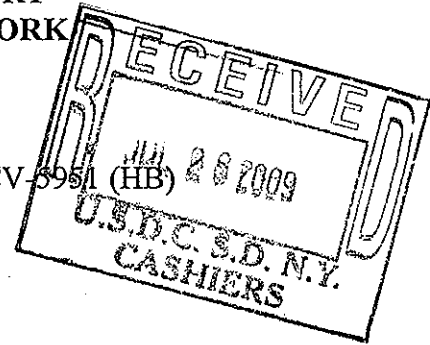


UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK



Stephen W. Perkins, Norman Stoehr and)
Catherine Stoehr, David and Stacey Schapiro,)
Mariellen Baker, Sangsoo Wesley Park,)
William Whetstone, Richard Luckett,)
Mark Nathan, Matthew Delaney,)
Peter and Lois Nathan, John D. Wilgeroth,)
Kerry B. Hoggard, Mike Berkley,)
David Goldberg, Paul Braoudakis,)
Aaron Lambert, Kimberly Quan,)
Stuart and Joan Schapiro, James B. Black, on)
behalf of themselves and all others similarly)
situated,)

Case No.: 09-CV-5951 (HB)

**FIRST AMENDED
CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

Plaintiffs,

v.

Verified Identity Pass, Inc., and Doe
Defendants 1-25,

Defendants.

Plaintiffs, by and through their attorneys, bring this nationwide class action against defendants Verified Identity Pass, Inc. ("VIP") and Doe Defendants 1-25 (collectively, "Defendants"), on behalf of themselves and a class of all others similarly situated. The proposed class includes all persons who purchased a membership in VIP's CLEAR Program ("CLEAR") and who were enrolled as CLEAR members as of June 22, 2009, the date on which VIP discontinued operations, stopped providing any services or benefits to CLEAR members and announced that no pro-rata refunds of membership fees would be provided. Plaintiffs bring this action for damages and for equitable, preliminary, and permanent injunctive relief against Defendants, who designed, operated, marketed, sold, and/or distributed CLEAR memberships to

the Class. Plaintiffs allege the following, based upon their own knowledge, or where there is no personal knowledge, upon information and belief and an investigation by counsel:

NATURE OF THE ACTION

1. The CLEAR program, which was offered and operated by VIP up until June 22, 2009, is an airport check-in membership program which features special security lanes in airports that allowed its members to bypass long check-in lines and proceed directly to airport screening. Hundreds of thousands of consumers across the United States, having provided sensitive and personal information such as social security numbers and fingerprints to VIP for the privilege of bypassing security check-in, were members of CLEAR.

2. VIP sold membership subscriptions for CLEAR for varying lengths of time at different prices. While some members purchased yearly memberships at prices of at least \$99.00, and typically \$199.00, others purchased ten-year memberships for over \$1,000.00. Pursuant to the Membership Agreement ("Agreement")¹ entered into between the consumer and VIP, if a member terminates his or her membership or is otherwise terminated from CLEAR, a pro-rated amount for the unexpired portion of his or her membership would be refunded. As further described below, however, such refunds never occurred.

3. Shortly before CLEAR ceased operations on June 22, 2009, VIP continued marketing and selling memberships to consumers and automatically renewing extended memberships. Upon information and belief, VIP continued charging consumers' credit cards for CLEAR subscriptions as late as June 22, 2009 – the same day VIP ceased operations.

¹ "Clear Terms and Conditions."

<http://web.archive.org/web/20071224014641/www.flyclear.com/enrollment/enroll_membership_agreement.html> (last visited July 22, 2009), attached hereto as Exhibit A.

4. On June 22, 2009, without any warning, VIP notified Plaintiffs and its other CLEAR customers (the “Class”) that VIP was shutting down operations. VIP advised Plaintiffs and the Class, in an electronic mail as well as on its website,² that VIP “was unable to negotiate an agreement with its senior creditor to continue operations.” Furthermore, Plaintiffs were informed that VIP’s “call center and customer support email service” were no longer available. VIP also disclosed that, although it had not filed for bankruptcy, “[a]t the present time, Verified Identity Pass, Inc. cannot issue refunds [to CLEAR members] due to the company’s financial condition.”³

5. Defendants, with their cut-and-run gambit, wrongfully converted monies of Plaintiffs and the Class, defrauded Plaintiffs and the Class, breached contracts with Plaintiffs and the Class, committed misleading acts and practices against Plaintiffs and the Class, acted negligently with respect to Plaintiffs and the Class, and were unjustly enriched at the expense of Plaintiffs and the Class. Defendants also have sensitive and confidential personal information of Plaintiffs and the Class that is believed to be at risk of disclosure to unauthorized third parties. In addition to damages and other relief sought herein, plaintiffs seek an order that such information be maintained in a secure manner until its disposal and that it be disposed of properly.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a), 18 U.S.C. § 1964 (a) and (c), and the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because Plaintiffs and the Class are of diverse citizenship from Defendant VIP, there

² “Clear Lanes Are No Longer Available.” <www.flyclear.com> (last visited July 22, 2009), attached hereto as Exhibit B.

³ *Id.*

are more than 200,000 class members nationwide, and the aggregate amount in controversy exceeds five million dollars (\$5,000,000.00) exclusive of interest and costs.

7. Venue is proper here pursuant to 28 U.S.C. § 1391 because a substantial part of the events and/or omissions giving rise to Plaintiffs' claims occurred in this District and Defendant VIP has its corporate headquarters in this District. In addition, the contract between Defendant VIP and members of the Class specifically provides that the "[v]enue for any claim, demand or action under this Agreement shall be New York County, New York."⁴

8. This Court has personal jurisdiction over VIP because VIP's corporate headquarters is located in this District and at all times material hereto VIP has conducted extensive and systematic business operations in this District.

PARTIES

A. Plaintiffs

9. Plaintiff Stephen W. Perkins ("Perkins") is a resident of Indianapolis, Indiana. Plaintiff, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently purchased an extended CLEAR membership from VIP. Plaintiff would not have purchased an extended CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Perkins has not received a refund for the unused portion of his membership. Plaintiff Perkins has been injured as a result of the unlawful conduct alleged herein.

10. Plaintiffs Norman Stoeck and Catherine Stoeck (the "Stoeck Plaintiffs") are residents of Altamonte Springs, Seminole County, Florida. The Stoeck Plaintiffs, having provided VIP personal and sensitive information for the privilege of CLEAR membership,

⁴ See Ex. A.

recently renewed their membership from VIP for a period of five years. The Stoehr Plaintiffs would not have purchased an extended CLEAR membership from VIP had they known that VIP would cease operations on June 22, 2009. The Stoehr Plaintiffs have not received a refund for the unused portion of their membership. The Stoehr Plaintiffs have been injured as a result of the unlawful conduct alleged herein.

11. Plaintiffs David Schapiro and Stacey Schapiro (the "Schapiro Plaintiffs") are residents of New York, New York. The Schapiro Plaintiffs, having provided VIP personal and sensitive information for the privilege of CLEAR membership, purchased four CLEAR memberships from VIP for the family. Plaintiffs would not have purchased an extended CLEAR membership from VIP had they known that VIP would cease operations on June 22, 2009. The Schapiro Plaintiffs have not received a refund for the unused portion of their membership. The Schapiro Plaintiffs have been injured as a result of the unlawful conduct alleged herein.

12. Plaintiff Mariellen Baker ("Baker") is a resident of Valley Center, San Diego County, California. Plaintiff Baker, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently purchased a CLEAR membership from VIP. Plaintiff Baker was never able to utilize her CLEAR membership benefits because Defendant ceased operations on June 22, 2009, two days after Ms. Baker received her membership materials. Plaintiff would not have purchased an extended CLEAR membership from VIP had she known that VIP would cease operations on June 22, 2009. Plaintiff Baker has not received a refund for the unused portion of her membership. Plaintiff Baker has been injured as a result of the unlawful conduct alleged herein.

13. Plaintiff Sangsoo Wesley Park ("Park") is a resident of San Jose, California. Plaintiff Park, having provided VIP personal and sensitive information for the privilege of

CLEAR membership, recently renewed his membership from VIP for a period of three years. Plaintiff Park would not have purchased an extended CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Park has not received a refund for the unused portion of his membership. Plaintiff Park has been injured as a result of the unlawful conduct alleged herein.

14. Plaintiff William Whetstone ("Whetstone") is a resident of Riverton, Salt Lake County, Utah. Plaintiff Whetstone, having provided VIP personal and sensitive information for the privilege of CLEAR membership, auto renewed his CLEAR membership from VIP for the period of one year. Plaintiff Whetstone would not have purchased a CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Whetstone has not received a refund for the unused portion of his membership. Plaintiff Whetstone has been injured as a result of the unlawful conduct alleged herein.

15. Plaintiff Richard Luckett ("Luckett") is a resident of Austin, Texas. Plaintiff Luckett, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently purchased a CLEAR membership from VIP for a two-year period. Plaintiff Luckett would not have purchased a membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Luckett has not received a refund for the unused portion of his membership. Plaintiff Luckett has been injured as a result of the unlawful conduct alleged herein.

16. Plaintiff Mark Nathan ("Nathan") is a resident of West Orange, New Jersey. Plaintiff Nathan, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently purchased a CLEAR membership from VIP. Plaintiff Nathan was never able to utilize his CLEAR membership benefits because Defendant did not expand to the

Newark airport as indicated in their marketing e-mails before they ceased operations on June 22, 2009. Plaintiff Nathan would not have purchased a CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Nathan has not received a refund for the unused portion of his membership. Plaintiff Nathan has been injured as a result of the unlawful conduct alleged herein.

17. Plaintiff Matthew Delaney ("Delaney") is a resident of Acworth, Cobb County, Georgia. Plaintiff Delaney, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently renewed his membership from VIP for a period of one year. Plaintiff Delaney would not have purchased an extended CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Delaney has not received a refund for the unused portion of his membership. Plaintiff Delaney has been injured as a result of the unlawful conduct alleged herein.

18. Plaintiffs Peter W. Nathan and Lois R. Nathan (the "Nathan Plaintiffs") are residents of Westport, Connecticut. The Nathan Plaintiffs, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently renewed their membership from VIP for a period of three years. The Nathan Plaintiffs would not have purchased extended CLEAR memberships from VIP had they known that VIP would cease operations on June 22, 2009. The Nathan Plaintiffs have not received a refund for the unused portion of their membership. The Nathan Plaintiffs have been injured as a result of the unlawful conduct alleged herein.

19. Plaintiffs John D. Wilgeroth ("Wilgeroth") and Kerry B. Hoggard ("Hoggard") are residents of Gerrardstown, Berkeley County, West Virginia. Plaintiffs Wilgeroth and Hoggard, having provided VIP personal and sensitive information for the privilege of CLEAR

membership, renewed their CLEAR memberships in or about December 2008, for three years. Plaintiffs Wilgeroth and Hoggard never received the benefit of fully utilizing their three-year extended memberships because Defendant ceased operations on June 22, 2009. Plaintiffs Wilgeroth and Hoggard have not received a refund for the unused portion of their membership. Plaintiffs Wilgeroth and Hoggard have been injured as a result of the unlawful conduct alleged herein.

