

VIP's Clear Demise Leaves Fate of Personal Data Unclear

John Girard, Avivah Litan

The abrupt demise of Clear, a fast-track airport security system for U.S. travelers, raises serious questions regarding the private and secure disposal and transfer of databases full of sensitive information.

NEWS ANALYSIS

Event

On 21 June 2009, Verified Identity Pass (VIP) announced on its Web site that it was ending business operations of its Clear service at 11 p.m. Pacific Standard Time on 22 June 2009. The Clear service allowed airline passengers to move quickly through security lines at U.S. airports in exchange for an annual fee. The company said that it has signed up more than 260,000 travelers since its inception four years ago and processed more than 2.5 million passengers through its Clear lanes in airports. VIP has taken down its regular Clear Web site and says it is unable to issue refunds.

Analysis

Clear was the most visible private company to provide expedited screening services authorized under the Registered Traveler (RT) program, which is a private/public partnership with the U.S. Transportation Security Administration (TSA). The RT program led to the Registered Traveler Interoperability Consortium (RTIC), which established standards and regulations for Clear and other private enrollment providers.

According to a preliminary statement on the Web site, VIP was unable to negotiate an agreement with its senior creditor to continue operations. Gartner believes that Clear failed to grow its enrollment fast enough to overcome operating costs for a number of reasons, including the high cost of terminal floor space in airports; its limited service to approximately 20 airports; its high price (\$199 per year) compared to the benefits for constant flyers; and some travelers' cautiousness regarding surrendering large amounts of personal data to government entities, especially when biometrics are involved.

Individuals who enrolled in Clear have larger concerns than their lost membership fees. A combination of government and private sources has access to the data gathered by service providers. The information policy on the RTIC's Web site is limited to the statement that service providers such as Clear "must establish a written privacy policy, in accordance with the Fair Information Practice Principles, to govern the data collected in connection with RT, and will be required to provide this policy, in writing, to each eligible RT applicant." But RTIC's Web site doesn't address the critical issue of data disposal. Neither the TSA nor the RTIC have issued statements on the disposal of Clear's data stores.

After the announcement, Clear's first action was to send an e-mail with no reassuring information about data handling or refunds. In a subsequent e-mail and Web site update (see www.flyclear.com for details), Clear provided a partial outline of the processes of data disposal and oversight. But Gartner believes the company needs to offer additional clarification to explain how its databases and servers will be secured and shut down, and how Clear's information might be transferred in the future to another RT program provider. When a company like Clear shuts down rapidly and without a transparent process for the disposal of data collected on its kiosks, workstations and servers, Gartner believes its customers have good reasons to demand that the company properly validates and oversees the handling of this sensitive data.

RECOMMENDATIONS

- **Clear customers:** Contact Clear's parent company, VIP and the TSA to demand an explanation of how the company's stored data will be copied, stored and used in the

future. Contact other TSA-approved RT service providers, which may arrange to support the Clear card.

- **Private and government entities that collect personal information (including biometric identifiers):** Plan ahead for downturns. Formulate a clear plan on the auditing and destruction of collected data and implement a process for informing all parties of the final disposition.
- **Corporate counsels and lawmakers:** Ensure that future rules for data security and privacy enforce responsible disposal of data.

RECOMMENDED READING

- "Protect Privacy and Data Security With Data Sanitization" — Disposal of PCs without proper disk-cleansing processes in place leads to security exposures and unnecessary risks for your organization. **By Frances O'Brien and Leslie Fiering**
- "Selecting an IT Asset Disposition Service Provider" — Carefully evaluate and select a service provider for asset disposition, because consolidation in this market means the provider you select may not be the one you end up with tomorrow. **By Frances O'Brien**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509