to-face transactions that are protected by the Song-Beverly Act, to online transactions.[106] Since the Song-Beverly Act applied to mail and telephone transactions that involved no visual confirmation of the buyer's identity, Justice Kennard felt there was no significant difference between a purchase conducted over the Internet and one conducted via mail or telephone.[107] In all situations, the credit card is not physically presented to the seller.[108] Therefore, Justice Kennard felt the Song-Beverly Act applied equally to online and "brick-and-mortar business" transactions.[109]

Furthermore, the court recently held that the legislatures "overriding" purpose in enacting the Song-Beverly Act's prohibition against a seller's recording of credit-card-using customer's personal information

100. *Id.*

101. *Id.*

102. Ardestani v. INS, 502 U.S. 129, 135 (1991) (citing INS v. Cardoza-Fonseca, 480 U.S. 421, 432, n.12 (1986); Consumer Product Safety Comm'n v. GTE Sylvania, Inc., 447 U.S. 102, 108 (1980)).

103. CAL. CIV. CODE § 1747.08(a) (1971).

104. *Apple,* 292 P.3d at 897 (Kennard, J., dissenting).

105. *Id.*

106. *Id.* at 898.

107. *See id.* at 890.

108. *Id.*

109. *Apple,* 292 P.3d at 902 (Kennard, J., dissenting).

was to protect the *consumer* right to privacy.[110] Hence, "the majority's focus on fraud protection for sellers is at odds with this court's recent" decisions, and overlooks "the fact the Legislature *already did* enact addition protections" to prevent credit card fraud.[111] Therefore, the majority erroneously provided businesses protection at the direct expense of consumer privacy, which was the focus of the Song-Beverly Act.[112]

Justice Baxter also dissented because he believed that the majority decision "reli[ed] on speculation and debatable factual assumptions [that] carved out an expansive exception to section 1747.08 that leaves online retailers free to collect and use the personal identification information of credit card users as they wish."[113] The statute expressly permits a seller to require positive forms of identification, but prohibits *requiring* personal information to complete the transaction.[114] The statute explicitly states that "personal identification information" is "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."[115] Therefore, the statute unequivocally prohibits sellers from recording an address and telephone number as a *requirement* of a credit card transaction.[116] Hence, Justice Baxter felt the majority, as a matter of law, erroneously applied the Song-Beverly Act to advocate online sellers from the undue risk of credit fraud because the purpose of the statute was to protect *consumers*.[117]

IV. ANALYSIS

This part seeks to objectively dissect the *Apple* court's holding and shed light on the specific legal issues raised in its decision. The first section reconciles the court's rule by applying the principle of caveat emptor, and the second section explains why the court's holding was incorrectly decided because the court restrained from applying a statute where the face and legislative intent of the Act was unclear; however, by deferring to apply the statute, the court essentially dictated public policy.

110. *Id.* at 899 (referring to Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 619 (Cal. 2011)).
111. *Id.* at 899 (emphasis added).
112. *Id.* at 900.
113. *Id.* (Baxter, J., dissenting).
114. *Apple*, 292 P.3d at 900 (Baxter, J., dissenting).
115. *Id.* at 901 (citing § 1747.08(b)).
116. *Id.* at 902.
117. *Id.* at 904.

A. *Revival of Caveat Emptor*

The *Apple* majority's reasoning is justified on the grounds of caveat emptor.[118] Online sales inherently present problems for both consumers and sellers: the question inevitably asks who should bear the risk? In *Apple*, the court decided consumers should bear the risk of online credit card fraud and identity theft, which was an unexpected development.[119] The decisions leading up to *Apple* all alluded that the court believed the Song-Beverly Act applies to online transactions. In *Archer*, which was decided in 2011, the court found the purpose of the Song-Beverly Act was to protect consumers in *any* credit card transaction in *any* form.[120] Thus, the previous interpretations of the Act indicated it protected consumers in all credit card transactions by making it illegal for sellers to record personal information. Accordingly, the *Apple* decision was completely divergent from the previous decisions that favored consumer protection.