20. Plaintiff Mike Berkley ("Berkley") is a resident of Orlando, Florida. Plaintiff Berkley, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently purchased an extended CLEAR membership from VIP. Plaintiff Berkley would not have purchased a membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Berkley has not received a refund for the unused portion of his membership. Plaintiff Berkley has been injured as a result of the unlawful conduct alleged herein.

21. Plaintiff David Goldberg ("Goldberg") is a resident of Blairsville, Union County, Georgia. Plaintiff Goldberg, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently renewed his membership from VIP for a period of one year. Plaintiff Goldberg would not have purchased an extended CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Goldberg has not received a refund for the unused portion of his membership. Plaintiff Goldberg has been injured as a result of the unlawful conduct alleged herein.

22. Plaintiff Paul Braoudakis ("Braoudakis") is a resident of Hoffman Estates, Cook County, Illinois. Plaintiff Braoudakis, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently renewed his CLEAR membership from VIP

for the period of one year. Plaintiff Braoudakis was never able to utilize his CLEAR membership benefits because Defendant ceased operations on June 22, 2009. Plaintiff Braoudakis would not have purchased a CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Braoudakis has not received a refund for the unused portion of his membership. Plaintiff Braoudakis has been injured as a result of the unlawful conduct alleged herein.

23. Plaintiff Aaron Lambert ("Lambert") is a resident of Rockville, Montgomery County, Maryland. Plaintiff Lambert, having provided VIP personal and sensitive information for the privilege of CLEAR membership, recently purchased CLEAR membership from VIP. Plaintiff Lambert would not have purchased a CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Lambert has not received a refund for the unused portion of his membership. Plaintiff Lambert has been injured as a result of the unlawful conduct alleged herein.

24. Plaintiff Kimberly Quan ("Quan") is a resident of San Francisco, California. Plaintiff Quan, having provided VIP personal and sensitive information for the privilege of CLEAR membership, purchased her membership from VIP for a period of three years. Plaintiff Quan would not have purchased an extended CLEAR membership from VIP had she known that VIP would cease operations on June 22, 2009. Plaintiff Quan has not received a refund for the unused portion of her membership. Plaintiff Quan has been injured as a result of the unlawful conduct alleged herein.

25. Plaintiffs Stuart Schapiro and Joan Schapiro ("Stuart and Joan Schapiro") are residents of Larchmont, New York. Plaintiffs, having provided VIP personal and sensitive information for the privilege of CLEAR membership, purchased CLEAR memberships from

VIP. Plaintiffs would not have purchased an extended CLEAR membership from VIP had they known that VIP would cease operations on June 22, 2009. Plaintiffs Stuart and Joan Schapiro have not received a refund for the unused portion of their membership. Plaintiffs have been injured as a result of the unlawful conduct alleged herein.

26. Plaintiff James B. Black (the "Black") is a resident of Altamonte Springs, Seminole County, Florida. Plaintiff, having provided VIP personal and sensitive information for the privilege of CLEAR membership, purchased a CLEAR membership from VIP. Plaintiff would not have purchased an extended CLEAR membership from VIP had he known that VIP would cease operations on June 22, 2009. Plaintiff Black has not received a refund for the unused portion of his membership. Plaintiff Black has been injured as a result of the unlawful conduct alleged herein.

B. Defendants

27. Defendant Verified Identity Pass, Inc. was, until at least June 22, 2009, an authorized Service Provider and/or Sponsoring Entity under the U.S. Government's Transportation Security's ("TSA") Registered Traveler ("RT") program. As such, it enrolled Plaintiffs and the Class in the RT program and provided services to them through CLEAR. VIP is a Delaware corporation, with its last-known headquarters and principal place of business at 600 Third Avenue, New York, New York. The founder and former Chief Executive Officer of VIP is Steven Brill. VIP, at the time it ceased operations, was run by acting CEO Jim Moroney.⁵ VIP distributed, marketed, promoted, and sold CLEAR memberships to consumers up until it

⁵ "Clear Promises to Delete Sensitive Flier Data, but No Refunds."

<<http://www.wired.com/epicenter/2009/06/where-will-registered-traveler-fingerprints-go-its-un-clear/>> (last visited July 15, 2009), attached hereto as Exhibit C.

ceased operations on June 22, 2009. VIP conducted substantial business and business operations in New York, including at New York's John F. Kennedy and LaGuardia International Airports.

28. Doe Defendants 1-25 are individuals, business organizations and affiliates and/or subsidiaries of VIP that funded and otherwise aided and implemented VIP's wrongful operations. Their identities will be uncovered during discovery.

FACTUAL BACKGROUND

A. The Company and the CLEAR Program

29. VIP was founded in 2003 by Steven Brill, who was also the company's Chief Executive Officer until he left the company in or about March 2009. VIP, at the time it ceased operations, was run by acting CEO Jim Moroney.⁶

30. VIP, until recently, provided biometric system solutions for airports, airlines, travel agents, and business travelers in the United States. VIP, as regulated by the TSA, a division of the U.S. Department of Homeland Security, offered the RT program called CLEAR that enabled airports to provide enhanced customer service to their passengers while addressing security concerns and allowing for resource allocation at security checkpoints. With nearly 700 million passengers traveling domestically in 2006, VIP touted the CLEAR program as a way to help avoid bottlenecks and, in some instances, reduce the wait time in security lines to as little as five minutes. VIP claimed that CLEAR members would enjoy benefits such as fast passage through airport security, fewer missed flights, extraordinary customer service, access to a designated CLEAR security lane, and a stress-free airport experience.

31. CLEAR's "fast-lane" program began at Orlando International Airport in 2005 and was expanded to at least 18 airports, including New York's John F. Kennedy and LaGuardia

⁶ *Id.*

International Airports, Washington, D.C.'s Dulles and Reagan National airports, as well as airports in Atlanta, Boston, Cincinnati, Denver, Reno-Tahoe, and San Francisco.

32. In order to facilitate this service, customers aged 12 and over who are citizens or permanent residents of the United States were required to complete extensive prescreening procedures in accordance with TSA regulations. Indeed, customers were required to provide VIP with certain identifying information, including, but not limited to, name, address, telephone number, date of birth, gender and height. Travelers also provided VIP with social security and driver's license information. As well, digital photos and digital images of fingerprints and irises were taken of a member once he or she was accepted into the program. All such biographical information was maintained by VIP and/or its agents and affiliates in one or more databases allegedly subject to various security and data protections.

33. Customers whose applications were approved were given a "CLEAR Card," which would allow them to check in using VIP's special security checkpoints instead of at general TSA checkpoints. At these CLEAR security lanes, a CLEAR member's identity would be confirmed via biometric verification.

34. Those utilizing VIP's CLEAR program paid annual fees of at least \$99, though memberships for multiple years were encouraged and advertised. Indeed, VIP, up until it ceased operations, promoted two-year memberships for \$199.90 or three-year memberships for \$299.85. Some customers even paid for ten-year memberships at a cost of \$1190.00. For instance, the Stoehr Plaintiffs renewed their memberships for an additional five year period only a few months before VIP shut down its operations.

35. Plaintiffs are informed and believed, based upon reports in *USA Today* and elsewhere, that the number of active CLEAR members at the time VIP ceased providing services was approximately 250,000.

B. The Membership Agreement and Privacy Policy

36. Pursuant to the Agreement entered into between VIP and the member, the consumer was “responsible for paying all fees associated with using” VIP’s services.⁷ “Once [the consumer has] been accepted for membership,” the consumer’s “credit card will be charged for both the TSA vetting fee [\$28] and [the consumer’s] enrollment in CLEAR.”

37. According to the Agreement, which “shall be governed by and construed in accordance with the laws of the State of New York,” if a consumer “cancels [his/her] CLEAR membership, [the consumer’s] card will be deactivated and [the consumer] will receive a pro-rated refund of [his/her] CLEAR membership; however, the TSA vetting fee is not refunded.” As well, the Agreement provides that if, “for any reason TSA revokes [the consumer’s] CLEAR membership, [the consumer’s] card will be deactivated and [the consumer] will receive a pro-rated refund of [his/her] CLEAR membership.”⁸

38. In addition, a member’s account was “set by default to auto-renew and to automatically charge [the consumer’s] credit card at the currently-applicable rate when [the] term expires. Renewals are subject to the same pro-rated refund policy as initial membership fees. [The consumer] can turn off auto-renew at any time by calling CLEAR support at (866) 848-

⁷ See Ex. A.

⁸ *Id.*

2415” and the consumer “will receive a pro-rated refund for the unexpired portion of [the consumer’s] membership.”⁹

39. Defendants, through a separate Privacy Policy referenced in the Agreement,¹⁰ represented to Plaintiffs that they would maintain “administrative, physical, and technical safeguards” to help protect a consumer’s personal information. Such safeguards included requiring VIP’s employees and subcontractors to pass background investigations and to sign a confidentiality pledge, as well as providing access to such information on a “need-to-know” basis. As well, all personal information was allegedly encrypted and subject to computer anti-virus and security protection. Finally, VIP and the TSA purportedly conducted periodic data security audits on such data.

40. Defendants, pursuant to the Privacy Policy, represented that they “do not sell or give lists or compilations of the personal information of [their] members or applicants to any business or non-profit organizations.” Defendants further represented that they “do not provide member or applicant personal information to any affiliated or non-affiliated organizations for marketing.” Defendants promised and represented that “[n]one of the information that [they] collect may be used for any purpose outside the operation and maintenance of the CLEAR Services.”¹¹

41. Beyond the representations and promises set forth in its Membership Agreement and the Privacy Policy, VIP touted its commitment to the security of members’ information and the right to pro-rated refunds for its customers in its “CEO message:”

⁹ *Id.*

¹⁰ “Clear’s Privacy Policy.” <http://www.flyclear.com/clear_privacy.pdf> (last accessed July 22, 2009), attached hereto as Exhibit D.

¹¹ *Id.*

Dear Clear members (and Potential members):

I want to tell you a bit about the background of our company and what Clear® is trying to do.

I started Verified Identity Pass with a simple idea: In the post 9-11 era we have to take new measures to protect ourselves yet not destroy our way of life by strangling the free flow of people and commerce. Somehow, we have to find common sense solutions that don't make everyone a suspect and create security bottlenecks everywhere we go. To be blunt, that means we need a fair, sensible way not to treat everyone the same when it comes to terrorism protection.

* * *

Second, we think we have a special responsibility to protect your privacy. Yes, we are using biometric identifiers such as fingerprints and iris images. Yes, your enrollment application will be submitted to the government for a basic security threat assessment before we can issue you a Clear card. But we do not believe the process and the questions stop there. We know that this kind of new idea and new process is bound to make many people uneasy about what we are doing with their personal information, especially at a time when every day seems to bring new headlines about identity theft. I started this company because I thought there was a right way to do something like this - a way that confronted privacy issues head on and embraced uncompromising dedication to privacy protection.

So, I urge you to read our privacy policies and what we believe are the innovative, no-strings-attached ways we've made ourselves strictly and publicly accountable for keeping them. They're in plain English. They're not in small print. In short, they're Clear. And we're as proud of them as we are of anything else about Clear.

