IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS

STEVE McPEAK, KATHERIN MURRAY, TIMOTHY ROLDAN and DARLA YOUNG,	)	
Plaintiffs,	)	**JURY TRIAL DEMANDED**
vs.	)	Case No. 3:14-cv-00899-DRH-DGW
SUPERVALU, INC., a Minnesota corporation,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

NOW COME the Plaintiffs, on behalf of themselves and all others similarly situated, and for their class action complaint state as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action as a result of a breach of the security system of Defendant SUPERVALU, INC. (SuperValu) governing electronic transactions, resulting in compromised security of Plaintiffs' and Class Members' personal financial information. Such personal information included, but upon information and belief was not limited to, the putative Class Members' (hereafter "Class Members") names, credit or debit card number, the card's expiration date, and the card's CVV (a three-digit security code) ("Personal Information").

2. Between June 22nd and July 17th this year, credit and debit cards in its United State stores were compromised, with the result that Personal Information of Plaintiffs and Class Members' Personal Information was used or is at risk of use in fraudulent transactions around the world. Upon information and belief, Defendant operates nearly 1,800 stores nationwide, and Defendant's security failures affected the credit and debit card of millions of customers,

including Plaintiffs and Class Members. Defendant has publicly stated: "Approximately 40 million credit and debit card accounts may have been impacted . . . ."

3. Defendant further confessed that, if Plaintiffs and Class Members seek to protect themselves from further damages resulting from Defendant's security failures by adding a fraud alert to Plaintiffs' and Class Members' credit report files, it "may delay your ability to obtain credit."

4. Upon information and belief, the security breach and theft of Personal Information was caused by Defendant's violations of its obligations to abide by the best practices and industry standards concerning the security of its payment processing systems and the computers associated therewith as set forth, for example, in Payment Card Industry Security Standards Council Data Security Standards ("PCI DSS") and the decisions of the Federal Trade Commission ("FTC") concerning protection of consumer financial information.

5. After learning of the security breach, Defendant failed to notify Plaintiffs and the putative Classes in a timely manner and failed to take other reasonable steps to inform them of the nature and extent of the breach. As a result, Defendant prevented Plaintiffs and the putative Class Members from protecting themselves from the breach and caused Plaintiffs and Class Members to suffer financial loss.

6. Plaintiffs, on behalf of themselves and all others similarly situated, assert the following claims: Violations of the Stored Communications Act ("SCA"), 18 U.S.C. § 2702; negligence; breach of implied contract; violations of the Missouri Merchandising Practices Act ("MMPA"), Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which Defendant conducts business; and violations of the Illinois Personal Information

Protection Act ("IPIPA"), 815 ILCS 530/1, and the substantially similar statutes of the other states in which Defendant conducts business.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, which confers upon the Court original jurisdiction over all civil actions arising under the laws of the United States, and pursuant to 18 U.S.C. § 2707. This Court has supplemental jurisdiction over Plaintiffs' and Class Members' state law claims under 28 U.S.C. § 1367.

8. In addition, this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all Members of the putative Classes are in excess of $5,000,000.00, exclusive of interest and costs, and many of the Members of the putative Classes are citizens of different states than Defendant. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d).

9. Venue is properly set in this District pursuant to 28 U.S.C. § 1391(b) since Defendant transacts business and is found within this judicial district. Likewise, a substantial part of the events giving rise to the claim occurred within this judicial district.

PARTIES

10. Plaintiff Steve McPeak is domiciled in Stookey Township, St. Clair County, Illinois and is a citizen of Illinois. McPeak shopped at Defendant's stores in St. Clair County, Illinois and swiped his debit card through a Defendant pin pad terminal. On information and belief McPeak's Personal Information was compromised as a result of Defendant's security failures. As a result of such compromise, McPeak suffered losses and damages in an amount yet to be completely determinable as such losses and damages are ongoing.

11. Plaintiff Katherin Murray is domiciled in Woodriver, Illinois and is a citizen of Madison County, Illinois. Murray shopped at Defendant's stores in Woodriver, Illinois and swiped her debit card through a Defendant pin pad terminal. On information and belief Murray's Personal Information was compromised as a result of Defendant's security failures. As a result of such compromise, Murray suffered losses and damages in an amount yet to be completely determined as such losses and damages are ongoing.

