



## 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](http://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