

1 SPENCER HOSIE (CA Bar No. 101777)  
 shosie@hosielaw.com  
 2 BRUCE WECKER (CA Bar No. 078530)  
 bwecker@hosielaw.com  
 3 GEORGE F. BISHOP (CA Bar No. 89205)  
 gbishop@hosielaw.com  
 4 HOSIE McARTHUR LLP  
 One Market, 22nd Floor  
 5 San Francisco, CA 94105  
 6 (415) 247-6000 Tel.  
 (415) 247-6001 Fax  
 7

8 ROBERT J. YORIO (CA Bar No. 93178)  
 yorio@carrferrell.com  
 9 CARR & FERRELL LLP  
 2200 Geng Road  
 10 Palo Alto, CA 94303  
 (650) 812-3400 Tel.  
 11 (650) 812-3444 Fax

12 Attorneys for Plaintiff  
 13 PRIVASYS, INC.

14 UNITED STATES DISTRICT COURT  
 15 FOR THE NORTHERN DISTRICT OF CALIFORNIA  
 16 SAN FRANCISCO DIVISION

17 PRIVASYS, INC.

18 Plaintiff,

19 v.

20 AMERICAN EXPRESS COMPANY and  
 21 AMERICAN EXPRESS TRAVEL RELATED  
 22 SERVICES COMPANY, INC.,

23 Defendants.

Case No. \_\_\_\_\_

**ORIGINAL COMPLAINT AND  
 DEMAND FOR JURY TRIAL**

1 Plaintiff PrivaSys, Inc. (“PrivaSys” or “Plaintiff”) hereby files its complaint against  
2 Defendants American Express Company and American Express Travel Related Services  
3 Company, Inc., (collectively “American Express” or “Defendants”) for patent infringement.  
4 For its complaint, Plaintiff alleges, on personal knowledge as to its own acts and on  
5 information and belief as to all other matters, as follows:

6 **PARTIES**

7  
8 1. PrivaSys is a corporation organized under the laws of the State of  
9 Delaware, and has its principal place of business in Newbury Park, California. PrivaSys  
10 is and at all pertinent times was the assignee and owner of the patent at issue in this case.

11 2. Defendant American Express Company is a corporation organized under  
12 the laws of the State of New York, and has its principal place of business in New York,  
13 New York.

14 3. Defendant American Express Travel Related Services Company, Inc., a  
15 wholly-owned subsidiary of the American Express Company, is a corporation organized  
16 under the laws of the State of New York, and has its principal place of business in New  
17 York, New York.

18 **JURISDICTION AND VENUE**

19  
20 4. This complaint asserts a cause of action for patent infringement under the  
21 Patent Act, 35 U.S.C. § 271. This Court has subject matter jurisdiction over this matter  
22 by virtue of 28 U.S.C. § 1338(a). Venue is proper in this Court by virtue of 28 U.S.C. §  
23 1391(b) and (c) and 28 U.S.C. § 1400(b).

24  
25 5. This Court has personal jurisdiction over American Express because it  
26 provides infringing products and services in the Northern District of California and  
27 American Express has a regular and established place of business in this district.

**INTRADISTRICT ASSIGNMENT**

1  
2 6. Pursuant to Civil LR 3-2(c), this case should be subject to district-wide  
3 assignment because it is an Intellectual Property Action.

4 **BACKGROUND**

5 **The Pervasive Payment Card Fraud Problem**

6 7. For the past 40 years, until relatively recently, payment cards (*e.g.*,  
7 credit, charge and debit cards) have been inanimate pieces of plastic. Each card has a  
8 primary account number in embossed characters, information about the cardholder also  
9 embossed, an encoded magnetic stripe (“magstripe”) on the back of the card, and a printed  
10 and visible three or four digit security code. Devices such as fobs are used in addition to  
11 cards to conduct payment transactions. As used herein the term “card” includes such  
12 payment devices and the term “device” includes payment cards.  
13

14 8. The magstripe contains data that can be read by magstripe readers, the  
15 terminals used by merchants at the point of sale (“POS”). When a merchant swipes a card, a  
16 magnetic head reads the encoded data and then transmits the data to the issuing financial  
17 institution with an authorization request. “Track 1” data on the magstripe typically contains  
18 the customer’s name, account number, expiration date, and a “discretionary data” field to be  
19 used by the issuing bank. “Track 2” data contains the account number, expiration date, and  
20 another “discretionary data” field, all of which must fit within approximately 40 digits of  
21 space.  
22

23 9. A person who obtains the Track 1 and Track 2 account information and the  
24 printed security code has all the information that he needs to manufacture a counterfeit card.  
25 An increasing form of fraud consists of collecting valid account numbers, either through  
26 “skimming” (*e.g.*, collecting card numbers electronically) or through data compromise (*e.g.*,  
27  
28

1 computer hacking) and then using the account numbers and printed security code to  
2 manufacture counterfeit cards. Payment card fraud using such techniques costs payment card  
3 networks and banks – and ultimately the cardholders – many billions of dollars a year.