The court justified its "buyer beware" position by drawing a distinction between traditional face-to-face sales and online transactions.[121] In the former, the California legislature permitted seller's to reference a California driver's license or state identification card to verify identity.[122] In the latter, however, sellers lack means to confirm that the credit card user is, in fact, the actual purchaser. Accordingly, the court reasoned online sellers are permitted to request and require personal information, such as street address, phone number and email address, to confirm the purchaser's identity.[123] As a result, consumers must divulge highly sensitive personal information to online sellers and hope this information is not stolen.

The court believed its decision was a sound method to prevent fraud and that there was "no tension between privacy protection and fraud prevention."[124] However, the court created a broad exception to protecting consumers from fraud and narrowed online privacy rights, thereby implicitly declaring preventing online sellers from fraud is a more important goal than consumer protection and the right to privacy. So, who must bear the risk of online identity theft and fraud? *Apple* unequivocally answered the legal question by allocating

118. "A doctrine holding that purchasers buy at their own risk." BLACK'S LAW DICTIONARY 102. (4th Pocket ed. 2011).

119. *Apple*, 292 P.3d at 899.

120. *See generally* Archer v. United Rentals, Inc., 126 Cal. Rptr. 3d 118 (Cal. Ct. App. 2011).

121. *Apple*, 292 P.3d at 892-93.

122. *Id.* at 891. It is important to note that this form of identification was only used to verify a purchaser's identity – it could *not* be recorded by the seller.

123. *Id.* at 894.

124. *Id.* at 889.

the burden on consumers, so long as the California's legislators do not say otherwise.

B. *Disguised Judicial Activism*

The *Apple* opinion – at first glance – is justified on the grounds of judicial restraint. It claims that because the California legislature did not foresee the expansion of e-commerce when the Song-Beverly Act was enacted, the court should not go so far as to apply it to unforeseeable developments.[125] The legislature had the opportunity to specifically address whether the Act should apply to the Internet transactions, and, since it declined to do so, the court held that the Act's protections were not intended to apply to online credit card sales.[126]

The potential issue with this justification is the fact that the court gives more weight to the absence of legislative intent than the plain meaning of the statute. The Song-Beverly Act, on its face, unequivocally bars sellers from "requesting, or requiring as a condition to accepting the credit card as payment . . . for goods or services, the cardholder to write any personal identification information upon the credit card transaction form or otherwise."[127] The legislature provided explicit exceptions to statute and "e-commerce" is not listed.[128] Hence, the plain meaning of the statute would support the position that the Act applied to all credit card transitions. However, the court ruled that online transactions are exempt from the protections of the Act because the Legislature did not *specifically* address the issue. By making this ruling, the court established a policy that could not be ascertained from the statute itself. The *Apple* court's decision essentially creates policy by stating there Song Beverly Act's protections do not apply to e-commerce transactions.

The *Apple* dissents present valid counter arguments that the majority fails to address.[129] The majority places great importance on the fact that the legislature could not foresee e-commerce and, therefore, the Song-Beverly Act only applies to face-to-face transactions. However, the court held in *Archer* the Act applies to all credit card transactions including telephone and mail order credit card transactions,

125. *Id.*

126. *Apple*, 292 P.3d at 895.

127. CAL CIV. CODE § 1747.08(a)(1).

128. *Id.* § 1747.08(c)(1)-(4).

129. *See supra* Part III.B.

which are also non-face-to-face transactions.[130] The dissenters refused to join the majority because precedent clearly indicated that the Act would most likely cover online transactions.[131] Accordingly, it is possible to conceive that the legislature did not make a specific e-commerce amendment to the Song-Beverly Act because prior to the *Apple* decision an amendment was not necessary: the *Archer* court ruled the Act applied to *all* credit card transactions, including non-face-to-face ones occurring in a typical "brick-and-mortar" store. However, the court decided to ignore the Act's purpose, consumer protection,[132] and implemented a judicially created policy that is detrimental to consumers.

