



PRODUCT SECURITY


Designed to Mitigate Risks


Manifest's transfer process is designed to help users consolidate their retirement savings easily while reducing risk and preserving control throughout the process. Our risk mitigation steps sits on top of existing controls that are

built into the transfer process by providers. Our easy digital solution combined with our risk mitigation steps provides a trusted transfer solution for our users.

-  **Verify Account Ownership**

Manifest performs a number of checks to verify the user owns the retirement account they are linking and is authorized to initiate a transfer. We gather personally identifiable information such as address, SSN directly from the user and require additional account statements or SSO authentication to confirm account ownership.
-  **Preserve Control**

Manifest has "read only" access to account data and does not have the ability to make any changes. Our application acts as a concierge service and highlights destination options for our users. We can not touch money in any part of the transfer process. Users preserve control on their savings and how they are invested.
-  **Prevent Fraud**

Manifest transfer process adds more layers of fraud prevention on top of the current industry standard procedures. We start with multi factor authentication for user security and only support direct rollovers. Providers have already created a number of processes to prevent transfer frauds and Manifest initiated transfers would go through the same process.
-  **Protect User Information**

Our experienced team of technologists and retirement professionals understand the need to incorporate key security features into each part of our infrastructure from day one. We protect all user data both in transit and at rest in accordance to data protection and compliance standards. We employ strict encryption processes, the same ones used by financial institutions.

PRODUCT SECURITY

Modern Security Standards Built-In

We designed Manifest's architecture to keep high reliability, scalability, and security standards at the forefront. At a foundational level, we gather and retain the absolute minimum information required to transfer a user's account.

As a neutral party, we can play a key role in developing and enforcing uniform security standards in partnership with technology teams at big and small financial institutions.



Service levels and backups

Manifest's infrastructure utilizes many layered techniques for increasingly reliable uptime, including the use of auto-scaling, load balancing, task queues, and rolling deployments. Every day, we automatically back up our databases, and all of these backups are encrypted.



Application architecture

The Manifest web application is tiered into logical segments (front-end, mid-tier, and database), which are all separated from one another and hosted in a private VPC. This guarantees maximum protection and independence between layers.



Employee access

We have strict access controls for the employees supporting our customers. Our tools are designed to reduce the need for direct access or manual data processing. We follow the principle of least privilege in how we write software and abstract away data from functionality, reducing employee need for access to user information.



Servers and networking

All our servers are hosted in Amazon AWS, and are comprehensively hardened AWS Infrastructure-as-a-Service (IaaS) platforms. All the software we run in production are modern, continuously-patched Linux systems.



Physical security

Manifest data centers (handled by Amazon AWS) are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to its AWS platform and infrastructure.



User Information

Because we gather and retain only a small amount of information, we protect user data both in transit and at rest. We employ strict encryption processes, the same ones used by financial institutions.