4 10. In the last few years, major payment card networks, including American  
5 Express, Visa and MasterCard, began to offer contactless cards or devices, *i.e.*, payment  
6 cards and devices that do not need to be swiped through a magnetic reader in order to  
7 conduct a transaction. These devices commonly contain a small computer chip and a  
8 contactless means of communication such as a radio-frequency antenna (RF) that allows a  
9 reader to receive data from the device when it is placed in proximity to the reader (typically  
10 within a few centimeters), and may send standardized magnetic stripe Track 1 or Track 2  
11 data streams, *i.e.*, data is packaged as per the existing magnetic stripe legacy system  
12 protocols. Contactless devices are, if anything, more vulnerable to fraud, as, *e.g.*, the radio  
13 signal can be intercepted and the account data stolen.  
14

15  
16 11. Payment card fraud is being addressed in Europe and in Asia, in part, through  
17 the adoption of “smart cards.” A smart card is a payment card equipped with a secure chip,  
18 possessing internal data processing functionality. Smart cards are more difficult to duplicate  
19 than conventional cards, and they have intrinsic security protection. In Europe, MasterCard  
20 and Visa have advanced smart cards through a joint venture known as EMVCo. (“EMV”).

21 12. While smart cards offer many benefits, they cannot be read by conventional  
22 magstripe POS terminal readers. Instead, smart cards require new, more sophisticated  
23 terminals. In essence, full smart card adoption requires wholesale replacement of the  
24 existing POS magstripe terminals. This “re-terminalization” is expensive but essential to  
25 widespread smart card adoption.  
26  
27  
28

1           13.     Payment card networks have accelerated smart card adoption in Europe  
2 through what is known as “liability shift.” In the United States, a POS merchant is not liable  
3 for loss when a fraudulent card is used in a “card present” transaction, so long as he properly  
4 obtains a “personal identification number” (“PIN”) or a signature and obtains issuer  
5 authorization. Instead, the issuing bank absorbs that loss. Conversely, in countries that  
6 mandate the issuing banks release smart cards, a POS merchant in Europe bears the fraud  
7 loss unless he has invested in a smart card terminal, even if he innocently accepts a  
8 fraudulent card. Shifting the fraud loss to the merchant gives the merchant a strong incentive  
9 to invest in new smart card terminals.  
10

11           14.     Payment card networks have been unable to introduce smart cards in the  
12 United States. In considerable part, this is due to the enormous cost of re-terminalization,  
13 estimated to be in the vicinity of \$12-13 billion. Because payment card networks have been  
14 unable to shift the fraud loss to POS merchants, those merchants lack the economic incentive  
15 to invest in new smart card terminals and have generally declined to do so.  
16

### 17                           **PrivaSys’ Solution To Payment Card Fraud**

18           15.     PrivaSys was founded to develop innovative ways to reduce payment card  
19 fraud while working within the existing legacy system of magstripe readers and transaction  
20 networks, and has developed solutions that are equally effective for contactless cards and  
21 devices as they are for magstripe devices. PrivaSys understood that smart cards would be  
22 adopted slowly if at all in this country, which gave rise to a compelling need to make the  
23 legacy system itself more secure. Prior security approaches, *e.g.*, card holograms or printed  
24 security codes, were easily circumvented, as they were static and unchanging. Thus,  
25 PrivaSys invented a new approach that would allow the card itself to become the center of  
26  
27  
28

1 innovation. Re-terminalization is unnecessary because data is received from the card in the  
2 traditional magnetic stripe data packet format.

3 16. The PrivaSys system creates an authentication code that is unique to each card  
4 and each transaction. The data are transmitted to the reader by a signal from the card.  
5 Because a counterfeit card lacks the ability to generate this unique code, or watermark, the  
6 issuing bank or network knows to reject the fraudulent transaction.

