

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

MERRICK BANK CORPORATION,)	
)	
Plaintiff,)	
)	
v.)	
)	
)	Case No.
SAVVIS, INC., and SAVVIS COMMUNICATIONS)	
CORPORATION,)	
)	
)	
Defendants.)	
)	
)	

COMPLAINT

NOW COMES plaintiff, Merrick Bank Corporation (“Merrick”), by and through undersigned counsel, and for its complaint respectfully represents to the Court as follows:

THE PARTIES

1. Merrick Bank Corp. is a Utah corporation with its principal place of business at 10705 South Jordan Gateway, South Jordan, Utah 84095. Merrick is a citizen of Utah.

2. Savvis, Inc. is a Delaware corporation with its principal place of business at 1 Savvis Parkway, Town & Country, Missouri 63017. Savvis, Inc. is a citizen of Delaware and a citizen of Missouri.

3. Savvis Communications Corp. is a Missouri corporation with its principal place of business at 1 Savvis Parkway, Town & Country, Missouri 63017. Savvis Communications Corporation is a citizen of Missouri.

JURISDICTION AND VENUE

4. There is complete diversity of citizenship in this action between the parties and the amount in controversy exceeds \$75,000, exclusive of interests and costs. Consequently, jurisdiction may properly be asserted in this case under the provisions of 28 U.S.C. § 1332.

5. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) by virtue of the fact that all of the defendants reside in this district.

FACTUAL BACKGROUND

Relevant Parties to and Responsibilities in connection with Card Transactions

6. Merrick Bank Corporation (“Merrick”) is a member bank of the Visa U.S.A., Inc. (“VISA”) and MasterCard Worldwide (“MasterCard”) networks. Visa and MasterCard (collectively, the “Associations”) are associations of bank and bank-like entities that participate in the debit and credit card (collectively “Cards”) payment system whereby cardholders are enabled to purchase goods and services through presentation of Cards (or through furnishing Card numbers in card-not-present transactions conducted via the internet or by telephone) (such transactions referred to herein as “Card Transactions”).

7. A Card Transaction involves four essential primary parties: (1) a cardholder, (2) an issuing bank, (3) an acquiring bank, and (4) a merchant. An issuing bank is the Association member bank that has determined to issue a Card to a cardholder. An acquiring bank, sometimes referred to herein as an “acquirer,” is the Association member bank that (i) has established a contractual relationship with the merchant pursuant to which the merchant is enabled to accept Cards as a means of payment and (ii) receives payment for the goods or services from the cardholder’s issuing bank which payment it forwards to the merchant.

8. When a cardholder initiates a Card Transaction to purchase goods or services from a merchant, the cardholder’s account information is sent electronically by the merchant to

the issuing bank for authorization (verification that the issuing bank will extend the credit necessary for the purchase). Upon nearly instantaneous receipt of such authorization, the merchant accepts the Card as a means of payment and later (usually that evening) electronically forwards data to the issuing bank seeking payment (or settlement) for the goods or services sold. The authorization and settlement functions are conducted through Association systems, sometime referred to as “interchange.”

9. Many acquiring banks retain third party Independent Sales Organizations (“ISOs”) and Card processors (“Processors”) in connection with their Card businesses. ISOs, generally, are sales forces that solicit merchants to contract with acquiring banks with which the ISO is aligned, and provide maintenance and servicing to such merchants. Processors process, on behalf of the acquiring bank, the authorization and settlement functions described above. Frequently one entity is both an ISO and a Processor, and frequently an acquiring bank will begin a relationship with a Processor through contracting with an ISO that works with a particular Processor.

10. In order to process authorizations and settlements, Processors must have access to the Associations’ interchange systems and must, of necessity, have access to sensitive cardholder data (such as, for example, cardholder name, account number and other data stored on the Card’s magnetic stripe).

11. The Associations, cognizant that many acquirers outsource authorization and settlement, have promulgated rules and regulations related to the activities of Processors, including, for example, rules that require acquirers to (i) register their Processors with the Associations, (ii) commit to ensure that their Processors process in strict compliance with Association operating regulations (iii) work only with Processors whose systems have been audited and certified compliant with Association system standards, and (iv) agree to reimburse

the Associations for all losses suffered by the Associations as a result of wrongdoing by such registered Processors.¹

Merrick Bank and its Processor

12. Merrick is an acquiring bank for approximately 125,000 merchants. In or about January 2004, Merrick entered into an agreement with CardSystems Solutions, Inc. (“CardSystems”), pursuant to which CardSystems would perform both ISO and Processor services for Merrick.

13. Notwithstanding execution of an agreement between them in or about January 2004, Merrick would not permit CardSystems to act as either ISO or Processor until Merrick was satisfied that CardSystems was compliant with all Association rules and regulations related to Processors, including the rules and regulations related to the security of the Processor’s systems and to the storage of cardholder data.

14. In or about January, 2004, Visa had in place the Cardholder Information Security Program (“CISP”) which set forth the specific network infrastructure, policies and operational procedures Visa required of Processors in an effort to ensure Card Transaction security and which required that Processors be certified as CISP compliant by a Visa approved systems auditor.

15. MasterCard had similar rules to CISP relating to Card Transaction security with respect to which Processors were required to comply.

16. Because CardSystems was not certified as CISP compliant in January, 2004, Merrick would not allow CardSystems to process any Card Transactions until it obtained such certification.

¹ Although not relevant to this matter, acquiring banks also must register with the Associations each of the ISO’s with which they do business.

17. Merrick was satisfied that a CISP compliant Processor also would be compliant with MasterCard's Card Transaction security regulations.

18. In January, 2004, Merrick also was negotiating a potential transaction with another acquiring bank whereby Merrick would assume approximately ten to fifteen ISO relationships (the "ISO Acquisition Agreement"), most of which ISOs were processed by CardSystems.

19. By in or about April, 2004, Merrick had agreed on all material terms of the ISO Acquisition Agreement with the assigning acquiring bank but would not execute the agreement until CardSystems had been certified CISP compliant by a Visa authorized auditor.

Savvis Audit of CardSystems

20. Savvis, Inc. ("Savvis"), formerly known as Savvis Communications Corporation, holds itself out to the public as a "global leader in IT infrastructure services for business applications" with expertise in information security.

21. At all times relevant herein, Savvis was certified by Visa as a professional service firm competent to audit and assess a company's compliance with CISP.

22. Savvis was retained by CardSystems for the express purpose of obtaining certification that its systems were CISP compliant. Initially, in or about 2003, CardSystems retained Cable & Wireless, Inc. ("Cable & Wireless") for such certification. Although Cable & Wireless submitted a Report on Compliance ("ROC") in or about December 2003, the Cable & Wireless ROC was not accepted or relied upon by Visa as proof of CardSystem's CISP compliance. Thereafter, in or about January, 2004, Savvis purchased the Processor auditing assets of Cable & Wireless. Savvis subsequently agreed to provide CardSystems with a ROC.

23. In June of 2004, Savvis issued a Report on Compliance to CardSystems and Visa which summarized its findings and conclusions with respect to CardSystems' CISP compliance.

Savvis concluded that CardSystems had implemented sufficient security solutions and operated in a manner consistent with industry best practices and the intent of CISP, and thus recommended that Visa recognize CardSystems systems as in "Full Compliance" with CISP.

24. Shortly thereafter, CardSystems was officially listed as CISP compliant by Visa.

25. Upon learning the conclusions contained in the Savvis ROC, Merrick allowed CardSystems to act as its Processor.

26. Additionally, in reliance on the Savvis ROC, in July, 2004, Merrick executed and completed the ISO Acquisition Agreement.

The CardSystems Data Breach

27. In May of 2005, less than one year after Savvis issued the clean CardSystems ROC, CardSystems notified Merrick that its computer systems had been breached by hackers. A forensic investigation of the security breach conducted immediately after CardSystems's discovery of the hack revealed that on numerous occasions over the course of the preceding several months hackers were able to export credit card account numbers and other personally identifiable cardholder data from CardSystems's computer systems. The report estimated that as many as 40 million individual Card account numbers may have been compromised as a result of the security breach.

28. CardSystems was vulnerable to the breach because its systems designed to prevent unauthorized intrusions ("firewalls") were not CISP compliant and because, once the hackers had penetrated the substandard firewalls, they were able to access usable data as a result of CardSystems long standing practice of improperly retaining unencrypted Card Transaction data on its servers in violation of CISP standards.

29. At the time that Savvis issued its ROC confirming CardSystems's CISP compliant status, CardSystems had, in fact, according to the forensic report, been improperly and continuously storing unencrypted Card Transaction data on its servers for over five years.