12. Plaintiff Timothy Roldan is domiciled in Creve Coeur, Missouri and is a citizen of Missouri. Roldan shopped at Defendant's locations in St. Louis County, Missouri, and swiped his debit card through Defendant's pin pad terminal(s). On information and belief Roldan's Personal Information was compromised as a result of Defendant's security failures. As a result of such compromise, Roldan suffered losses and damages in an amount yet to be completely determined as such losses and damages are ongoing.

13. Plaintiff Darla Young is domiciled in Lake St. Louis, Missouri and is a citizen of Missouri. Young shopped at Defendant's locations in St. Louis and St. Charles Counties, Missouri, and swiped her debit card through Defendant's pin pad terminal(s). On information and belief Young's Personal Information was compromised as a result of Defendant's security failures. As a result of such compromise, Young suffered losses and damages in an amount yet to be completely determined as such losses and damages are ongoing.

14. Defendant is a corporation organized under Minnesota law with its headquarters and principal place of business in Minneapolis, Minnesota.

FACTUAL BACKGROUND

15. Upon information and belief, Defendant's data breach has impacted thousands of its stores and potentially affected retail chains recently sold by the company in two dozen states.

16. Hackers accessed a network that processes SuperValu transactions, with account numbers, expiration dates, card holder names and other information, according to the Defendant.

17. Those systems are still being used by the stores sold off by SuperValu last year for $3.3 billion, potentially opening up customer data at those stores as well.

18. Defendant claims that the breach is limited to between June 22th and July 17th of this year. Minimally, the Defendant has admitted that the cards from which data may have been stolen were used at 180 SuperValu stores and liquor stores run under the Cub Foods, Farm Fresh, Hornbacher's, Shop 'n Save and Shoppers Food & Pharmacy names. Data may also have been stolen from 29 franchised Cub Foods stores and liquor stores. Those stores in North Dakota, Minnesota, Illinois, Virginia, North Carolina, Maryland and Missouri.

19. Plaintiffs herein, shopped at the Defendant's stores in St. Clair and Madison Counties, Illinois and St. Louis and St. Charles Counties in Missouri.

20. Importantly, the Defendant has noted that a related criminal intrusion occurred at the chain stores it sold to Cerebus Capital Management in March 2013, stores that SuperValu continues to supply with information technology services. Those stores include Albertsons, Acme, Jewel-Osco, Shaw's and Star Market — and related Osco and Sav-on in-store pharmacies in two dozen states.

21. Upon information and belief, the Defendant accepts customer payments for

purchase through credit and debit cards issued by members of the payment card industry ("PCI") such as Visa or MasterCard.

22. In 2006, the PCI members established a Security Standards Counsel ("PCI SSC") as a forum to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

23. The PCI DSS provides, "If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard." Defendant, or course, is a merchant that accepts payment cards.

24. The PCI DSS requires a merchant to:

a. **Assess**—identify cardholder data, take inventory of IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data.

b. **Remediate**—fix vulnerabilities and do not store cardholder data unless needed.

c. **Report**—compile and submit required remediation validation records (if applicable) and submit compliance reports to the acquiring bank and card brands with which a merchant does business.

25. Additionally, since 1995, the FTC has been studying the manner in which online entities collect and use personal information and safeguards to assure that online data collection practice is fair and provides adequate information privacy protection. The result of this study is the FTC Fair Information Practice Principles. The core principles are:

a. **Notice/Awareness**--Consumers should be given notice of an entity's information practices before any personal information is collected from them. This requires that companies explicitly notify of some or all of the following:

- Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected;
- Whether the provision of the requested data is voluntary or required; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

b. **Choice/Consent**--Choice and consent in an online information-gathering sense means giving consumers options to control how their data is used with respect to secondary uses of information beyond the immediate needs of the information collector to complete the consumer's transaction.

c. **Access/Participation**--Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

d. **Integrity/Security**--Information collectors should ensure that the data they collect is accurate and secure. They should improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors should keep their data secure by protecting against both internal and external security threats. They should limit access within their company to only necessary

employees to protect against internal threats, and they should use encryption and other computer-based security systems to stop outside threats.

e. **Enforcement/Redress--**In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures. The FTC identifies three types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement, which can include civil and criminal penalties levied by the government.