Third, we try to be obsessive about customer service. We value your business, indeed your willingness to join us in this new venture. And we're determined to earn your loyalty in many ways - from an *always-available pro rata refund*, to a state of the art, 24/7 customer call center, to executives like me reaching out to customers at random and calling them (or greeting them at airports) to ask how we are doing. And if we don't deliver on that, please email me directly. As hard as we try, we're bound to make a mistake occasionally. I'd like to hear from you if we do.

Common sense security. Privacy. Obsessive customer service. Everyone at Clear is determined to stand for all of that and more. When you join Clear, we want you to think you're signing on with a new service that has real value – and real values.¹²

(Emphasis added.)

C. Cessation of Operations

42. Immediately prior to June 22, 2009, VIP continued to sell and actively market its CLEAR program services to consumers. Indeed, Plaintiffs received an electronic mail advertisement from the VIP soliciting customers to purchase a CLEAR membership as a gift for Father's Day (June 21, 2009).

43. On June 22, 2009 at 11:00 PST, VIP ceased all CLEAR operations. On that day, the CLEAR airport kiosks were unstaffed with a paper note stating that CLEAR had "ceased operations" and that passengers should "please utilize regular security checkpoint lanes." The content of the VIP website was removed and replaced with a statement that the company was ceasing operations, effective immediately.

44. An electronic mail from CLEAR to Plaintiffs and the Class on June 22, 2009 stated that CLEAR was stopping operations because CLEAR's "parent company," *i.e.*, VIP – which, upon information and belief, was the corporate alter ego for any and all of its subsidiaries and/or corporate affiliates that were involved in the CLEAR program – was unable to negotiate an agreement with its senior creditor to continue operations.¹³

45. A follow-up electronic mail from CLEAR to Plaintiffs and the Class, dated June 26, 2009, further stated that "[a]t the present time, Verified Identity Pass, Inc. cannot issue

¹² "A Message from Clear's CEO, Steven Brill."

<http://web.archive.org/web/20080205002341/www.flyclear.com/about/clear_ceosmessage.html> (last visited July 22, 2009), attached hereto as Exhibit E.

¹³ See also Ex. B.

refunds due to the company's financial condition."¹⁴ This despite that, in the weeks leading up to June 22, 2009, VIP was both selling and renewing extended CLEAR program memberships to Plaintiffs and the Class and charging Plaintiffs and the Class hundreds of dollars in fees for those memberships – monies that VIP now refuses to return to Plaintiffs and the Class. VIP has not, however, filed for bankruptcy.

46. VIP has also indicated that it may sell, transfer or otherwise make available Plaintiffs' and Class members' provide biographic and biometric identifying information to another provider of similar services. The VIP website message announcing the cessation of CLEAR's operations specifically states:

Will personally identifiable information be sold?

The personally identifiable information that customers provided to Clear may not be used for any purpose other than a Registered Traveler program operated by a Transportation Security Administration authorized service provider. Any new service provider would need to maintain personally identifiable information in accordance with the Transportation Security Administration's privacy and security requirements for Registered Traveler programs. If the information is not used for a Registered Traveler program, it will be deleted.¹⁵

47. Upon information and belief, there are two other companies that are approved by the TSA to provide services similar to VIP. These companies are reportedly interested in purchasing such information.

48. Defendant VIP has also terminated all of its employees, eliminated its presence on the internet other than its closure announcement, and has shut down its telephone and email systems:

¹⁴ See also Ex. B.

¹⁵ *Id.*

How can I contact Clear?

Please visit our website, www.flyclear.com, for the latest updates. Clear's call center and customer support email service are no longer available.¹⁶

As such, there is no meaningful ability to contact VIP for the purpose of making any inquiry about the status and security of the private biographic and biometric information, refunds, or otherwise.

49. On June 25, 2009, US Representatives Bennie G. Thompson, Sheila Jackson-Lee, and Christopher P. Carney, leaders of the U.S. House of Representatives Homeland Security Committee, jointly sent a letter to the TSA regarding VIP's shut down of CLEAR and sought information concerning VIP's disposal of consumer information.¹⁷ Similarly, on June 26, 2009, Senator Jay Rockefeller, chairman of the US Senate Commerce, Science and Transportation Committee, called for the safe and appropriate disposal of consumer information collected by VIP. Senator Rockefeller further sought information on the ability of CLEAR applicants and participants to reclaim their fees.¹⁸ To date, there has been no response to Congress' concerns.

CLASS ALLEGATIONS

50. This action is brought as a nationwide class action individually and on behalf of all others similarly situated under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Class defined as:

¹⁶ *Id.*

¹⁷ See U.S. House of Representatives Committee on Homeland Security June 25, 2009 letter to Transportation Security Administration. <http://epic.org/dhs-committee_tsa-ltr.pdf> (last accessed July 22, 2009), attached hereto as Exhibit F.

¹⁸ See U.S. Senate Committee on Commerce, Science, and Transportation June 26, 2009 letter to Transportation Security Administration. <http://commerce.senate.gov/public/_files/LettertoTSAaboutClearProgram.pdf> (last accessed July 22, 2009), attached hereto as Exhibit G.

All persons in the United States who purchased CLEAR program memberships from Verified Identity Pass, Inc. and who were enrolled as CLEAR members as of June 22, 2009.

Excluded from the Class are Defendants and any entity in which any Defendant has a controlling interest, and their legal representatives, officers, directors, assignees, and successors. Also excluded from the Class is any judge to whom this action is assigned, together with any relative of such judge within the third degree of relationship, and the spouse of any such persons.

51. Class certification is appropriate under Fed. R. Civ. P. 23(a) and (b)(1), (b)(2), and/or (b)(3).

52. The class satisfies the numerosity requirement because it is composed of thousands of persons in numerous locations. The number of class members is so large that joinder of all Class members is impracticable. The identity and exact number of Class members, estimated to be about 250,000, are unknown but can be determined through appropriate discovery.

53. There are numerous and substantial questions of law and fact common to all of the members of the Class which control this litigation and predominate over any individual issues pursuant to Rule 23(b)(3). Common questions of law and fact include:

- a. Whether Defendants knowingly or negligently concealed or omitted material information to Plaintiffs and the Class, including VIP's financial standing and subsequent cessation of operations;
- b. Whether VIP wrongfully converted monies or property of Plaintiffs and the Class;
- c. Whether VIP breached contracts into which it entered with Plaintiffs and the Class by, among other things, failing to provide the services offered for the full membership period and failing to provide pro-rata refunds for

the period of membership remaining after the discontinuance of the service;

- d. Whether Defendants defrauded Plaintiffs and members of the Class and were unjustly enriched thereby at the expense of Plaintiffs and members of the Class;
- e. Whether Defendants violated applicable consumer protection statutes through their misleading acts and practices;
- f. Whether the Class has been injured by virtue of Defendants' negligence, breaches, wrongful conduct, and/or deceptive business practices and conduct;
- g. Whether Defendants are refusing to reimburse Plaintiffs and the Class for the cost of the CLEAR membership and are planning to divest its assets, including disposal of personal information of Plaintiffs and the Class, to potential buyers; and
- h. Whether Plaintiffs and the Class are entitled to an Order requiring Defendants to secure and properly dispose of their sensitive and private biographic and biometric information.

54. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs and the Class have sustained damages arising out of Defendants' wrongful conduct as detailed herein. Plaintiffs have no interests that are antagonistic to the claims of the Class. Plaintiffs understand that this matter cannot be settled without the Court's approval.

55. Plaintiffs will fairly and adequately protect the interests of the Class, and are committed to the vigorous representation of the Class. Plaintiffs have retained counsel that is

competent and experienced in consumer class action litigation. Counsel has agreed to advance the costs of the litigation contingent upon the outcome. Counsel is aware that no fee can be awarded without the Court's approval.

56. A class action is the superior method for the fair and efficient adjudication of this controversy. Joinder of all members of the class is impracticable. The losses suffered by some of the individual members of the Class may be relatively small, and it would therefore be impracticable for individual members to bear the expense and burden of individual litigation to enforce their rights. Litigation of this dispute on a class-wide basis would serve the purpose of judicial economy by avoiding the multiplicity of lawsuits against the same Defendants involving common issues of law and fact. Further, individual proceedings here would pose the risk of inconsistent adjudications. Plaintiffs are unaware of any difficulty in the management of this action as a class action.

57. This Court should apply New York substantive state law to each of the claims of Plaintiffs and the putative Class members because the Agreement entered into between each Class member and Defendants provides that the "agreement shall be governed by and construed in accordance with the laws of the State of New York."¹⁹

¹⁹ See Ex. A.

CLAIMS FOR RELIEF

COUNT I

Conversion

58. Plaintiffs incorporates the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein.

59. Plaintiffs entrusted to VIP specific monies for the particular and intended purpose of providing membership services to Plaintiffs and the Class, including easy and quick access through airport security.

60. Such funds were and are the property and possession of Plaintiffs and the Class.

61. However, VIP has failed to provide the services the monies were entrusted for and has failed to return such monies to Plaintiffs and the Class. Indeed, VIP failed to use those funds for their specified purpose and has no intention of using those funds for the purposes Plaintiffs and the Class entrusted such specific funds for.

62. Instead, VIP is exercising unauthorized control over such property that does not belong to it and is interfering with the superior possessory right of Plaintiffs and the Class to such property by failing to return the funds to Plaintiffs and the Class.

63. VIP's conversion of the funds of Plaintiffs and the Class has caused damage to Plaintiffs and the Class.

COUNT II

Fraud

64. Plaintiffs incorporate the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein.

65. This claim is brought by Plaintiffs and the Class against all Defendants based upon common law principles of fraud.

66. Defendants owed to Plaintiffs and the Class a duty of full disclosure, honesty, and complete candor.

67. VIP made material misrepresentations to Plaintiffs and the Class that were false. Specifically, VIP represented to Plaintiffs when they purchased, renewed, or extended their CLEAR memberships that, in exchange for paying a membership fee and providing extensive personal information, VIP would provide services to Plaintiffs including, but not limited to, expedited airport check-in privileges at airports participating in VIP's CLEAR program.

68. VIP also omitted material information to customers who purchased or renewed their CLEAR memberships concerning VIP's financial status and anticipated shut down. In advertisements as recently as the day before its shut down, for example, VIP solicited customers and potential customers to buy membership packages for their fathers as a Father's Day gift without notifying them of VIP's financial status.

69. VIP made such material misrepresentations and omissions to Plaintiffs and the Class knowing based on the aforementioned facts that those representations were false and its omissions material. VIP made these representations and omissions with the intent to deceive Plaintiffs and the Class.

70. The aforementioned representations and omissions were material, were designed to cause Plaintiffs and the Class to purchase or renew their CLEAR memberships and, in fact, caused them to do so. In paying their membership fees for CLEAR, Plaintiffs and the Class justifiably relied upon the aforementioned representations and omissions, reasonably expecting that they would receive the services promised in exchange for payment of such fees. Plaintiffs and the Class had no ability to know the truth about VIP's intent not to provide the services

contract for, its financial condition or the imminent shutdown of CLEAR's operations or the termination of its services when they purchased or renewed their CLEAR memberships.

71. Plaintiffs and the Class were injured and damaged as a result of VIP's fraudulent representations and omissions.

COUNT III

Breach of Contract

72. Plaintiffs incorporate the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein.

73. Plaintiffs and the Class entered into valid contracts with VIP, pursuant to which Plaintiffs and the Class agreed to pay a membership fee and provide personal and confidential information, including but not limited to fingerprints and iris scans, in consideration for enrollment and participation in the RT program through CLEAR, by which they would be entitled to quick access through airport security.

74. Plaintiffs and the Class performed all of their obligations under these contracts with VIP by, among other things, paying the required membership fees and providing personal and confidential biographic and biometric information to VIP.

75. Despite the performance by Plaintiffs and the Class of their obligations under the terms of these contracts, VIP has failed to perform its duties to Plaintiffs and the Class under the contracts. Beginning on June 22, 2009, with the termination of CLEAR and the cessation of the services that were provided by CLEAR, VIP failed to provide the benefits and privileges Plaintiffs and the Class bargained for, including but not limited to a functional CLEAR program, pro-rated refunds upon termination of membership, and properly secured maintenance of Class members' personal and confidential information.

76. Accordingly, VIP has breached its contracts with Plaintiffs and the Class.

77. VIP's breach of these contracts has caused damage to Plaintiffs and the Class.

COUNT IV

Negligence

78. Plaintiffs incorporate the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein with the exception that previously stated assertions of intentional or reckless misconduct of Defendants and all references to fraud are not incorporated herein for purposes of this claim. For purposes of this claim, Plaintiffs allege that Defendants' conduct was negligent and not intentionally, recklessly and/or grossly negligent.

79. VIP, at all times material hereto, owed a duty of reasonable care to Plaintiffs and the Class.

80. VIP breached that duty by terminating the aforementioned services to Plaintiffs and the Class without taking reasonable precautions and/or other actions to ensure continuation of those services and the protection of the Plaintiffs and Class' private information, even in modified form.

81. VIP's breach of duty damaged Plaintiffs and the Class and was the proximate cause of harm and damage to Plaintiffs and the Class.

82. VIP's breach of duty to Plaintiffs and the Class foreseeably caused harm and damage to Plaintiffs and the Class.

COUNT V

Unjust Enrichment

83. Plaintiffs incorporate the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein.

84. Plaintiffs and the Class assert their claim for unjust enrichment in the alternative to their breach of contract claim; if the contracts between Plaintiffs and the Class and VIP are

rescinded due to fraud in the inducement of those contracts or for other reasons, then Plaintiffs and the Class are entitled to restitution of their damages based on the doctrine of unjust enrichment.

85. VIP has received from Plaintiffs and the Class benefits and/or was enriched at the expense of Plaintiffs and the Class under circumstances that make it unjust and against equity and good conscience for VIP to retain the monies of Plaintiffs and the Class.

COUNT VI

New York Consumer Protection Act (General Business Law § 349)

86. Plaintiffs incorporate the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein.

87. Plaintiffs and the Class are consumers.

88. Defendants' acts and practices described herein were directed at consumers.

89. Defendants' acts and practices were misleading in a material way. This conduct includes, but is not limited to, soliciting, selling to, and renewing CLEAR memberships for consumers without intending to provide the services promised and without disclosing that VIP lacked the ability to provide those services and was planning to close its operations, continuing to charge consumers membership fees even though VIP knew that it would shut down operations in the immediate future, making material misstatements and omissions concerning its sales and promotions, making misleading affirmative statements concerning pro-rated refunds and the sale of consumers' personal and confidential information, and otherwise failing to return any moneys to consumers after VIP ceased operations and to protect Class' private information.

90. Defendants' unfair and deceptive practices directly and/or proximately caused damages to Plaintiffs and Class members, including the loss of the services contracted for, the

loss of their pro-rata refunds and the potential disclosure of their private and personal information.

91. By reason of Defendants' violations, Plaintiffs and Class members are also entitled to recover treble damages.

COUNT VII

Alternative Claim for Relief Under the State Consumer Protection Laws

92. Plaintiffs incorporate the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein.

93. In the alternative to pleading the above nationwide class under New York's Consumer Protection Act, Plaintiffs and the Class allege that Defendants violated the substantive consumer protection and unfair and deceptive trade practices acts or statutes of all fifty states and U.S. territories where their consumers reside.

94. Plaintiffs and the Class are consumers.

95. Defendants' acts and practices described herein were directed at consumers.

96. Defendants' acts and practices were misleading in a material way. This conduct includes, but is not limited to, soliciting, selling to, and renewing CLEAR memberships for consumers without intending to provide the services promised and without disclosing that VIP lacked the ability to provide those services and was planning to close its operations, continuing to charge consumers membership fees even though VIP knew that it would shut down operations in the immediate future, making material misstatements and omissions concerning its sales and promotions, making misleading affirmative statements concerning pro-rated refunds and the sale of consumers' personal and confidential information, and otherwise failing to return any moneys to consumers after VIP ceased operations and to protect Class' private information.

97. Defendants have accordingly violated the laws prohibiting unfair and deceptive trade practices of the states and territories wherein Plaintiffs and other Class members reside: Ariz. Rev. Stat. § 44-1522, *et seq.*; Ark. Code § 4-88-101, *et seq.*; Cal. Bus. & Prof. Code § 17200, *et seq.*; Cal. Civ. Code §§ 1750, *et seq.*, Cal. Bus. & Prof. Code § 17500, *et seq.*; Colo. Rev. Stat. § 6-1-105, *et seq.*; Conn. Gen. Stat. § 42-110b, *et seq.*; 6 Del. Code § 2511, *et seq.*; D.C. Code § 28-3901, *et seq.*; Fla. Stat. § 501.201, *et seq.*; Haw. Rev. Stat. § 480, *et seq.*; Idaho Code § 48-601, *et seq.*; 815 ILCS § 505/1, *et seq.*; Kan. Stat. § 50-623, *et seq.*; Md. Com. Law Code § 13-101, *et seq.*; Mich. Stat. § 445-901, *et seq.*; Minn. Stat. § 325F.67, *et seq.*; Mo. Rev. Stat. § 407.010, *et seq.*; Neb. Rev. Stat. § 59-1601, *et seq.*; Nev. Rev. Stat. § 598.0903, *et seq.*; N.H. Rev. Stat. § 358-A:1, *et seq.*; N.J. Stat. Ann. § 56:8-1, *et seq.*; N.M. Stat. Ann. § 57-12-1, *et seq.*; N.C. Gen. Stat. § 75-1.1, *et seq.*; N.D. Cent. Code § 51-15-01, *et seq.*; Ohio Rev. Stat. § 1345.01, *et seq.*; Okla. Stat. tit. 15 § 751, *et seq.*; Or. Rev. Stat. § 646.605, *et seq.*; 73 Pa. Stat. § 201-1, *et seq.*; S.C. Code Laws § 39-5-10, *et seq.*; S.D. Code Laws § 37-24-1, *et seq.*; Tenn. Code. § 47-18-101, *et seq.*; Tex. Bus & Com. Code Ann. § 17.45, *et seq.*; Utah Code Ann. § 13-11-1, *et seq.*; Vt. Stat. Ann. Tit. 9, § 245 1, *et seq.*; Wash. Rev. Code § 19.86.010, *et seq.*; W. Va. Code § 46A-6-101, *et seq.*, and; Wis. Stat. § 100.18, *et seq.*

98. Defendants' unfair and deceptive practices directly and/or proximately caused damages to Plaintiffs and Class members, including the loss of the services contracted for, the loss of their pro-rata refunds and the potential disclosure of their private and personal information.

99. By reason of Defendants' violations, Plaintiffs and Class members are entitled to recover treble damages where available.

COUNT VIII

Preliminary and Permanent Injunctive Relief

100. Plaintiffs incorporate the allegations contained in the previous paragraphs of this Amended Complaint as if fully set forth herein.

101. Defendants, pursuant to the Privacy Policy, are barred from selling or giving “lists or compilations of the personal information” of Plaintiffs and Class members “to any business or non-profit organizations” and may “not provide member or applicant personal information to any affiliated or non-affiliated organizations for marketing.” None of the information that Defendants collect from Plaintiffs and Class members may be used “for any purpose outside the operation and maintenance of the CLEAR Services.”²⁰

102. VIP is also bound to abide by applicable standards developed and implemented by the TSA for securing biographic and biometric information collected in connection with the RT program as set forth in the TSA Registered Traveler Program Security, Privacy Compliance Standards.²¹

103. CLEAR customers have provided personal and confidential biographic information to Defendants, including, but not limited to, name, address, telephone number, gender, height, date of birth, social security and driver’s license information. As well, biographic information, including digital photos and digital images of fingerprints and irises scans, were taken of the consumer as part of the RT enrollment program. Such biographic and biometric information of travelers is maintained on databases in VIP’s control.

²⁰ See Ex. D.

²¹ “TSA Registered Traveler Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers.” <http://www.tsa.gov/assets/pdf/rt_standards.pdf> (last accessed July 22, 2009), attached hereto as Exhibit H.

104. Defendant VIP has suggested that its database of private biographic and biometric member information may be sold to another provider of similar services. In the website announcement of the cessation of CLEAR's operations, VIP responded to an anticipated question as follows:

Will personally identifiable information be sold?

The personally identifiable information that customers provided to Clear may not be used for any purpose other than a Registered Traveler program operated by a Transportation Security Administration authorized service provider. Any new service provider would need to maintain personally identifiable information in accordance with the Transportation Security Administration's privacy and security requirements for Registered Traveler programs. If the information is not used for a Registered Traveler program, it will be deleted.²²

105. The sale, transfer or disclosure to third parties of the database and the information contained therein is contrary to and in violation of the Privacy Policy. More importantly, such information is private, confidential, and personal to Plaintiffs and the Class, and the sale or transfer thereof would damage Plaintiffs and the Class.

106. With the termination of CLEAR, Defendant VIP also terminated all of its employees, eliminated its presence on the internet other than its closure announcement, shut down its telephone and email systems and deprived Plaintiffs, Class members and all other members of the public of any meaningful ability to contact the company for the purpose of making any inquiry about the status and security of the private biographic and biometric information it collected from CLEAR members. VIP's effective disappearance as an accessible entity with which any communication can be had has resulted in a lack of accountability with respect to its security obligations under the Privacy Policy and TSA's Registered Traveler

²² See Ex. B.

Program Security, Privacy Compliance Standards. Such lack of accountability creates a substantial risk that the private information collected by it in connection with CLEAR will be inadvertently lost, stolen or disclosed to unauthorized third parties.

107. By reason of thereof, Plaintiffs and Class members are entitled to preliminary and permanent relief enjoining Defendants from selling, transferring or disclosing the private information of Plaintiffs and the Class to any unauthorized person or entity and prohibiting Defendants from maintaining the data in a manner that is unsecure or inconsistent in any way with its Privacy Policy and with TSA's Registered Traveler Program Security, Privacy Compliance Standards.