V. IMPACT

This part contemplates the potential impact the *Apple* decision will have on the public. The first section explains the increased amount of risk consumers must now bear and the second analyzes the impact the decision might have in the legal world by demanding a separate and specific body of law for online transactions.

A. *Consumers Face Increased Risk of Identity Theft & Internet Fraud*

Apple imposed a strict standard of caveat emptor on consumers who purchase products online with credit cards. In effect, consumers must provide online sellers with whatever personal information the seller requests and/or requires – i.e. address, phone number, email address – to continue with the online transaction. Thus, consumers face increased risk of being subject to credit card fraud and identity theft because they are required to provide all sellers with the necessary personal information needed to steal someone's identity.

The situation imposes three potential risks on consumers: (1) higher instances of fraudulent transactions, (2) the increased chance of hav-

130. *See* Archer v. United Rentals, Inc., 126 Cal. Rptr. 3d 118, 132 (Cal. Ct. App. 2011); *Apple*, 292 P.3d at 900 (citing *Archer*, 126 Cal. Rptr. 3d at 132). The dissent finds not only that this point very persuasive, but it is also a huge point that the majority failed to address. In both mail order and telephone order sales, the seller and purchaser never come into physical contact with one another. In these instances, the seller has no means to verify the buyer's identify via a State issued identification card. Hence, the dissent found these situations analogous to online purchases because, just like in mail and telephone sails, there is no means for the seller to verify the purchaser's identity. Accordingly, the dissent could not rationalize why the Song-Beverly Act would apply to some credit card transactions where the purchaser's identity cannot be readily verified, but not to e-commerce sales.

131. *See Apple*, 292 P.3d at 897-98.

132. *Id.*

ing a credit card and personal information stolen on the Internet, and (3) decreased incentives for sellers to proactively prevent credit card fraud. The combined effect of subjecting consumers to these risks is a decrease in consumers' confidence in the purchasing online products, which could result in fewer online sales. Rather than strict caveat emptor for online sales, a better policy would be to increase consumer's desire to purchase online by increasing their confidence in the market.

The *Apple* decision opens the door for online scams to exploit consumers by allowing fraudulent sellers to acquire the consumer's credit card and personal information. Because consumers cannot verify with whom they are dealing, they bear the burden of transacting with a fraudulent seller who could steal the individual consumer's credit card and identity. With this information, the thief can fraudulently use the consumers' credit card and information. Even more problematically, the *Apple* court specifically stated its holding applies to downloadable content where there is no physical delivery of the product.[133] Hence, the sale is transmitted to a computer address that can be easily changed by a thief using a public computer and storing the information on a flash drive. Permitting a seller to demand as a condition of the sale all of the requisite information to steal a credit card and identity, therefore, imposes a heightened risk of consumers dealing with parties that can abuse this personal information.

The *Apple* decision also increases the risk that third parties steal consumers' credit card number and identity. Internet thieves develop in tandem with policy of the Internet market.[134] Accordingly, cybercriminals have a greater opportunity to intercept consumers' credit card and personal information. While a variety of businesses use methods such as a "secured checkout" to prevent such from occurring, there is nothing to prevent a hacker from devising a method to infiltrate the secured checkout and steal the consumers' credit card number and identity. One of the biggest issues not even addressed in the opinion is the fact that under the Song-Beverly Act, "brick and mortar" stores were permitted to require a valid form of identification as a condition to sale, but the seller could not record the personal information contained thereon. History has already proven that consumers are a high risk for credit card and identity theft because businesses often store the purchasers' credit card number and personal information in a database. For example, in December of 2013, Target Corpo-

133. Apple Inc. v. Super. Ct., 292 P.3d 883, 896 (Cal. 2013).
134. *See supra* Part II.A.

rate's ("Target Corp.") systems were infiltrated and all of the information contained on consumers' credit cards was stolen.[135] However, in January 2014, Target Corp. discovered in addition to credit card information being stolen that the consumers' personal information including street address, telephone number, and email address were intercepted as well.[136] Neiman Marcus has also reported similar credit card thefts.[137] Therefore, not only are consumers at risk every time they use their credit card online, but also when they are not using their card, if the online seller records the card and personal information and it is hacked.

