Outseer Security & Privacy

Frequently Asked Questions

Version 1.0 - August 2023

Corporate Security & Privacy

Does Outseer have a formal information security and/or privacy program in place?

Yes. Outseer has a formal information security program in place which aligns with various industry standards including PCI-DSS and NIST (National Institute of Standards and Technology).

Which Security standards and certifications does Outseer comply with?

The Outseer 3-D Secure service undergoes annual independent assessments against PCI-DSS and PCI-3DS. Additionally, the offering is independently audited against the AICPA (American Institute of Certified Public Accountants) Trust Service Criteria of Security, Availability, and Confidentiality for SOC 2 Type II.

The Outseer Fraud Manager on Cloud service is independently audited against the AICPA Trust Service Criteria of Security, Availability, and Confidentiality for SOC 2 Type II.

Does Outseer have dedicated Security personnel?

Yes. Outseer's security practices are overseen and implemented by our Security and Risk office which is led by our CISO and is made up of resources in our Security Operations and Governance Risk and Compliance (GRC) teams.

Is Outseer SOC2 Compliant?

Yes. Outseer's hosted offerings, 3-D Secure and Fraud Manager on Cloud undergo annual SOC 2 Type II audits against the AICPA Trust Service Criteria of Security, Availability, and Confidentiality.

Is Outseer PCI (Payment Card Industry) Compliant?

Yes. Outseer 3-D Secure undergoes annual PCI-DSS and PCI-3DS Assessments with independent third-party QSA (Qualified Security Assessor) firms.

Is Outseer ISO certified?

No. Outseer does not currently undertake ISO certification.

Does Outseer have an information security awareness program?

Yes. Outseer employees undergo security awareness training as part of the new hire onboarding process and current employees undergo training on a quarterly basis in security awareness. In addition, Outseer developers undergo annual secure.

Does Outseer perform background checks on all personnel with access to Customer data?

Yes.

How frequently are Outseer's information security related policies reviewed?

Outseer reviews and updates (where necessary) all information security related policies on an annual basis.

Do you have a Privacy Policy?	Yes, you can find the Outseer privacy policy here.
Is Outseer a Processor, Controller, or both?	Outseer is a processor.
What type of data does Outseer collect?	Outseer Fraud Manager on Cloud requires that anonymized data be provided by the data controllers. Outseer 3-D Secure utilizes data that is required by the EMVCo 3-D Secure protocol. Overall, no sensitive data must be sent to Outseer.
Does Outseer engage any third parties (sub-processors) who will have access to the personal data you share with us?	Outseer maintains a listing of its sub-processors which can be found here.
Does Outseer have a Data Retention and Disposal Policy	Yes.
Does Outseer have a formal incident response process?	Yes. Outseer's Incident Response Plan sets forth internal guidelines for detecting incidents, escalating them to the relevant personnel, communication (internal and external), investigation, mitigation, and root-cause analysis.
Do you have cyber insurance?	Yes.
Where are your legal entities based?	-RSA Security LLC (for: US and Latam customers) -RSA Security UK Limited (for: UK customers) -RSA Security Australia Pty. Ltd. (for: Australian customers) -RSA Security Canada LLC (for: Canadian customers) -RSA Security & Risk Ireland Limited (for: EMEA; APJ; and rest of world customers) Outseer complies with all relevant laws and regulations within these countries.

Application & Infrastructure Security

Do you perform penetration testing on your environment? How often is it performed

Yes. Outseer engages independent third-party penetration testing service providers on an annual basis to test both the 3-D Secure and Fraud Manager on Cloud services. An executive summary of the testing results is available upon request for Outseer customers under NDA (Non-Disclosure Agreement). Please contact your Account Manager to request this documentation.

Does Outseer secure its users' access into its hosted offerings?

Yes, Outseer implements a variety of controls for securing user access into the Outseer hosted offerings. Please reference the hosted offering specific relevant audit reports for specific details on controls.

Do you encrypt customer data in transit and when stored?

Yes.

How does Outseer ensure that its code is being developed securely?

Outseer utilizes OWASP (Open Web Application Security Project) Top 10 and CVSS (Common Vulnerability Scoring System) standards to build in security for our software development lifecycle. All code

Does Outseer perform application security testing?

Yes. Outseer engages independent third-party penetration testing service providers on an annual basis to perform application penetration testing on the 3-D Secure and Fraud Manager cloud services.

Where are Outseer's data centers located?

The Outseer 3-D Secure offering is hosted within third-party data center locations in either the US or EMEA (Europe, Middle East, and Africa) region depending on customer implementation. The Outseer Fraud Manager on Cloud offering is within the Microsoft Azure cloud environment either in the US or EMEA regions depending on customer implementation. Please work with your account manager for further details on data center locations.

Do you have a Business Continuity and Disaster Recovery Plan?

Yes. Outseer's hosted offerings have product specific Business Continuity and Disaster Recovery plans implemented. These plans are reviewed and tested annually in line with industry standard best practice.

Does Outseer support secure deletion of customer data?

Yes. Outseer ensures data deletion processes align with DOD (Department of Defense) 5220.22M secure deletion standards. All data must be securely erased after the useful life of the data. Certificates of Destruction are obtained where required.