7 17. The PrivaSys method works as follows:

- 8 • Each card securely stores a card-specific, cryptographic key on a chip.
- 9 • Each card contains a “counter” that increments with every use or attempted  
10 use of the card.
- 11 • Each card contains a cryptographic algorithm, to calculate an authentication  
12 code.
- 13 • The information is processed through a triple-DES (or 3DES) encryption  
14 algorithm. The output of this algorithm is reduced to several digits unique to  
15 the specific transaction for the given card.
- 16 • These digits are referred to as a “dynamic authentication code” (or DAC).  
17 The DAC is placed in the discretionary data field of Track 1 and/or Track 2.  
18 The DAC is then communicated along with the account number, expiration  
19 date and a request for authorization to the issuing bank, all through the  
20 existing legacy infrastructure.
- 21 • The issuing bank has backend software that reproduces the DAC computation  
22 on a per-card, per-transaction basis. When the issuing bank receives an  
23 authorization request and accompanying DAC, it computes its own DAC for  
24 that card using that card’s specific cryptographic key. It then compares its  
25 issuer-generated DAC to the card-generated DAC, and approves the  
26 transaction if the two match, and the other account information appears  
27 proper.

28 A counterfeit card does not have the ability to create the unique, transaction-specific DAC.

In this way, the PrivaSys method detects the use of counterfeit cards and denies any  
transaction attempted, and does so within the existing magstripe legacy system.

1 18. PrivaSys' fraud prevention technology is not, however, limited to the legacy  
2 magstripe reader system. PrivaSys designed it to be adaptable to a variety of  
3 communications systems and transmission means—including radio frequency (RF), mobile  
4 (cellular wireless), IR (infrared) and broadcasted magnetic stripe systems.

5 19. PrivaSys' technology is designed to bridge the gap between traditional credit  
6 cards and fully EMV-compliant smart cards. Because it does not require full re-  
7 terminalization, PrivaSys reasonably believed that its technology would be adopted quickly,  
8 populating the United States market with intelligent cards and payment devices. This would  
9 facilitate the ultimate transition to smart cards.  
10

### 11 **The PrivaSys Patent**

12 20. Plaintiff owns a patent, U.S. Patent No. 7,195,154 (“’154 Patent” or  
13 “Routhenstein Patent”), issued on March 27, 2007, to inventor Larry Routhenstein covering  
14 PrivaSys' methods for providing secure transactions between a money source and its  
15 customer credit or debit card holders. A true and correct copy of the ’154 Patent is attached  
16 as Exhibit “A.” Plaintiff is the legal and rightful owner of the Routhenstein Patent.  
17

18 21. The ’154 Patent contains thirty-five (35) patent claims covering a unique and  
19 novel method for generating and validating a dynamic code with each transaction transmitted  
20 over the existing payment card networks. In general, the patent discloses a method that uses  
21 an encrypted and compressed authentication code that is dynamically calculated with each  
22 transaction and transmitted via the discretionary data field through the legacy payment card  
23 processing system and which is validated at the back end by the payment network or issuing  
24 bank.  
25

26 22. PrivaSys has licensed this technology to several of American Express's  
27 principal competitors in the contactless payment card and transaction processing businesses,  
28

1 including MasterCard, transaction processor First Data, Inc. and others. American Express,  
2 however, has refused to take a license.

### 3 American Express's Infringing Services

4 23. Plaintiff's patent application was publicly known as early as March 27, 2003,  
5 when the application was published by the Patent Office. On the issuance of the patent,  
6 American Express became aware of it through ongoing licensing discussions among counsel.  
7 Despite this knowledge, American Express has proceeded on a path of selling infringing  
8 products and services as detailed below.  
9

10 24. American Express operates general purpose payment card network, card  
11 issuing and merchant acquiring and processing businesses that are global in scope. It is one  
12 of the world's largest providers of charge and credit cards to consumers, small businesses  
13 and corporations. These cards and devices, which include cards issued by American Express  
14 as well as cards issued by third-party banks and other institutions that are accepted on the  
15 American Express network, are currently issued in over 40 currencies. American Express  
16 cards and devices permit consumers to charge purchases of goods and services in most  
17 countries around the world at the millions of merchants that accept cards bearing the  
18 American Express logo. American Express, as of 2006, had 78 million cards in force,  
19 including Cards issued by third parties. Worldwide spending on American Express cards  
20 totals \$561 billion.  
21