26. On information and belief, Defendant failed to adequately analyze its computer systems for vulnerabilities that could expose cardholder data. Defendant further failed to fix the vulnerabilities in its computer systems which allowed Plaintiffs' and Class Members' Personal Information to become compromised.

27. Additionally, on information and belief, Defendant unlawfully collected consumer financial data for marketing purposes beyond the needs of specific transactions, in order to accrue financial benefit at the risk and likelihood of compromising consumers' Personal Information.

28. As a result, Defendant allowed Personal Information connected with thousands of consumers' credit cards and debit cards, including credit cards and debit cards of Plaintiffs and Class Members, to become compromised for a minimum period between June 22nd and July 17th of this year.

29. Plaintiffs and Class Members are subject to continuing damage from having their Personal Information comprised as a result of Defendant's inadequate systems and failures. Such damages include, among other things, out-of-pocket expenses incurred to mitigate the

increased risk of identity theft and or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit/debit cards of Defendant's customers by identity thieves who wrongfully gained access to the Personal Information of Plaintiffs and the Classes.

CLASS ACTION ALLEGATIONS

30. Plaintiffs bring this action on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following three (3) multi-state classes:

> All persons who shopped at Defendant's locations, whose Personal Information was subject to Defendant's security failures and who suffered damages in the loss of time and use of their credit and debit cards until such time as replacement cards could be obtained.
>
> All persons who shopped at Defendant's locations, whose Personal Information was subject to Defendant's security failures and who suffered damages in the amount of fraudulent charges / unauthorized withdrawals made to their credit and/or debit cards or suffered damages in the amount of overdraft charges made to their credit and/or debit cards.
>
> All persons who shopped at Defendant's locations, whose Personal Information was subject to Defendant's security failures and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendant's security failures.

Excluded from the Classes are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors.

31. The Members of the Classes are so numerous that joinder of all Members is impracticable. Defendant has publicly admitted that thousands of credit and/or debit cards may have been compromised, and the Members of the Classes are geographically dispersed.

Disposition of the claims of the proposed Classes in a class action will provide substantial benefits to both the parties and the Court.

32. The rights of each member of the proposed Classes were violated in a similar fashion based upon Defendant's uniform wrongful actions and/or inaction.

33. The following questions of law and fact are common to each proposed Class Member and predominate over questions that may affect individual Class Members:

a. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' private financial information;

b. Whether Defendant properly implemented its purported security measures to protect consumers' private financial information from unauthorized capture, dissemination and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the security breach after it first learned of the same;

d. Whether Defendant's delay in informing consumers of the security breach was unreasonable;

e. Whether Defendant's method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of the same was unreasonable;

f. Whether Defendant's conduct violated the Stored Communications Act, 18 U.S.C. § 2702;

g. Whether Defendant breached an implied contract with Class Members;

h. Whether Defendant's conduct violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantively similar statutes of the other states where Defendant conducts business;

i. Whether Defendant's conduct violated the Illinois Personal Information Protection Act, 815 ILCS 530/1, and the substantially similar statutes of the other states in which Defendant conducts business; and

j. Whether Plaintiffs and others Members of the Classes are entitled to compensation, monetary damages, equitable relief and injunctive relief, and, if so, the nature and amount of such relief.

34. Plaintiffs' claims are typical of the claim of absent Class Members. If brought individually, the claim of each Class Member would necessarily require proof of the same material and substantive facts, and seek the same remedies.

35. The Plaintiffs are willing and prepared to serve the Court and the proposed Classes in a representative capacity. The Plaintiffs will fairly and adequately protect the interest of the Classes and have no interests adverse to, or which directly and irrevocably conflicts with, the interests of other Members of the Classes. Further, Plaintiffs have retained counsel experienced in prosecuting complex class action litigation.

36. Defendant has acted or refused to act on grounds generally applicable to the proposed Classes, thereby making appropriate equitable relief with respect to the Classes.

37. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual claims by the Class Members are impractical, as the costs of prosecution may exceed what any Class Member has at stake.

38. Members of the Classes are readily ascertainable through Defendant's records of the purchases made at its stores.

39. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incomparable standards of conduct for Defendant. Moreover, adjudications with respect to individual Class Members would, as a practical matter, be dispositive of the interests of other Class Members.