30. CardSystems inadequate firewalls, improper data retention and failure to encrypt data were all obvious failures to comply with CISP.

31. Consequently, Savvis's ROC indicating that CardSystems was in full compliance with CISP was false and misleading.

32. Merrick has incurred approximately \$16 million in damages as a result of the data security breach consisting of payments to the Associations (that were in turn delivered by the Associations to issuing banks that had suffered fraud loss as a result of the security breach), payments of assessments to the Associations for registering a Processor that was not compliant with the Associations' data security Rules, and legal fees incurred in security breach related matters.

COUNT I - NEGLIGENCE

33. Merrick incorporates by reference the preceding numbered Paragraphs 1 through 32 as if fully set forth herein.

34. Savvis, at all relevant times a professional service company certified by Visa to assess compliance with CISP, owes a duty of care to acquiring banks such as Merrick to audit Processors in a professional and reasonably prudent manner.

35. Savvis provided the ROC to VISA knowing and intending that VISA would provide the ROC and its recommendation of "Full Compliance" with CISP to banks, like Merrick, then considering a direct contractual relationship with CardSystems and that VISA and such banks would rely thereon.

36. Savvis provided the ROC to VISA for the express purpose and with knowledge that Visa would publish the ROC to the Card industry through the Visa web site and that acquirers needing the services of a Processor (and diligently taking all steps possible to engage only a CISP compliant Processor) would rely on the audit in determining that CardSystems met such standards.

37. In preparing the ROC and delivering the ROC to VISA, Savvis intended that the ROC would directly influence decisions made by Merrick and banks in a like position to Merrick with regard to CardSystems and the ability of CardSystems to safely participate in the Association networks.

38. When Savvis issued the ROC, it was reasonably foreseeable that Merrick, as an acquiring bank for which CardSystems was to act as a Processor, would rely thereon.

39. Indeed, as a certified and experienced auditor for CISP compliance, Savvis knew, or reasonably should have known, that its certification of CardSystems was directly for the benefit and guidance of those acquiring banks, such as Merrick, with which CardSystems sought to establish a processing relationship.

40. Savvis breached its duty to Merrick by failing to audit CardSystems in a competent and professional manner. Specifically, Savvis breached its duty to competently and professionally assess CardSystems' compliance with CISP by certifying CardSystems as CISP compliant even though CardSystems had substandard firewalls, was retaining cardholder account information it was not permitted to retain, and was retaining data in unencrypted format, all in clear violation of CISP.

41. Merrick would not have allowed CardSystems to process its merchants' Card Transactions but for Savvis' audit finding CardSystems to be in full compliance with CISP.

42. Merrick's reasonable and detrimental reliance on Savvis's audit and ROC directly and substantially caused Merrick harm. Specifically, Savvis exposed Merrick to liability for CardSystems's inadequate Card Transaction security through its negligent audit of CardSystems, resulting in Merrick paying millions of dollars in damages.

WHEREFORE, plaintiff Merrick prays that this court enter judgment against defendants in an amount to be determined at trial, plus interest and costs, and for such other and further relief as this court deems just and proper.

COUNT II – NEGLIGENT MISREPRESENTATION

43. Merrick incorporates by reference the preceding numbered Paragraphs 1 through 42 as if fully set forth herein

44. Savvis issued the ROC stating that CardSystems was in full compliance with CISP. As CardSystems was operating with substandard firewalls, retaining account information, and retaining it in an unencrypted manner, it was in fact operating in direct contravention of CISP. Savvis' ROC was therefore false and misleading.

45. Savvis failed to use reasonable care and competence in representing that CardSystems was CISP compliant when in fact it was not.

46. As a certified and experienced auditor of computer systems for data security purposes and as a Visa certified CISP auditor, Savvis knew, or reasonably should have known, that its certification of CardSystems was directly for the benefit and guidance of those acquiring banks, such as Merrick, with which CardSystems sought to establish a processing relationship.

47. Moreover, Savvis knew, or reasonably should have known, that CardSystems would immediately supply the findings in the ROC to acquiring banks for which it processed and to acquiring banks, like Merrick, with which CardSystems sought to establish a processing

relationship and that these acquiring banks would necessarily rely on Savvis's representation that CardSystems was CISP compliant.