Exacerbating the problem is the fact that credit card companies have little incentive to implement fraud detection technologies.[138] Specifically, credit card companies have little incentive to combat identity theft and fraud because "[t]hey get paid every time their card is used, even in a fraudulent transaction."[139] The credit card companies get paid an "assessment fee" – "a percentage of the price of every purchase made using their card brand" – 0.0925% for Visa and 0.0950% for MasterCard and Discover.[140] Counter intuitively, the credit card industry itself is presently profiting from the increases in credit card fraud and, therefore, will unlikely implement more advanced fraud detection technologies that would benefit consumers. Furthermore, the credit card companies themselves are not liable for any of the loss: the seller is the one who "takes the hit when the thief makes the purchase over the phone, Internet, or by mail, known as

---

135. Anne D'Innocenzio, *Target Breach Appears to Be Part of a Broader Scam*, ASSOCIATED PRESS (Jan. 16, 2014), http://bigstory.ap.org/article/target-breach-appears-be-part-broader-scam.

136. *Id.* In fact, I purchased a product on Target Corp.'s website in October of 2013 and received the following email from Target Corp: "As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion." Email from Target.com to James John Shield, Jr. (Jan. 17, 2014, 7:02 AM).

137. D'Innocenzio, *supra* note 135.

138. *See* Segal, *supra* note 27, at 751 ("Technology Plays a central role in data security, but as criminal tactics continually evolve, it is important that the incentives first change to encourage the industry to select the best technological solutions for itself on a continuing basis. Right now, although a plethora of technological innovations exist, the banks and card companies appear more interested in not 'rocking the boat' than in pushing for the best options for all parties."); *see, e.g.*, Ian Heller, *How the Internet has Expanded the Threat of Financial Identity Theft, and What Congress Can Do to Fix the Problem*, 17 KAN. J.L. & PUB. POL'Y 84, 106-08 (2007) (arguing that using biometrics is an alternative to combat identity theft).

139. Segal, *supra* note 27, at 770.

140. *Id.*

'card-not-present' transactions."[141] Because the sellers absorb the cost of fraud, they require more detailed and more personal information from the purchasers to protect themselves from fraud. The problem with this arrangement is the fact that consumers are forced to give up a plethora of information on the Internet, which can readily be stolen by hackers. Therefore, consumers are the ultimate losers under the system affirmed by *Apple*.

The question *Apple* inevitably poses is who should bear the risk of *future* online credit card fraud. Because online sellers require consumers to divulge sensitive personal information as a condition to accepting payment, *consumers* bear the risk of this information being intercepted and reproduced in *future* transactions. The retroactive and proactive dichotomy of "bearing the risk" is not a new problem in the realm of consumer protection.[142] If the consumers have to bear the risk of fraud and are not guaranteed protection when conducting in e-commerce, then, most likely, the consumers will be wary to conduct in Internet sales.[143] Here lies the bone of contention in the *Apple* decision – *consumers* drive the economy, not businesses. If consumers are not purchasing the goods that are offered for sale, then the buyer is not selling, and the economy is suffers. Consumers should be afforded more protection while using the Internet and not subject to the risk of loss when their credit card and/or identity is stolen and then used. Consumer confidence in a market is essential to the market's success and, therefore, the laws should promote – or be interpreted to encourage – consumer confidence in e-commerce. The more consumers feel confortable in making purchases the more buyers and sellers benefit; it is a win-win for both parties to the transaction. The *Apple* decision, while a sound decision as a matter of law, ignored this policy aspect[144] and decided caveat emptor applies to e-commerce, leaving consumers to bear the risk of future fraud at the expense of protecting sellers.