PRAYER FOR RELIEF

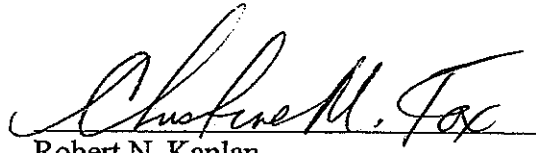
WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray for judgment as follows:

- A. An Order: 1) certifying the proposed nationwide Class herein under Fed. R. Civ. P. 23 or 2) in the alternative, certifying a New York State Class and other such sub-Classes under Fed. R. Civ. P. 23 and applying the substantive consumer protection and unfair and deceptive acts or practices statutes of all fifty states and U.S. territories where the sub-Classes reside; and 3) appointing Plaintiffs and Plaintiffs' counsel of record to represent said Class;
- B. Awarding Plaintiffs and the members of the Class damages, including applicable punitive, compensatory, actual, consequential, and treble damages, and interest;
- C. Awarding Plaintiffs' reasonable costs and attorneys' fees;
- D. Awarding equitable, preliminary, and permanent injunctive relief; and
- E. Awarding other relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and the putative Class, hereby demand a trial by jury.

DATED: July 28, 2009



Robert N. Kaplan
Frederic S. Fox
Christine M. Fox
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue
New York, New York 10022
Tel: (212) 687-1980
Fax: (212) 687-7714

Laurence D. King
Linda M. Fong
Mario M. Choi
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, California 94104
Tel: (415) 772-4700
Fax: (415) 772-4707

Todd M. Schneider
Mark T. Johnson
SCHNEIDER WALLACE COTTRELL
BRAYTON KONECKY LLP
180 Montgomery Street, Suite 2000
San Francisco, California 94104
Tel: (415) 421-7100
Fax: (415) 421-7105

Garrett W. Wotkins
SCHNEIDER WALLACE COTTRELL
BRAYTON KONECKY LLP
7702 East Doubletree Ranch Road, Suite 300
Scottsdale, Arizona 85258
Tel: (480) 607-4368
Fax: (480) 348-3999

Attorneys for Plaintiffs

EXHIBIT A



Search >

☐ select this link to skip main navigation

-
- [About Clear](#)
 - [Airports](#)
 - [enrollment](#)
 - [my account](#)
 - [help](#)

☐ select this link to skip local navigation

- [Enrollment](#)
 - [Enrollment Locations](#)
 - [Membership Agreement](#)
 - [For Businesses](#)
 - [TMC Partners](#)
 - [For Partners](#)

For Business

Find out how your company can benefit from Clear.
[read more >](#)

Enroll Downtown

[Atlanta](#)

[Denver](#)

[Manhattan](#)

[San Francisco](#)

[Washington, DC](#)

Membership Agreement

Terms and Conditions
Clear®

Registered Traveler Program
Verified Identity Pass, Inc.

MEMBERSHIP AGREEMENT

This is a membership Agreement between Verified Identity Pass, Inc. (Verified ID) and its applicants and members. The Clear® Program is operated by Verified ID, a privately held company. It is regulated by the U.S. Government's Transportation Security Administration (TSA), which is a division of the U.S. Department of Homeland Security.

I. Introduction

Below you will find the contractual terms that will govern our relationship with you. Although by nature much of it is complicated, we have attempted to write it in plain English. And we've drafted it in a way that is consistent with the overall idea behind Clear - that we are engaged in a risk management service, not a risk elimination service.

II. Membership Eligibility

Our service is available only to U.S. Citizens and permanent foreign residents aged 12 and over, and may only be used by individuals who can form legally binding contracts under applicable law. Our service is not available to children (persons under the age of 18), unless you use this service in conjunction with, and under the supervision of a parent or guardian. If you do not qualify, please do not apply for membership.

According to Transportation Security Administration policies, children under the age of 12 may not enroll in a registered traveler program, but may access the Clear lanes when accompanied by a parent or legal guardian that is a registered traveler participant in good standing.

Children using the Clear lane who are under 12 will be processed through the security checkpoint as "non-members". Minors above the age of 12 are eligible to join the program through the same process as adults with the additional requirement that a parent or legal guardian must be an approved registered traveler member and must consent in writing to permit the child to join the program.

III. Fees and Services

You are responsible for paying all fees associated with using our service. As part of the national rollout of the registered traveler program, the Transportation Security Administration (TSA) will charge a fee to conduct a security threat assessment of each applicant. Once you have been accepted for membership, your credit card will be charged for both the TSA vetting fee and your enrollment in Clear.

If you are not approved for membership in the program, your credit card will not be charged for the TSA vetting fee or for enrollment in Clear.

Should you cancel your Clear membership, your card will be deactivated and you will receive a pro-rated refund of your Clear membership; however, the TSA vetting fee is not refunded.

If for any reason TSA revokes your Clear membership, your card will be deactivated and you will receive a pro-rated refund of your Clear membership.

Your credit card will be billed at the time of approval of your membership for \$99.95, which includes the \$28 TSA vetting fee. Unless you instruct us otherwise after we give you advance notice, at expiration of your initial membership term, we will bill your credit card for renewal of the service at the then-applicable rate.

Your Clear Account is set by default to auto-renew and to automatically charge your credit card at the currently-applicable rate when your term expires. Renewals are subject to the same pro-rated refund policy as initial membership fees. You can turn off auto-renew at any time by calling Clear support at (866) 848-2415 — you will receive a pro-rated refund for the unexpired portion of your membership.

If your membership application is not approved, your credit card will not be charged. Our pro-rated refund policy does not apply to advance payments for multiple memberships paid for by third parties.

If you are enrolling in Clear through a promotion, the Terms and Conditions of that promotion shall apply.

IV. Use of Our Website

This website is owned and operated by Verified ID. Verified ID provides its services to you subject to the terms and conditions described in the Terms and Conditions section of our website. When you use this service, you accept those conditions.

V. Privacy

Please review our [Privacy Policy](#) to understand our privacy practices that govern this membership Agreement.

VI. Verified Identity Pass' Obligations to Applicants and Members

In providing the Clear membership Service, Verified ID agrees as follows:

1. Verified ID shall administer an application and enrollment process which will serve to ascertain

through the collection of biographic information that the applicant meets certain criteria to prove his identity ("the enrollment process").

2. Verified ID shall register applicants in-person by taking biometric identifiers, including fingerprints and iris (the biometric information), and photographs for Clear membership.
3. Verified ID shall send applicant's biometric and biographic identifying information to the U.S. Government's Transportation Security Administration (TSA) for a security threat assessment.
4. Verified ID shall issue a membership card upon applicant's successful completion of both the online enrollment process, the in-person registration and the TSA screening process.
5. Verified ID warrants that it will keep the promises contained in its Privacy Policy referenced in V above, and instruct its directors, officers, employees or agents not to commit any action which causes it to be in violation of those principles. Verified ID reserves the right from time to time to change these policies, and if it does so it shall inform all customers by email.

VII. Applicants' and Members' Obligations

In contracting for the Clear membership service, applicants and members (who shall be known collectively as "Customers") agree as follows:

1. Customer acknowledges and agrees that when Verified ID submits an applicant's name to TSA for checking against terrorist threat lists or similar data maintained by the United States government, such lists and data are by their nature inherently fallible. They may result in incorrect or unjustified matches of names of applicants who pose no terrorist threat, and they may not contain names of people who do present a terrorist threat. Customer also acknowledges that TSA does not transmit to Verified ID or to the airport any information about the applicant or any reasons for its decisions. Therefore, customer releases Verified ID and the facilities in which the Verified ID product is used, from any liability, and holds it harmless for any and all damages or injury resulting directly or indirectly from the use of these lists and data.
2. Customer acknowledges and agrees that for the fee charged, Verified ID cannot be an insurer against injuries or losses related to the performance of the membership cards, the card readers, and/or the overall system for granting access to the members' designated lane ("the access system"); and therefore, that the customer will not hold Verified ID liable for any injury or loss in connection with the access system and from any loss or expense suffered by Customer resulting directly or indirectly from its performance or failure.
3. Customer acknowledges that in the case of a lost or stolen card, it is the customer's responsibility to notify Verified ID at www.FlyClear.com or (866) 848-2415 as soon as possible.
4. Customer acknowledges that the enrollment term begins on the day that the card can first be used by the member.
5. Customer acknowledges that all decisions related to who is allowed to board or not to board an airplane at any airport are solely the responsibility of the federal Transportation Security Administration (TSA) and that Verified ID cannot in any way be responsible for any direct or indirect consequences or damages related to those decisions.
6. Customer acknowledges and agrees that Verified ID is intended to be and is offered as a risk management tool, not a risk elimination tool, and that while Verified ID may lessen the risk of criminal, terrorist and other dangerous acts in places where the Verified ID Service is used, while enhancing convenience, Verified ID is not an insurer and in no way eliminates those risks. Because of the limits inherent in the Verified ID process, including the limits of, and possibility of errors in the screening process, as well as the impossibility of predicting human behavior based on the prior acts of members, neither Verified ID nor the facilities in which it is used shall be liable for any loss, injury or damage to property, to customer or to third parties, arising from any use of the Clear card and its access system.

VIII. TSA Required Conditions

1. Customer acknowledges that Registered Traveler is linked to the national security environment and that the Transportation Security Administration (TSA) can suspend the program at any or all locations at any time if changes in the security environment warrant. If the registered traveler program is suspended by the TSA, the amount of days missed due to the suspension will be added to the end of the membership term. If the registered traveler program is shut down by the TSA, the customer will be provided a pro-rata refund of his or her membership fee.
2. Customer acknowledges and agrees that if additional information is required for the TSA to perform adjudication, the TSA will work directly with the customer to resolve the matter, and that TSA will be responsible for any enforcement action resulting from fraudulent matches.
3. Customer acknowledges and agrees that TSA will be responsible for notifying the customer if the customer receives a "Not Approved" TSA Security Threat Assessment.
4. Customer acknowledges and agrees that TSA or its agents may transmit an "Approved" or "Not Approved" determination of the customer's TSA Security Threat Assessment directly to Clear. TSA or its agents will not transmit the content of the TSA Security Threat Assessment nor the reason behind the "Approved" or "Not Approved" determination.
5. Customer acknowledges and agrees that payment of a fee to participate in Registered Traveler neither guarantees acceptance into RT nor continued enrollment status in RT.
6. Customer authorizes Clear to collect and retain information necessary to provide customer support including the biometric information collected at enrollment.
7. Customer acknowledges and agrees to update his/her biographical data, such as address or phone number, within 30 days of any changes taking effect.
8. Customer acknowledges and agrees that he/she has received a copy of the TSA Privacy Act Statement.

TSA Privacy Act Statement

Authority: 49 U.S.C. 114 authorizes collection of this information.

Purpose: TSA is collecting this information from all individuals who apply to participate in the Registered Traveler program. TSA will use this information to verify your identity, to conduct and adjudicate a security threat assessment, and, if you are accepted into Registered Traveler, to conduct ongoing security threat assessments and to issue a "smart card" to you that will identify you as a Registered Traveler. Furnishing this information is voluntary. However, failure to provide it may delay or prevent the completion of the security threat assessment, without which you may not be permitted to participate in this program.

Routine Uses: The information will be used by and disclosed to TSA personnel and contractors or other agents who need the information to assist in the operation of Registered Traveler. Additionally, TSA may share this information with airports and airlines to the extent necessary to ensure proper identification, ticketing, security screening, and boarding of Registered Travelers. TSA may disclose information to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security. TSA may also disclose information pursuant to its published system of records notices, DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS) and DHS/TSA 015, Registered Traveler Operations Files, both of which were last published in the Federal Register on November 8, 2005, at 70 FR 67731-67736.