22 25. The payment cards and devices offered by American Express and third-party  
23 banks include contactless cards and devices, *i.e.*, payment cards that do not need to be swiped  
24 through a magnetic reader, commonly called ExpressPay. References herein to American  
25 Express cards and devices and to ExpressPay cards and devices include all contactless cards  
26 and devices issued by American Express and all contactless cards and devices issued by  
27  
28



1 third-party banks or other institutions that bear the logos American Express, ExpressPay or  
2 other logos associated with American Express. Contactless cards contain a small computer  
3 chip, and, for example, “RF” cards contain a radio-frequency antenna (RF) that allows a  
4 reader to receive data from the device when it is placed in proximity to the reader (typically  
5 within a few centimeters). American Express’s contactless cards are designed to send  
6 standardized magnetic stripe Track 1 or Track 2 data streams, *i.e.*, data is packaged as per the  
7 existing magnetic stripe legacy system protocols.  
8

9 26. American Express’s contactless payment protocols operate in general as  
10 follows. There is a unique cryptographic key for each American Express payment card and  
11 device. The card or device generates a unique several digit cryptogram for each and every  
12 card-specific transaction; this unique cryptogram is packaged as per existing magnetic stripe  
13 data protocols and sent in Track 1 or Track 2 data fields through the existing legacy system.  
14 The data is sent to American Express and/or to a bank where pursuant to American Express  
15 specifications the data is decrypted in the backend system and the transaction validated or  
16 denied.  
17

18 27. Each step in the infringement of the ‘154 patent is performed by American  
19 Express or by a cardmember, merchant, financial institution or other entity whose  
20 performance is directed or controlled by American Express.  
21

22 28. The use of a dynamic cryptogram is essential to the success of the American  
23 Express ExpressPay product. Absent such a cryptogram, the RF transactions could be easily  
24 skimmed or breached, and fraud would proliferate.  
25  
26  
27  
28

**COUNT I**  
**(Patent Infringement)**

1  
2 29. American Express has infringed and is still infringing the Routhenstein Patent  
3 by, without authority, consent, right or license, and in direct infringement of the Routhenstein  
4 Patent, making, using, offering for sale and/or selling products using the methods claimed in  
5 the patent in this country. This conduct constitutes infringement under 35 U.S.C. § 271(a).  
6

7 30. In addition, American Express has infringed and is still infringing the  
8 Routhenstein Patent in this country, through, *inter alia*, its promotion of ExpressPay (and  
9 similar brand names) and agreements and cooperation with banks and merchants in  
10 distributing ExpressPay cards and devices and authenticating and processing transactions  
11 initiated from those devices and its active inducement of others to make, use, and/or sell the  
12 systems, products and methods claimed in one or more claims of the Routhenstein Patent.  
13 This conduct constitutes infringement under 35 U.S.C. § 271(b).  
14

15 31. In addition, American Express has infringed and is still infringing the  
16 Routhenstein Patent in this country through, *inter alia*, providing and selling goods and  
17 services designed for use in practicing one or more claims of the Routhenstein Patent, where  
18 the goods and services constitute a material part of the invention and are not staple articles of  
19 commerce, and which have no use other than infringing one or more claims of the  
20 Routhenstein Patent. American Express has committed these acts with knowledge that the  
21 goods and services it provides are specially made for use in a manner that directly infringes  
22 the Routhenstein Patent. This conduct constitutes infringement under 35 U.S.C. § 271(c).  
23

24 32. American Express's infringing conduct is unlawful and willful. American  
25 Express's willful conduct makes this an exceptional case as provided in 35 U.S.C. § 285.  
26  
27  
28

1 33. As a result of American Express's infringement, Plaintiff has been damaged,  
2 and will continue to be damaged, until American Express is enjoined from further acts of  
3 infringement.