---

141. *Id.*

142. For a discussion about the retroactive problems of current consumer protection laws and a proposition for a more proactive approach to preventing consumer fraud before it occurs, see David Adam Friedman, *Reinventing Consumer Protection*, 57 DEPAUL L. REV. 45 (2007).

143. Kristen Weisse, Comment, *Remedies for Internet Fraud: Consumers Need All the Help They Can Get*, 14 LOY. CONSUMER L. REV. 205, 218-221 (2002).

144. It is important to note that prior to *Apple* the California courts had applied the Song-Beverly Act to non-face-to-face transactions, such as through the mail or over the telephone. Apple Inc. v. Super. Ct., 292 P.3d 883, 889-900 (Cal. 2013). As a matter of law, the California Supreme Court was justified in extending the Act's protection because the Legislature did not explicitly convey its intent; however, as a matter of policy and economics, it is fair to argue the court should have afforded consumers more protection, not subject them increased chances of future fraud.

As a matter of public policy, this situation presents a lose-lose for consumers and sellers alike: consumers are forced to bear the risk, which will – potentially – discourage them from utilizing e-commerce, and sellers will sell less, resulting in lower profits. In order to improve the economy, it would be beneficial for consumers to be afforded more protection to boost their confidence in the market. The increase in confidence will lead to more purchases, which will help both sellers and the economy. As online theft becomes more prevalent and thieves become more sophisticated in their methods for obtaining information to commit credit card and/or identity theft, the *Apple* court's rule clearly opens the door for increased instances of credit card fraud and identity theft. Consumers bear all the risk of purchasing online and such a policy will discourage consumer confidence in the online market, instead of stimulating it by protecting consumers from fraud. A far better policy is to make security standards for credit card companies mandatory and have them absorb more liability from fraudulent transactions.[145]

B. *Legal Implications of Distinguishing Online and Traditional Sales*

The *Apple* dissents point out the potential problems with the majority: a commerce related law does not apply to e-commerce unless this is what the legislature explicitly states.[146] It points out that nowhere in California's Uniform Commercial Code ("Code") does it state that it applies to the transaction of goods on the Internet.[147] Thus, based on the majority's own logic, the Code does not apply to online transactions. The impact of such a solution is frightening: every state would need to enact two different bodies of law – one pertaining to traditional sales and another for online transactions. This solution is clearly undesirable for a variety of reasons. Requiring the legislature to specifically amend every law that applies to traditional credit sales to specifically state that the statutes apply to online sales or enacting online credit card laws that differ from the traditional ones will decrease consumer confidence in the market place and negatively impact their purchasing decisions, not to mention the enormous undertaking

145. *Credit Card Fraud* advocates a method that is molded after the European Union where a public authority oversees the development of security rules. The Article provides that making mandatory security standards, appointing a Data Security Commissioner, establishing incentives for credit card companies to increase, establishing a system of penalties for companies that act in bad faith, and reducing the ability to shift fraud losses downstream would be an advantageous solution to the presently flawed system. *See* Segal, *supra* note 27, at 778-81.

146. *Apple*, 292 P.3d at 889-900.

147. *Id.*

such an overhaul would demand. While consumers will bear the initial harm of this policy, the online sellers will be the ultimate losers. Because consumers will be less confident in purchasing online products there is the possibility that the consumer will forgo the purchase. Thus, sellers would be missing the opportunity for a potential sale and their revenue would likely suffer. In the aggregate, this loss of economic output will harm consumers and sellers. Therefore, it is a lose-lose for both.