48. Merrick justifiably relied on Savvis' ROC to its detriment.

49. Specifically, Savvis' failure to exercise reasonable care or competence in undertaking the CardSystems audit and in communicating its incorrect findings caused Merrick substantial harm. Savvis exposed Merrick to liability for CardSystems's inadequate Card Transaction security through its negligent misrepresentations of CardSystems CISP compliance, resulting in Merrick paying millions of dollars in damages.

WHEREFORE, plaintiff Merrick prays that this court enter judgment against defendants in an amount to be determined at trial, plus interest and costs, and for such other and further relief as this court deems just and proper.

Respectfully Submitted,

OF COUNSEL:
Daniel G. Gurfein, Esq.
Mario Aieta, Esq.
James Regan, Esq.
SATTERLEE STEPHENS BURKE &
BURKE LLP
230 Park Avenue
New York, NY 10169

By: /s/ Joseph P. Whyte
Heyl, Royster, Voelker & Allen by:
Joseph P. Whyte, #5424
Suite 100
Mark Twain Plaza III
105 West Vandalia
P.O. Box 467
Edwardsville, Illinois 62025
Telephone - (618) 656-4646
Fax - (618) 656-7940

United States District Court

EASTERN DISTRICT OF MISSOURI

MERRICK BANK CORPORATION,
(Plaintiff)

SUMMONS IN A CIVIL CASE

v.

CASE NUMBER:

SAVVIS, INC. and SAVVIS
COMMUNICATIONS CORPORATION,
(Defendants)

TO: SAVVIS, INC.
c/o CT Corporation System
120 S. Central Avenue
Clayton, Missouri 63105

YOU ARE HEREBY SUMMONED and required to serve upon PLAINTIFF'S ATTORNEY (name and address)

Joseph P. Whyte
Heyl, Royster, Voelker & Allen
105 W. Vandalia, Suite
Edwardsville, Illinois 62025

an answer to the complaint which is herewith served upon you, within 20 days after service of this summons upon you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint. You must also file your answer with the Clerk of this Court within a reasonable period of time after service.

CLERK

DATE

(BY) DEPUTY CLERK

AO 440 (Rev. 10/93) Summons in a Civil Action

RETURN OF SERVICE

Service of the Summons and Complaint was made by met	DATE
NAME OF SERVER (PRINT)	TITLE

Check one box below to indicate appropriate method of service

- Served personally upon the defendant. Place where served:

- Left copies thereof at the defendant's dwelling house or usual place of abode with a person of suitable age and discretion then residing therein.
Name of person with whom the summons and complaint were left:

- Returned unexecuted:

- Other (specify):

STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on _____
Date

_____ Signature of Server

_____ Address of Server

(1) As to who may serve a summons see Rule 4 of the Federal Rules of Civil Procedure.

United States District Court

EASTERN DISTRICT OF MISSOURI

MERRICK BANK CORPORATION,
(Plaintiff)

SUMMONS IN A CIVIL CASE

v.

CASE NUMBER:

SAVVIS, INC. and SAVVIS
COMMUNICATIONS CORPORATION,
(Defendants)

TO: SAVVIS COMMUNICATIONS CORPORATION
c/o CT Corporation System
120 S. Central Avenue
Clayton, Missouri 63105

YOU ARE HEREBY SUMMONED and required to serve upon PLAINTIFF'S ATTORNEY (name and address)

Joseph P. Whyte
Heyl, Royster, Voelker & Allen
105 W. Vandalia, Suite
Edwardsville, Illinois 62025

an answer to the complaint which is herewith served upon you, within 20 days after service of this summons upon you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint. You must also file your answer with the Clerk of this Court within a reasonable period of time after service.

CLERK

DATE

(BY) DEPUTY CLERK

AO 440 (Rev. 10/93) Summons in a Civil Action

RETURN OF SERVICE

Service of the Summons and Complaint was made by met	DATE
NAME OF SERVER (PRINT)	TITLE

Check one box below to indicate appropriate method of service

- Served personally upon the defendant. Place where served:

- Left copies thereof at the defendant's dwelling house or usual place of abode with a person of suitable age and discretion then residing therein.
Name of person with whom the summons and complaint were left:

- Returned unexecuted:

- Other (specify):

STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on _____
Date

_____ *Signature of Server*

_____ *Address of Server*

(1) As to who may serve a summons see Rule 4 of the Federal Rules of Civil Procedure.