4 34. American Express will continue to infringe the Routhenstein Patent unless  
5 enjoined by this Court. Plaintiff faces real, substantial and irreparable damage and injury of  
6 a continuing nature from American Express's infringement for which Plaintiff has no  
7 adequate remedy at law.  
8

9 WHEREFORE, Plaintiff prays:

10 (a) That this Court find American Express has committed acts of patent  
11 infringement under the Patent Act, 35 U.S.C. § 271;

12 (b) That this Court enter judgment that:

13 (i) The Routhenstein Patent is valid and enforceable and;

14 (ii) American Express has willfully infringed the Routhenstein Patent;  
15

16 (c) That this Court issue a preliminary and final injunction enjoining  
17 American Express, its officers, agents, servants, employees and attorneys, and any other  
18 person in active concert or participation with them, from continuing the acts herein  
19 complained of, and more particularly, that American Express and such other persons be  
20 permanently enjoined and restrained from further infringing the Routhenstein Patent;

21 (d) That this Court require American Express to file with this Court, within  
22 thirty (30) days after entry of final judgment, a written statement under oath setting forth  
23 in detail the manner in which American Express has complied with the injunction;

24 (e) That this Court award Plaintiff the damages to which it is entitled due to  
25 American Express's patent infringement, with both pre-judgment and post-judgment  
26 interest;  
27  
28

1 (f) That American Express’s infringement of the Routhenstein Patent be  
2 adjudged willful and that the damages to Plaintiff be increased by three times the amount  
3 found or assessed pursuant to 35 U.S.C. § 284;

4 (g) That this be adjudged an exceptional case and that Plaintiff be awarded its  
5 attorney’s fees in this action pursuant to 35 U.S.C. § 285;

6 (h) That this Court award Plaintiff its costs and disbursements in this civil  
7 action, including reasonable attorney’s fees; and

8 (i) That this Court grant Plaintiff such other and further relief, in law or in  
9 equity, both general and special, to which it may be entitled.  
10

11 Dated: February 22, 2008

12 Respectfully submitted,

13  
14 /s/ George F. Bishop  
15 SPENCER HOSIE (CA Bar No. 101777)  
16 shosie@hosielaw.com  
17 BRUCE WECKER (CA Bar No. 078530)  
18 bwecker@hosielaw.com  
19 GEORGE F. BISHOP (CA Bar No. 89205)  
20 gbishop@hosielaw.com  
21 HOSIE McARTHUR LLP  
22 One Market, 22nd Floor  
23 San Francisco, CA 94105  
24 (415) 247-6000 Tel.  
25 (415) 247-6001 Fax

26 ROBERT J. YORIO (CA Bar No. 93178)  
27 yorio@carrferrell.com  
28 CARR & FERRELL LLP  
2200 Geng Road  
Palo Alto, CA 94303  
(650) 812-3400 Tel.  
(650) 812-3444 Fax

*Attorneys for Plaintiff*  
*PRIVASYS, INC.*

**DEMAND FOR JURY TRIAL**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Plaintiff, by its undersigned attorneys, demands a trial by jury on all issues so triable.

Dated: February 22, 2008

Respectfully submitted,

/s/ George F. Bishop  
SPENCER HOSIE (CA Bar No. 101777)  
shosie@hosielaw.com  
BRUCE WECKER (CA Bar No. 078530)  
bwecker@hosielaw.com  
GEORGE F. BISHOP (CA Bar No. 89205)  
gbishop@hosielaw.com  
HOSIE McARTHUR LLP  
One Market, 22nd Floor  
San Francisco, CA 94105  
(415) 247-6000 Tel.  
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)  
yorio@carrferrell.com  
CARR & FERRELL LLP  
2200 Geng Road  
Palo Alto, CA 94303  
(650) 812-3400 Tel.  
(650) 812-3444 Fax

*Attorneys for Plaintiff*  
**PRIVASYS, INC.**

**DISCLOSURE OF NON-PARTY INTERESTED ENTITIES OR PERSONS**

Pursuant to Civil L.R. 3-16, Plaintiff, by its undersigned attorneys, certifies that as of this date, there is no such interest to report.

Dated: February 22, 2008

Respectfully submitted,

/s/ George F. Bishop  
SPENCER HOSIE (CA Bar No. 101777)  
shosie@hosielaw.com  
BRUCE WECKER (CA Bar No. 078530)  
bwecker@hosielaw.com  
GEORGE F. BISHOP (CA Bar No. 89205)  
gbishop@hosielaw.com  
HOSIE McARTHUR LLP  
One Market, 22nd Floor  
San Francisco, CA 94105  
(415) 247-6000 Tel.  
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)  
yorio@carrferrell.com  
CARR & FERRELL LLP  
2200 Geng Road  
Palo Alto, CA 94303  
(650) 812-3400 Tel.  
(650) 812-3444 Fax

*Attorneys for Plaintiff*  
*PRIVASYS, INC.*