

CIP vendor and sub-vendor declaration:

A portion of our Customer Identification Program (CIP) is provided by HyperVerge [www.HyperVerge.co].

222 West Las Colinas Boulevard
Suite #755E
Irving, TX 75039
contact@hyerpverge.co

Below are the attestations provided by HyperVerge with regards to their application and their sub-vendors.

HyperVerge is certified for ISO 27001, ISO 27018, ISO 30107-3 and SOC 2 Type 1.

ISO 27001 is a standard for information security management. It helps organizations to protect their information assets and comply with legal and contractual obligations. It also guides organizations to improve their information security practices. ISO 27001 certification is a way of demonstrating that an organization's information security system meets the standard's requirements.

ISO 27018 is a standard for cloud privacy. It helps cloud service providers to protect the personal data of their customers and comply with the privacy principles in ISO/IEC 29100. It also helps cloud service customers to choose and audit the cloud services they use. ISO 27018 is based on ISO/IEC 27002, but adds specific controls for personal data in the cloud.

ISO 30107-3 is a standard for testing biometric presentation attack detection (PAD). It helps biometric system developers and evaluators to measure and report the performance of PAD mechanisms against different types of presentation attacks. It also provides a classification of known attack types, such as artefacts, impersonation, and concealment. ISO 30107-3 is based on ISO/IEC 27002, but adds specific requirements for biometric systems. ISO 30107-3 applies to both local and cloud-based biometric solutions.

SOC 2 Type 1 is a report that evaluates the design and suitability of an organization's security controls at a specific point in time. It is based on the Trust Services Criteria, which are standards for security, availability, processing integrity, confidentiality, and privacy. SOC 2 Type 1 is useful for demonstrating that an organization has implemented security policies and procedures that align with industry best practices and customer expectations. SOC 2 Type 1 is different from SOC 2 Type 2, which also tests the operating effectiveness of the controls over a period of time. SOC 2 Type 1 is voluntary and not required by any regulation, but it can help an organization to build trust and credibility with its customers and partners.

HyperVerge sources certain ID Verification (IDV) related services from other third parties to augment the utility of its own KYC platform:

“Microblink” to augment optical character recognition (OCR) [<https://microblink.com/>]

“Comply Advantage” for AML including the Office of Foreign Assets Control (OFAC) check of the US Department of the Treasury [<https://complyadvantage.com/>]

“ID Scan” does government ID database checks like Social Security Number Verification Service (SSNVS) and American Association of Motor Vehicle Administrators’ (AAMVA) Driver License Data Verification (DLDV) System [<https://idscan.net/>]

HyperVerge could add or replace third party vendors in the future, but agrees to inform us of any changes.

Regarding the cross-border transfer of data. When HyperVerge's Case Management Portal is used for the review of new account application data, certain textual data crosses U.S. borders. However, they assure us that the data does not persist and is purged immediately. The OFAC (AML) service provided by ComplyAdvantage does currently involve data transfer beyond the U.S. as this information is processed in Ireland; however, HyperVerge is working to bring this back to the U.S. within 4 to 6 weeks (December 2023). With respect to individual modules like OCR, Liveness, FaceMatch, Government Database checks, these services do not involve any cross-border data transfer.