Having two separate bodies of laws governing online and traditional sales will only result in confusion that would discourage consumer confidence in the market. It is counter intuitive to have one set of rules apply when a consumer walks into a store to buy a good, but a different set when the same consumer purchases the same good online. Because the Code does not specifically apply to the sale of *online* goods, does *Apple* mean the California legislature must amend California Commercial Code and specifically declare it applies to e-commerce? – In all practical sense, no. While this is an extreme side of the spectrum, it helps illustrate the potential issue of requiring two distinct bodies of laws governing sales.

Furthermore, if the laws differ, then the difference could impact purchasing decisions. For example, one of the major benefits of online sales is convenience; however, if that market becomes subject to more stringent laws that make it a less desirable mode of purchasing goods online, then it is possible that consumers will forego purchasing the goods it intended on purchasing online altogether. The transaction costs of having to physically go into a store might cause the consumer to forego the sale altogether, thereby decreasing the producers sales and the economy at large. On the flip side of the coin, if online transactions are loosely regulated and consumers face ever increasing chances of fraud, then consumers may purchase less on the Internet, which thereby decreases the seller's profits and, in the aggregate, economic productivity of as a whole.[148] The problem requires a balance the costs of fraud between both consumers and sellers; placing the burden on one party will only hurt the economy and, therefore, be detrimental to both.

Consumer protection laws and policies generally seek to protect buyers from fraud in the first instance; however, e-commerce has opened "Pandora's Box" and has only been able try and remedy the fraud after it occurs.[149] Cyber law is no longer in its infancy and its

148. For a discussion of Internet regulations and consumer protection, see Weisse, *supra* note 143, at 216-223.

149. Friedman, *supra* note 142, at 46-51

needs to be streamlined with the body of consumer protection law governing traditional sales.[150] Consumers drive the economy and need to be confident in the security of the Internet market. Different protections applying to traditional and Internet sales will result in consumer confusion, as opposed to consumer confidence. The *Apple* decision impairs consumer confidence by essentially declaring that consumers must post any and all private information on the Internet if a seller desires it.[151] This is a punctuated departure from the present state of law that distinguishes traditional and Internet sales. While it is only possible to speculate on the potential issues that will result from different rules regarding online and traditional sales, it is simply good policy that the same rules apply to the purchase of the same good, no matter the forum.

VI. CONCLUSION

The Internet presented and continues to present obstacles that were unforeseeable when countless statutes were enacted. While it is understandable that special rules should govern the new form of technology that presents unprecedented issues, it is a slippery slope to require an entirely different set of commercial rules to govern e-commerce. Consumer protection against credit card fraud and identity theft occurring on the Internet should be treated legally analogous – if not the same – to those that occur in the course of a traditional sale. If a statute clearly states that a seller cannot require, request, and record consumers' personal information, then it should not matter whether the sale is in person or online, regardless of whether the legislature could have foreseen e-commerce. After all, the legislative intent clearly wanted to do one thing – protect consumers from fraud. Furthermore, if a law's purpose is to protect consumers from credit card fraud then that is exactly what it should do: it should not subject consumers to an *increased* chance that credit card fraud and identity theft might occur in the future. Instead, it should promote consumer confidence and stimulate the economy.

The *Apple* court implemented a policy that diverges from plain meaning of the Song-Beverly Act and the implicit legislative intent. It

150. Fedorek, *supra* note 29, at 10 (explaining the evolution of Cybercrime).

151. The implication of the *Apple* decision is profoundly far more reaching than the court meant it to be. Based on dicta, the Song-Beverly Act's protections *do not apply in any way whatsoever*. Therefore, it is potentially fair game for an online seller to require a social security number as a condition to the sale. While this may protect the seller from fraud, it comes at the expense of the consumer being required to produce said private information and bear the risk of it being intercepted/stolen and fraudulently used.

will be interesting to see how the California courts fill in the questions that *Apple* court left unanswered and how other jurisdictions react. One can only hope that the trend does not catch on and an entirely separate body of law must be specifically legislated. Until then, caveat emptor.