IX. Miscellaneous

1. This Agreement shall be governed by and construed in accordance with the laws of the State of New York. Venue for any claim, demand or action under this Agreement shall be New York County, New York.
2. This Agreement and any Terms and Conditions of any promotion through which Customer enrolls, constitute the entire understanding of Verified ID and Customer. If any provisions in this agreement are declared invalid, illegal, or unenforceable in any respect, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired and shall not render this agreement unenforceable, invalid or illegal as whole.
3. The Customer may not assign, transfer or delegate any rights or obligations hereunder.

[Corporate Information](#) [Online Privacy](#) [Press Room](#) [Careers](#) [Contact](#) [Site Map](#)
[privacy-policy](#)

Verified Identity Pass, 600 Third Avenue, 10th Floor, New York, NY 10016

Copyright © 2007 Verified Identity Pass, Inc. All rights reserved.

Use of this website signifies your agreement to the Terms of Use and Online Privacy Policy (updated 10-17-2007).

EXHIBIT B

Clear Lanes Are No Longer Available.

At 11:00 p.m. PST on June 22, 2009, Clear ceased operations. Clear's parent company, Verified Identity Pass, Inc., was unable to negotiate an agreement with its senior creditor to continue operations. Verified Identity Pass regrets that Clear will not be able to continue operations.

How is Clear securing personal information?

Clear stands by our commitment to protect our customer's personally identifiable information – including fingerprints, iris images, photos, names, addresses, credit card numbers and other personal information provided to us - and to keep the privacy promises that we have made. Information is secured in accordance with the Transportation Security Administration's Security, Privacy and Compliance Standards.

How is Clear securing any information at the airports?

Each hard disk at the airport, including the enrollment and verification kiosks, has now been wiped clean of all data and software. The triple wipe process we used automatically and completely overwrites the contents of the entire disk, including the operating system, the data and the file structure. This process also prevents or thoroughly hinders all known techniques of hard disk forensic analysis.

How is Clear securing any information in central databases and corporate systems?

Lockheed Martin is the lead systems integrator for Clear, and is currently working with Verified Identity Pass, Inc. to ensure an orderly shutdown as the program closes. As Verified Identity Pass, Inc. and the Transportation Security Administration work through this process, Lockheed Martin remains committed to protecting the privacy of individuals' personal information provided for the Clear Registered Traveler program. Lockheed's work will also remain consistent with the Transportation Security Administration's federal requirements and the enhanced security and privacy requirements of Verified Identity Pass, Inc.

The computers that Verified Identity Pass, Inc. assigned to its former corporate employees are being wiped using the same process described for computers at the airports.

Will personally identifiable information be sold?

The personally identifiable information that customers provided to Clear may not be used for any purpose other than a Registered Traveler program operated by a Transportation Security Administration authorized service provider. Any new service provider would need to maintain personally identifiable information in accordance with the Transportation Security Administration's privacy and security requirements for Registered Traveler programs. If the information is not used for a Registered Traveler program, it will be deleted.

How will members be notified when information is deleted?

Clear intends to notify members in a final email message when the information is deleted.

Who is monitoring this process?

Clear is communicating with TSA, airport and airline sponsors, and subcontractors, to ensure that the security of the information and systems is maintained throughout the closure process. Clear thanks these partners for their continuing cooperation and diligence.

How can I contact Clear?

Please visit our website, www.flyclear.com, for the latest updates. Clear's call center and customer support email service are no longer available.

Will I receive a refund for membership in Clear?

At the present time, Verified Identity Pass, Inc. cannot issue refunds due to the company's financial condition.

Has Verified Identity Pass, Inc. filed for bankruptcy?

At the present time, Verified Identity Pass has not commenced any proceedings under the United States Bankruptcy Code.

[Clear's Privacy Policy](#)

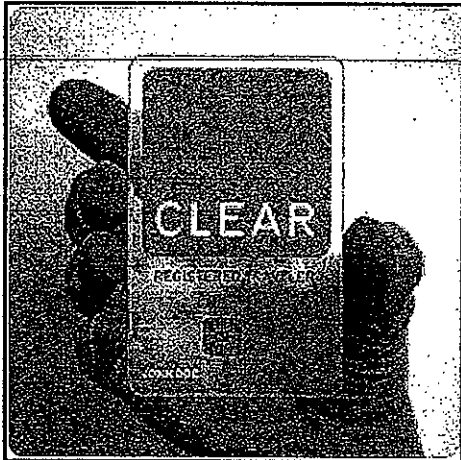
[Clear's Online Privacy Policy](#)

EXHIBIT C

Epicenter
The Business of Tech

Clear Promises to Delete Sensitive Flier Data, but No Refunds

By Ryan Singel June 23, 2009 | 6:32 pm | Categories: Investing, Startups



The airport security fast-track company Clear, which closed abruptly Monday night, belatedly assured customers Tuesday that their data was safe, while the company's main competitor dithered in the face of an opportunity to corner the market on getting people through airport security lines faster. Refunds of the \$200 annual fee, the company also noted, were unlikely.

Clear, the most popular Registered Traveler company, shut down its airport lanes Monday night with just a few hours notice, stranding some 250,000 subscribers to its jump-to-the-front-of-the-airport security-line program and leaving them wondering Tuesday about refunds and the fate of the sensitive data they'd given the company.

Clear members' concerns were real. Each of those travelers enrolled in Clear biometric identification program that let them enter the company's dedicated security lanes in 20 of the nation's busiest airports. That means that the company's databases have digital images of their fingerprints, irises and faces — along with date of birth, Social Security number, place of birth, gender, address, phone numbers, e-mail addresses, employer, driver's license number and height. Oh, and credit card numbers, too.

The company's website Monday simply said it had run out of money.

On Tuesday, no one knew what would happen with the sensitive data.

Clear's customer service line diverted to a message saying Clear is closed. The company's founder and former CEO Steven Brill claimed he doesn't know what happened to the company. The Transportation Security Administration, which licensed Clear, didn't know. GE, which invested more than \$16 million in the company, didn't know either.

And the company's acting CEO Jim Moroney knew, but did not return a message Wired.com left on his cell phone.

Finally, late in the afternoon Tuesday, someone at the company updated the website to say that Clear would delete the data.

Applicant and Member data is currently secured in accordance with the Transportation Security Administration's Security, Privacy and Compliance Standards. Verified Identity Pass, Inc. will continue to secure such information and will take appropriate steps to delete the information.

Clear's privacy policy (.pdf) seems to bar the company from selling the data, but does not say what happens if the company is liquidated or bought by another company. Nothing in the privacy policy explicitly prohibits a data-collection company from purchasing Clear just for its data on what is likely a largely well-heeled clientele.

Marc Rotenberg, who heads the Electronic Privacy Information Center, took the opportunity to pun off Deep Throat's Watergate mantra to follow the money.

"Follow the data! It's typically the primary asset," Rotenberg said. "And what makes this collapse particularly interesting is that the data is so detailed and was collected to promote national security. Now it could be heading for eBay."

Ari Schwartz of the Center for Democracy and Technology wondered also about the fate of users' data but seemed happy to have Clear cleared out of the nation's airports."

"All it really was was a lane for rich people to get on the plane faster," Schwartz said. "It had nothing to do with security."

Steven Brill, the company's founder, said he had no idea what happened, because he got forced out in February.

"I can only speculate about the causes of the company's demise," Brill said, though clearly he knows much more than the rest of the world. "What I do know for sure, however, is that the need for intelligent risk management hasn't diminished and that programs like Clear should have a role in our future."

What about the Registered Traveler program generally?

Clear was the most popular and well-known of the vendors in TSA's open Registered Traveler program, which required that all vendors' systems had to interoperate — at least for a few years.

Now that Clear is gone, what does the No. 2 company FLO have to say? Is it ready to snap up new customers and take over Clear's lanes?

It hardly sounds that way from the statement put out by FLO senior vice president Fred Fischer:

Flo is currently working with other participants in the industry as well as the Transportation Security Administration to analyze the implications of this announcement and to formulate a plan for the advancement of the program. We have no additional comment at this time but would expect to release further information pending additional discussions with the TSA.

What does the TSA make of Clear clearing out of the nation's airports?

“TSA has no comment on Verified Identity Pass’s announcement,” spokesman Greg Soule said by e-mail. “The Clear program was a market-driven, private sector venture offered in partnership with airports and airlines in certain locations.”

TSA, not surprisingly, never liked the program, which it viewed as competition, and never allowed the program to actually let so-called Registered Travelers actually skip any of the security checks that other passengers faced. That meant the security background check was simply for show, and TSA eventually abandoned the requirement.

Then-head of TSA Kip Hawley accurately described the RT program in 2008 as nothing more than “a front-of-the-line program with a good biometric ID.”

Ayal Vogel, a vice president at the biometric company Identica disputed even that assertion, arguing that Clear’s reliance on iris and fingerprints raised privacy issues that creeped out potential customers. Instead, the company should have been using technology like his company’s. It uses blood vessels under the skin to verify a person. That captured biometric avoids privacy questions, since it can’t be used for other purposes the way fingerprints can.

Signs of trouble came in March, when founder Steven Brill stepped down due to pressure from investors who led a financing round last fall. Those investors are still unknown and are likely to be the ones with the strongest claims to Clear’s assets, including any undeleted user data.

At the same time, lines at TSA had gotten better in many cities — with a few standout exceptions — cutting into the necessity for the cards. Add to that the dramatic decline in travel and the cutback in spending by individuals and corporations, and you have a recipe for large cash-flow problems.

While 250,000 paying customers sounds good, it’s not really not enough, not when you are trying to staff 20 airports, some with multiple checkpoints, from 4 a.m. to 11 p.m. daily.

For its part, Clear had long pushed for its card to do more, because its members had been vetted by the Transportation Security Administration to make sure they weren’t terrorists.

They wanted travelers to be able to be able to avoid getting picked for extra screening by computer algorithms and to keep their shoes and coats on. TSA was never convinced, and security experts derided the idea since it would not be hard for a terrorist organization to find ‘clean’ hijacking candidates who could get the cards.

Photo: Flickr/[RustyBrick](#)

Tags: [air travel](#), [biometrics](#), [Clear](#), [ebay](#), [privacy](#), [Registered Traveler](#), [TSA](#), [Venture Capital](#)
[Post Comment](#) | [Permalink](#)

EXHIBIT D



Clear's Privacy Policy

The Clear® Registered Traveler program ("Clear") is owned and operated by Verified Identity Pass, Inc., a privately held company. This program is operated in accordance with standards set and oversight conducted by the U.S. Government's Transportation Security Administration (TSA), a division of the Department of Homeland Security.

In this privacy statement, Clear explains the steps we take to protect the privacy, confidentiality, and security of personal information about our applicants and members.

If, after reading this explanation, you have questions or want further information, please contact Clear's Chief Privacy Officer.

1. WHAT INFORMATION WE COLLECT AND HOW WE USE IT

Participation in Clear is voluntary. If you choose to apply for Clear membership, we request certain information from you as part of the enrollment process which we retain and use in connection with the administration of Clear.

A. Initial application and identity verification. Applicants are required to provide certain basic personal information about themselves in order to initiate an application, some of which we are required by TSA to request. The information that TSA requires us to request is full legal name, other names used, Social Security number (optional), citizenship, Alien Registration Number (if applicable), current home address, primary and secondary telephone numbers, current email address, date of birth, place of birth, gender and height. TSA also lists as optional, but helpful, the following personal information: home addresses, driver's license number and employer's name and address.

All information that is related to you is encrypted when stored or in transit.

We recognize the sensitivity of all of this information. With respect to your Social Security number in particular, we take extra precautions to protect it. For example, your Social Security number is stored in a separate facility and device from the personal information that is needed for customer service issues. We have also used an extra layer of encryption to ensure the protection of your Social Security number.

TSA also requires Clear to request that applicants appear in-person with two forms of government-issued identification (one of which must contain a photo) – such as a passport or driver's license. We carefully examine these documents for authenticity using document inspection technology to detect tampering or counterfeiting. So that we have a complete record of your application, we store in a secure database the biographical information you supply and an image of the documents you submit to enroll. We use this information to provide customer service where your biographical information and document images are required, such as for card re-issuance.

In order to minimize the possibility of someone committing identity fraud, we are partnering with the American Association of Airport Executives' Transportation Security Clearinghouse and with nationally-recognized identity verification and fraud detection companies to compare the information you provide with publicly-available records such as telephone number listings, as well as personally identifiable information (but not any financial information) associated with credit reports. (We and our partners never collect or use financial information in any way in connection with Clear.) Our partner(s) will also check your name and other identifying information against global terrorist watch lists. Although we pass your biographical data through these identity verification processes, our partners have signed contracts agreeing not to retain, use or sell your data for any reason.

There may be one or more mismatches between your biographical data on the one hand, and the underlying public records on

the other. For example, your Social Security number may be linked in public records to a different name and address than the one you give us. This may be the result of someone having stolen your Social Security number or a clerical error, to name just two possibilities. In any case, we will be able to alert you to this and will be able to assist you in correcting any mismatch if it is an error.

Clear also collects an applicant's credit card information for membership payment. This information is collected solely for our use, although we must share it with a credit card processor to charge your credit card account. It is not transmitted to or shared with TSA, and TSA does not require its collection. As an extra precaution, your credit card information is stored in a separate facility from the personal information that we are required by TSA to request from you (described above).

B. Biometrics. Following successful initial identity verification, Clear takes your digital photo and digital images of all of your fingerprints and your irises and stores these images in your record in Clear's secure database – all in compliance with TSA requirements. If you are approved for Clear membership, your biometrics are used as part of our identity verification processes when you use your Clear card.

C. Enhanced Equipment. If you are using any of our enhanced equipment at the Clear lane, such as the shoe scanner, you may be issued a receipt to show the TSA officer at the lane whether you have been processed by that equipment. For example, the receipt might say that your shoes have been cleared and, therefore, that you do not have to remove them before going through the metal detector. The receipt has your digital photo on it to ensure that you cannot switch it with someone else. But it does not have your name, and the TSA requires its officers to destroy the receipts they collect by the end of each day.

D. Verification. When your Clear card is presented at the Clear lane kiosk, you are also asked to present your biometric — your fingerprint or your iris image — at the kiosk to make sure it matches the biometric embedded in the card. This is our way of making sure that the card actually belongs to you. If approval is granted, the Clear member's entry is authorized. For purposes of real-time maintenance and customer support (e.g., if your card doesn't work, we need to be able to run tests to understand why), we will maintain "log files" of entrances to local venues. However, we purge these records automatically on a daily basis, and we have designed our network so that neither we nor any of our subcontractors can track and record members' activities from location to location. Thus, Clear has developed a system that addresses customer service inquiries and system maintenance needs while still ensuring the privacy of our members.

2. INFORMATION SECURITY

Clear maintains (and we require our subcontractors to maintain) administrative, physical, and technical safeguards to help us protect your personal information and the integrity of our systems. Examples of the safeguards we employ include: Each of our employees and the employees of our subcontractors with access to personal information must pass a background investigation.

Each of our employees and the employees of our subcontractors with access to personal information is required to sign a confidentiality pledge promising to adhere to Clear's privacy rules and security procedures, with discipline up to and including dismissal for violations.

Each of our employees and the employees of our subcontractors with access to personal information receives Privacy and Fair Information Practices training (i) when they are hired, (ii) if the Policy is changed and (iii) annually.

Access to personal information of applicants and members by Clear employees and subcontractors is provided only on a need-to-know basis.

- We use user IDs, passwords and biometrics to regulate access to the personal information of applicants and members in our systems.
- We encrypt all personal information about applicants and members in our systems, both in transit and in storage.
- We apply firewalls to guard our computers against outside intruders.
- We conduct periodic data security audits. TSA also conducts periodic audits to ensure that we comply with their

standards for data security.

- We have a regular update process for anti-virus protection and implement operating system security updates for our network infrastructure.

3. ADDITIONAL LIMITATIONS ON APPLICANT AND MEMBER PERSONAL INFORMATION

A. We do not sell or give lists or compilations of the personal information of our members or applicants to any business or non-profit organization. We do not provide member or applicant personal information to any affiliated or non-affiliated organizations for marketing.

B. None of the information that we collect may be used for any purpose outside the operation and maintenance of the Clear Services.

C. We would only disclose personal information about members or applicants if required to do so by law or legal process.

4. APPLICANT AND MEMBER ACCESS

The Record of an applicant or member in the Clear system is a slim file — as already described. However, an applicant or member can request a copy of everything that we have in his or her information systems files for Clear identified to the applicant or member personally, and we will provide this information. If you believe that any of the information we have about you is inaccurate, please contact Clear Support at (866) 848-2415.

5. COMPLIANCE WITH OUR POLICIES

To assure members and potential members that Clear is following its Privacy and Fair Information Practices Policies, we have adopted these safeguard processes:

A. Independent Audit. To provide an independent professional and technical review of Clear's compliance with its Privacy and Fair Information

Practices Policies, including our data security procedures, we commission an annual outside audit from an Independent Public Accounting firm. That professional audit, and our response to it, is available to Clear members and the public who wish to see it. This privacy audit includes audits of any Clear subcontractors who are collecting or maintaining our data.

B. Annual Privacy Report. Our Chief Privacy Officer conducts a yearly privacy and data security report which is presented to Clear's CEO and its Board of Directors. This Annual Privacy Report, including any problems identified and steps to be taken to resolve those, is made available to Clear members upon request.

C. Identity Theft Warranty. Clear has put in place what we believe to be strong, effective measures to protect the security of the limited personal information we collect from applicants and members. Because we have implemented these measures and because the public is rightfully concerned about identity theft, we make the following promise to all applicants and members: In the highly unlikely event that an applicant or member is the victim of identity theft (defined as the taking of personal information of an applicant or member resulting in fraudulent transactions being made in the name of that applicant or member), resulting from any unauthorized dissemination by Clear or its subcontractors, or theft from Clear or its subcontractors, of the applicant's or member's personal data collected by Clear, we will reimburse the applicant or member for any otherwise unreimbursable monetary costs directly resulting from such Identity Theft. In addition, Clear will, at its own expense, offer any such applicant or member assistance in restoring the integrity of the applicant's or member's financial or other accounts.

D. Privacy Ombudsman. Clear has appointed an independent, outside Privacy Ombudsman, Law Professor Paul Schwartz, noted privacy expert and advocate. He will be identified to members as the person to contact if a member has a privacy complaint or privacy problem with administration of the Clear system or compliance with our published Privacy Policies. The Independent Privacy Ombudsman is empowered to investigate all privacy complaints, gather the facts, and respond to

members, as well as to post responses publicly and prominently on our website. He will also provide Clear's management with recommendations for resolving disputes in keeping with our Privacy promises. The Ombudsman can be contacted at www.flyclear.com.

E. Notice of Unauthorized Acquisition of Personal Information. We promise all members that we will notify them promptly as soon as we believe that any of their personally identifiable information has been acquired without our authorization. TSA will also be notified promptly of any such event.

F. Privacy Policy Changes. Finally, we pledge to notify all members by email of any material changes in our privacy policies, so that they can cancel their membership if they so decide. And so that members and others can see exactly what changes we have made, we also promise to make available online a "redline" copy that tracks all such changes. We post our current privacy policy on our website here.

6. WHAT HAPPENS TO YOUR DATA WHEN YOU ARE NO LONGER A MEMBER

When your account is cancelled for any reason, we will remove your personal information from our system automatically after 90 days. There are some limited exceptions. Our credit card processors require us to retain a record of the financial transactions we conduct for 24 months. This includes your name, credit card number, address, and email address, so we can notify you if the financial transaction is disputed. Also, a copy of your biometric information (but not your name) is retained by the Transportation Security Clearinghouse to prevent fraudulent enrollments under alternate identities.

If you apply for Clear membership online, but do not complete the enrollment process within nine months, we will then delete all of the personal information you provided during your initial application.

7. WEBSITE PRIVACY

We have a separate privacy policy related to the use of our website. You can access it by clicking here.

+++++

This is the U.S. Transportation Security Administration's Privacy Policy as it relates to the registered traveler Pilot Program. A copy will be distributed to applicants at enrollment.

TSA Privacy Act Statement

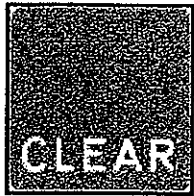
Authority: 49 U.S.C. 114 authorizes collection of this information.

Purpose: TSA is collecting this information from all individuals who apply to participate in the Registered Traveler program. TSA will use this information to verify your identity, to conduct and adjudicate a security threat assessment, and, if you are accepted into Registered Traveler, to conduct ongoing security threat assessments and to issue a "smart card" to you that will identify you as a Registered Traveler. Furnishing this information is voluntary. However, failure to provide it may delay or prevent the completion of your security threat assessment, without which you may not be permitted to participate in this program.

Routine Uses: The information will be used by and disclosed to TSA personnel and contractors or other agents who need the information to assist in the operation of Registered Traveler. Additionally, TSA may share this information with airports and airlines to the extent necessary to ensure proper identification, ticketing, security screening, and boarding of Registered Travelers. TSA may disclose information to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security. TSA may also disclose information pursuant to its published system of records notice, DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS) and DHS/TSA 015, Registered Traveler Operations Files, both of which were last published in the Federal Register on November 8, 2005, at 70 FR 67731-67736.

Effective as of October 1, 2008

EXHIBIT E



Search >

☐ select this link to skip main navigation

-
- [about clear](#)
 - [Airports](#)
 - [Enrollment](#)
 - [my account](#)
 - [help](#)

☐ select this link to skip local navigation

- [About Clear](#)
 - [Benefits](#)
 - [Member Testimonials](#)
 - [How Clear Works](#)
 - [Enrollment](#)
 - [CEO's Message](#)

Join our mailing list

Join now and receive updates as Clear opens new locations.
[read more >](#)

☐ [Enroll Now](#)

CEO's Message

Dear Clear members (and Potential members):

I want to tell you a bit about the background of our company and what Clear® is trying to do.