CAUSES OF ACTION

COUNT I – VIOLATION OF THE FEDERAL STORED COMMUNICATIONS ACT, 18 U.S.C. § 2702

40. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

41. The Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 at 3557.

42. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

43. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* at § 2510(15).

44. Through its payment processing equipment, Defendant provides an "electronic communication service to the public" within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability that enables them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

45. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Defendant was aware that customers' Personal Information had been compromised, Defendant has knowingly divulged customers' private financial information that was communicated to financial institutions solely for customers' payment verification purposes, while in electronic storage in Defendant's payment system.

46. Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

47. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. § 2711(2).

48. An "electronic communications systems" is defined by the SCA as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(4).

49. Defendant provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photooptical or photoelectric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer private financial information.

50. By failing to take commercially reasonable steps to safeguard sensitive private financial information, Defendant has knowingly divulged customers' private financial information that was carried and maintained on Defendant's remote computing service solely for the customer's payment verification purposes.

51. As a result of Defendant's conduct described herein and its violations of Section 2702(a)(1) and (2)(A), Plaintiffs and putative Class Members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiffs, on their own behalf and on behalf of the putative Classes, seek an order awarding themselves and the Classes the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

COUNT II – NEGLIGENCE

52. Plaintiffs repeat, reallege, and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

53. Upon coming into possession of Plaintiffs' and Class Members' Personal Information, i.e., private, non-public, sensitive financial information, Defendant had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen.

54. Defendant also had a duty to timely disclose to Plaintiffs and Class Members that a breach of security had occurred and their Personal Information pertaining to their credit cards and/or debit cards had been compromised, or was reasonably believed to be compromised.

55. Defendant also had a duty to put into place internal policies and procedures designed to detect and prevent the theft or dissemination of Plaintiffs' and Class Members' Personal Information.

56. Defendant, by and through its above negligent acts and/or omissions, breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding their Personal Information which was in Defendant's possession, custody, and control.

57. Defendant, by and through its above negligent acts and or omissions, further breached its duty to Plaintiffs and Class Members by failing to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of Plaintiffs and Class Members' Personal Information.

58. Defendant, by and through its above negligent acts and or omissions, breached its duty to timely disclose the fact that Plaintiffs' and Class Members' Personal Information had been or was reasonable believed to be have been compromised.

59. Defendant's negligent and wrongful breach of its duties owed to Plaintiffs and Class Members, their Personal Information would not have been compromised.

60. Plaintiffs' and Class Members' Personal Information was compromised and/or stolen as a direct and proximate result of Defendant's breach of its duties as set forth herein.

61. Plaintiffs and Class Members have suffered actual damages including, but not limited to, having their personal information compromised, incurring time and expenses in

cancelling their debit and/credit cards, activating new cards and re-establishing automatic payment authorizations from their new cards, and other economic and non-economic damages, including irrecoverable losses due to unauthorized charges on their credit/debit cards.

COUNT III -- BREACH OF IMPLIED CONTRACT

62. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

63. Plaintiffs and Class Members were required to provide Defendant with their Personal Information in order to facilitate their credit card and/or debit card transactions.

64. Implicit in this requirement was a covenant requiring Defendant to take reasonable efforts to safeguard this information and promptly notify Plaintiffs and Class Members in the event their information was compromised.

65. Similarly, it was implicit that Defendant would not disclose Plaintiffs' and Class Members' Personal Information.

66. Notwithstanding its obligations, Defendant knowingly failed to safeguard and protect Plaintiffs' and Class Members' Personal Information. To the contrary, Defendant allowed this information to be disseminated to unauthorized third parties.

67. Defendant's above wrongful actions and/or inaction breached its implied contracts with Plaintiffs and Class Members, which in turn directly and/or proximately caused Plaintiffs and Class Members to suffer substantial injuries.

COUNT IV – VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT AND SUBSTANTIALLY SIMILAR STATUTES OF THE OTHER STATES WHERE DEFENDANT DOES BUSINESS

68. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

69. Defendant violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which it conducts business by failing to properly implement adequate, commercially reasonable security measures to protect customers' private financial information, and by failing to immediately notify affected customers of the nature and extent of the security breach.

70. Defendant's fraudulent and deceptive omissions and misrepresentations regarding the company's security measures to protect customers' private financial information and the extent of the breach of those security measures were intended to deceive and induce Plaintiffs and the putative Class Members' reliance on Defendant's misrepresentations that their financial information was secure and protected when using debit and credit cards to shop at Defendant stores.

