



**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.

¹Transportation 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.shtm>. 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.

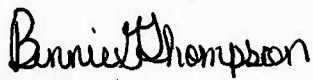
Many members of the traveling public have trusted TSA's RT program. This level of trust can only be maintained by TSA providing clear and proper protocols to govern the disposition of data when an RT provider decides to leave the program. Pursuant to Rule X(3)(g) and Rule XI of the Rules of the House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

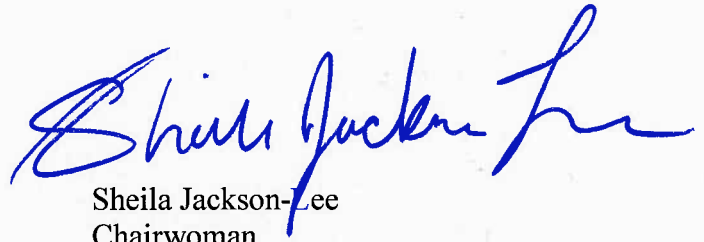
We understand that the Clear was not run by TSA. However, it was a part of TSA's RT program. It collected information pursuant to TSA guidelines, and TSA received fees collected by Clear. Moreover, Clear's customers are also customers of TSA. Therefore, having been integrally involved and obtained a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