I started Verified Identity Pass with a simple idea: In the post 9-11 era we have to take new measures to protect ourselves yet not destroy our way of life by strangling the free flow of people and commerce. Somehow, we have to find common sense solutions that don't make everyone a suspect and create security bottlenecks everywhere we go. To be blunt, that means we need a fair, sensible way not to treat everyone the same when it comes to terrorism protection.

Because when it comes to security at an airport or any place else, we have to think about how we allocate scarce resources and time.

Security experts call this idea "risk management," by which they mean they concentrate more on greater threats and less on lesser threats. It does not mean risk elimination. Just because someone has no record of being a threat doesn't mean they might not suddenly become one (which is why you'll still go through the metal detector.)

At Clear, we see ourselves, first and foremost, as exactly that kind of common-sense risk management solution to the security bottlenecks that are the by-product of the post-September 11 world.

Second, we think we have a special responsibility to protect your privacy. Yes, we are using biometric identifiers such as fingerprints and iris images. Yes, your enrollment application will be submitted to the government for a basic security threat assessment before we can issue you a Clear card. But we do not believe the process and the questions stop there. We know that this kind of new idea and new process is bound to make many people uneasy about what we are doing with their personal information, especially at a time when every day seems to bring new headlines about identity theft. I started this company because I thought there was a right way to do something like this - a way that confronted privacy issues head on and embraced uncompromising dedication to privacy protection.

So, I urge you to read our privacy policies and what we believe are the innovative, no-strings-attached ways we've made ourselves strictly and publicly accountable for keeping them. They're in plain English. They're not in small print. In short, they're Clear. And we're as proud of them as we are of anything else about Clear.

Third, we try to be obsessive about customer service. We value your business, indeed your willingness to join us in this new venture. And we're determined to earn your loyalty in many ways - from an always-available pro rata refund, to a state of the art, 24/7 customer call center, to executives like me reaching out to customers at random and calling them (or greeting them at airports) to ask how we are doing. And if we don't deliver on that, please email me directly. As hard as we try, we're bound to make a mistake occasionally. I'd like to hear from you if we do.

Common sense security. Privacy. Obsessive customer service. Everyone at Clear is determined to stand for all of that and more. When you join Clear, we want you to think you're signing on with a new service that has real value - and real values.

Sincerely,



Steven Brill
CEO, Verified Identity Pass, Inc.

[Corporate Information](#) [Online Privacy](#) [Press Room](#) [Careers](#) [Contact](#) [Site Map](#)
[privacy policy](#)

Verified Identity Pass, 600 Third Avenue, 10th Floor, New York, NY 10016

Copyright © 2007 Verified Identity Pass, Inc. All rights reserved.

Use of this website signifies your agreement to the [Terms of Use](#) and [Online Privacy Policy](#) (updated 10-17-2007).

EXHIBIT F



One Hundred Eleventh Congress
 U.S. House of Representatives
 Committee on Homeland Security
 Washington, DC 20515

June 25, 2009

Ms. Gale Rossides
 Acting Assistant Secretary
 Transportation Security Administration
 East Building, 601 South 12th Street
 Arlington, VA 22202-4220

Ms. Rossides:

On June 22, 2009, the Committee on Homeland Security received notification that Clear, which is owned by Verified Identity Pass, Inc., and is the largest Registered Traveler (RT) service provider, will cease operations and will, therefore, no longer staff its lanes at airports across the country.

This year, Clear operated in 20 airports, with approximately 165,000 members. While we recognize that Clear is not a government program managed by TSA, we are concerned about the protocols Verified Identity Pass will implement in the next few days as Clear winds down. Specifically, we are concerned about the handling of personal-identity information possessed by Clear. Additionally, we are interested in TSA's involvement in the closing of Clear.

Even though RT is a private sector program, TSA used its authority to mandate requirements on service providers, including Clear. These requirements included obtaining personally identifiable information such as an individual's legal name, citizenship status, Alien Registration Number, current home address, date and place of birth, gender, and height.¹ Additionally, TSA required Clear to request that applicants appear in person with two forms of government issued identification, such as a passport or driver's license. Clear also stored images of the documents submitted by applicants. Importantly, TSA conducted periodic oversight through audits and promulgated reporting requirements.

While TSA mandated many data collection requirements for these private sector service providers, it appears that TSA allowed the private sector to determine a method of storage and disposal of extremely sensitive personal information. It is our understanding that TSA's directives are silent on the disposal of data in the event of a company's merger, buy out, or bankruptcy.

¹ Transportation Security Administration, TSA Registered Traveler Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers Version 3.1, January 2008, page 20.
<http://www.tsa.gov/approach/rt/index.shtml>, June 24, 2009.

Given Clear's status, we write to acquire information on the actions TSA intends to undertake. We are concerned about the security and safety of the information currently held by Clear. Specifically, we need to understand the role TSA will play in assuring that adequate privacy protections are in place prior to any disposition of the personally identifiable information of over 165,000 people. Needless to say, the sale, disposal, transfer, or destruction of this type of data cannot be undertaken without safeguards designed to ensure that the information will not be compromised.

Many members of the traveling public have trusted TSA's RT program. This level of trust can only be maintained by TSA providing clear and proper protocols to govern the disposition of data when an RT provider decides to leave the program. Pursuant to Rule X(3)(g) and Rule XI of the Rules of the House of Representatives, please respond in writing to the following questions:

- 1) When was TSA notified that Clear was ceasing its operations?
- 2) Has TSA requested Verified Identity Pass' plan for secure document deletion, destruction, or transfer? If so, please provide a copy of this plan to the Committee.
- 3) Has TSA contacted the DHS Chief Privacy Office and requested a Privacy Impact Assessment on the cessation of Clear's service?
- 4) In its Security, Privacy, and Compliance Standards for the RT program, TSA requires its RT program service providers to follow the Fair Information Principles with regard to privacy. These standards require RT service providers to provide an incident report to their various stakeholders when there is a loss of control of privacy information or when there is potential access to personally identifiable information. Since Clear has ceased its operations, will Verified Identity Pass, or any other relevant entity, be required to provide an incident report?
- 5) Since Clear has ceased operations for the RT program, has TSA implemented a contingency plan for safeguarding the personally identifiable data in the event other RT service providers suffer the same fate as Clear?
- 6) It is our understanding that even after all Clear kiosks have been cleared of all membership information and personal information, Verified Identity Pass will still have its core membership database maintained by Lockheed Martin. Has TSA been in contact with Verified Identity Pass to determine how long it plans to maintain its core membership database? Has TSA been in contact with Lockheed Martin and obtained a copy of its plan for keeping the personally identifiable information secure?

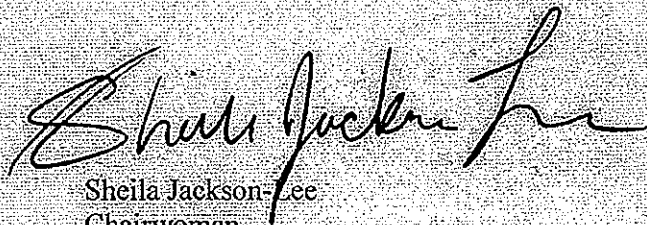
We understand that the Clear was not run by TSA. However, it was a part of TSA's RT program. It collected information pursuant to TSA guidelines, and TSA received fees collected by Clear. Moreover, Clear's customers are also customers of TSA. Therefore, having been integrally involved and obtained a benefit, TSA has a responsibility to meticulously oversee Clear's cessation of operations.

Please respond to the questions by July 8, 2009. If you have any questions, contact Cherri Branson, Chief Oversight Counsel, at 202-226-2616.

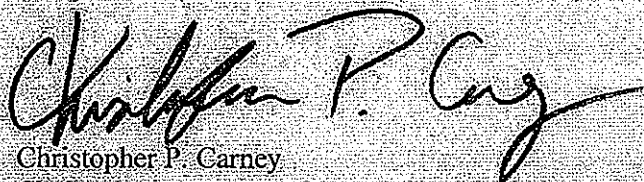
Sincerely,



Bennie G. Thompson
Chairman
House Committee on Homeland Security



Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation Security
and Infrastructure Protection



Christopher P. Carney
Chairman
Subcommittee on Management, Investigations, and
Oversight

EXHIBIT G

JOHN D. ROCKEFELLER IV, WEST VIRGINIA, CHAIRMAN

DANIEL K. INOUYE, HAWAII
JOHN F. KERRY, MASSACHUSETTS
BYRON L. DORGAN, NORTH DAKOTA
BARBARA BOXER, CALIFORNIA
BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
FRANK R. LAUTENBERG, NEW JERSEY
MARK PRYOR, ARKANSAS
CLAIRE MCCASKILL, MISSOURI
AMY KLOBUCHAR, MINNESOTA
TOM UDALL, NEW MEXICO
MARK WARNER, VIRGINIA
MARK BURGESS, ALASKA

KAY BAILEY HUTCHISON, TEXAS
OLYMPIA J. SNOWE, MAINE
JOHN ENSIGN, NEVADA
JIM DEMINT, SOUTH CAROLINA
JOHN THUNE, SOUTH DAKOTA
ROGER F. WICKER, MISSISSIPPI
JOHN W. ISAKSON, GEORGIA
DAVID VITTER, LOUISIANA
SAM BROWNBACK, KANSAS
MEL MARTINEZ, FLORIDA
MIKE JOHANNIS, NEBRASKA

United States Senate

COMMITTEE ON COMMERCE, SCIENCE
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEB SITE: <http://commerce.senate.gov>

ELLEN DONESKI, CHIEF OF STAFF
CHRISTINE KURTZ, REPUBLICAN STAFF DIRECTOR AND GENERAL COUNSEL

June 26, 2009

Ms. Gale Rossides
Acting Administrator
Transportation Security Administration
U.S. Department of Homeland Security
61 South 12th Street
Arlington, VA 20598

Dear Acting Administrator Rossides:

Verified Identity Pass, Inc., (VIP) ceased its operations as a provider of the Transportation Security Administration's (TSA) Registered Traveler (RT) program on June 22, 2009. VIP provided this service through its Clear program. As you are aware, the RT program permits an airline passenger to be expedited through airport security with the use of a biometrically verifiable and encrypted smart card. This biometric identification provides airport and TSA officials greater certainty regarding the identity of an airline passenger. It is my understanding that total RT enrollment in VIP's Clear program exceeded 200,000 individuals.

To enroll in the RT program individuals are required to provide personal information, including biometric data and credit card information, and submit to a background check. Given the sensitive nature of the information collected by VIP through its Clear program, I have concerns regarding how the company will dispose of its clients' personal information. Such information in the wrong hands could lead to identity theft, and have severe consequences for VIP's clients.

Accordingly, I am requesting that you carefully review what steps VIP is taking to make certain the personal information it has collected from its clients is disposed of properly. I am also asking that you review the guidelines that govern the RT program to make sure that all RT providers have processes in place to dispose of client information in a safe and appropriate manner in the event that the company ceases its RT operations. Additionally, I am interested in knowing if the clients of RT providers have the ability to reclaim their fees when a provider ceases RT operations.

I appreciate your cooperation in addressing these matters.

Sincerely,


John D. Rockefeller IV
United State Senator