71. Defendant's unlawful misrepresentations and omissions occurred in the course of conduct involving trade or commerce.

72. Defendant's unlawful misrepresentations and omissions were material because Plaintiffs and the other putative Class Members, if they had known the truth, would not have risked compromising their private financial information by using their debit or credit cards at Defendant stores. Plaintiffs and the other putative Class Members would consider the omitted and misrepresented material facts important in making their purchasing decisions.

73. Defendant's unlawful misrepresentations and omissions damaged Plaintiffs and the other putative Class Members because Plaintiffs and Class Members would not have chosen to expose their private financial information to a security breach and subsequent exploitation by the defrauders.

74. Plaintiffs, individually and on behalf of the putative Classes, seek an order requiring Defendant to pay: monetary and punitive damages for the conduct described herein; three years of credit card fraud monitoring services for Plaintiffs and Members of the putative Classes; and the reasonable attorney's fees and costs of suit of Plaintiffs and Class Members; together with all such other and further relief as may be just.

COUNT V -- VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT AND SUBSTANTIALLY SIMILAR STATUTES OF THE OTHER STATES WHERE DEFENDANT DOES BUSINESS

75. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

76. At all times relevant hereto, there was in full force and effect the Illinois Personal Information Protection Act (IPIPA), 815 ILCS 530/1, together with other relevant state statutes providing that any data collector that owns or licenses personal information concerning a state resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach.

77. The relevant statutes provide that disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

78. Defendant is a data collector within the meaning of the IPIPA and other relevant statutes.

79. Defendant came into possession of Plaintiffs' and Class Members' personal information, as that is defined by the IPIPA and other relevant statutes.

80. Defendant had a duty to disclose in the most expedient time possible and without unreasonable delay the breach of the security of the system data.

81. Defendant, through its actions and/or omissions, failed to disclose in the most expedient time possible and without unreasonable delay the breach of the security of the system data.

82. Defendant's failure to timely disclose is a violation of the IPIPA and other relevant statutes.

83. Plaintiffs and Class Members request that an injunction be issued to require Defendant to comply with the IPIPA and other relevant statutes.

84. To the extent that a violation of the IPIPA and other relevant statutes also constitutes a violation of pertinent state consumer protection laws, *see, e.g.*, Section 20 of the IPIPA, providing that a violation of this IPIPA constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, Defendant's violation of the IPIPA and other pertinent statutes is also a violation of pertinent state consumer protection law.

JURY TRIAL DEMAND

Plaintiffs and class members demand a jury trial as to all claims and issues triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Members of the proposed Classes pray that this Honorable Court do the following:

A. Certify the matter as a class action pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class Members;

B. Designate Plaintiffs as representative of the Classes and the undersigned counsel as Class Counsel;

C. Award Plaintiffs and the Classes compensatory and punitive damages in an amount to be determined by the trier of fact;

D. Award Plaintiffs and the Classes statutory interest and penalties;

E. Award Plaintiffs and the Classes appropriate injunctive and/or declaratory relief;

F. Award Plaintiffs and the Classes their costs, prejudgment interest, and attorney fees; and

G. Grant such other relief as is just and proper.

Respectfully submitted,
THE DRISCOLL FIRM, P.C.

By: /s/John J. Driscoll
John J. Driscoll, #6276464
211 N. Broadway, 40th Floor
St. Louis, Missouri 63102
314-932-3232 telephone
314-932-3233 facsimile

JS 44 (Rev. 12/12)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

STEVE McPeak, Katherin Murray, Timothy Roldan and Darla Young

(b) County of Residence of First Listed Plaintiff St. Clair Co., IL
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
John J. Driscoll, Esq.
The Driscoll Firm, PC, 211 N. Broadway, 40th Fl, St. Louis, MO 63102
(314) 932-3232

DEFENDANTS

SUPERVALU, INC., a Minnesota corporation,

County of Residence of First Listed Defendant Minneapolis, MN
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
18 USC 2702

Brief description of cause:
Violation of the Federal Stored Communications Act

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE
08/15/2014

SIGNATURE OF ATTORNEY OF RECORD
/s/ John J. Driscoll

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE