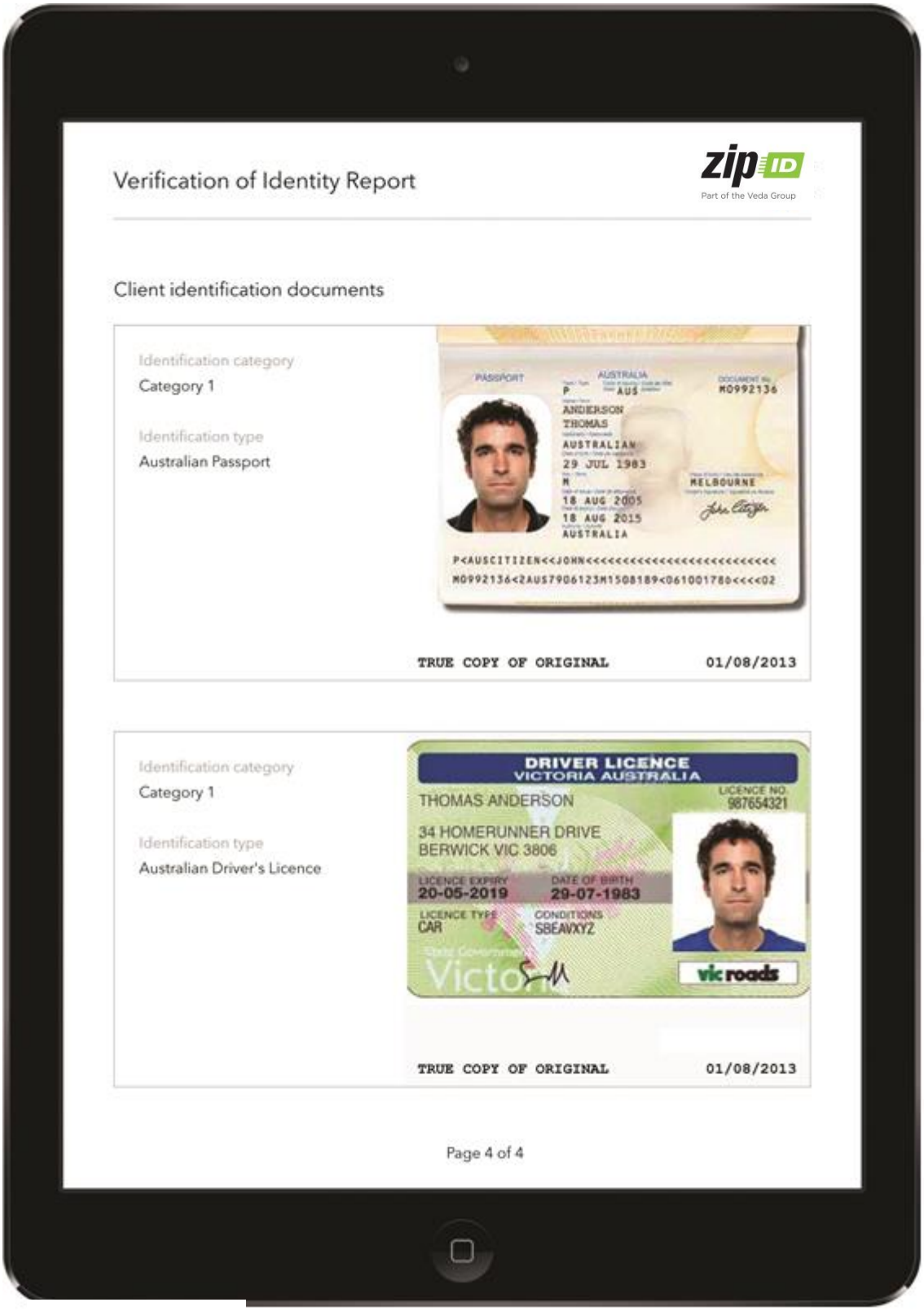
ZipID App Compliance Summary



ZipID App Compliance Summary

Requirement	How it works?
Face-to-face in person interview	The ZipID digitised and mobilised face-to-face verification solution is used by the authorised broker to perform the identity check of the client in person.
Categories of ID documents used	All categories of eligible documents are satisfied. IDwizard™ will guide brokers with selecting compliant ID document categories using the correct hierarchy.
Retention of copies of ID documents	High resolution true copies of the original ID documents are captured and retained by the broker and lender as digitised evidence. Note: the solution maintains a geolocated and time stamped audit trail of each broker who conducts the ID check. No identity information is stored locally on the mobile device (see security credentials below).
Further checks	The solution captures a photograph of the person being identified and the signature of the person being identified using a stylus. This assists best practice fraud mitigation. The client's signature can be compared by the lender / assessor against signatures on the identity documents and also on subsequent transaction instruments or other documents (if applicable). Reports are also digitally signed by the App user (i.e. broker), providing proof of who authored the report and validation that the report contents have not been tampered with.
Compliance with Privacy Laws and Information Security	The solution is supported by secure digitised data management. This is crucial to managing security and is superior practice to use of browser-based upload methods, emailing over open networks, using devices which store data locally, or relying on paper record keeping of identity information. The solution contains prompts to enable the broker to confidently and consistently explain key elements of the process including data security to the person being identified. The solution is part of a secure purpose-built data workflow and information management environment housed in AWS Sydney. Identity data is encrypted in transit and at rest using AES-256 bit SSL (Secure Sockets Layer). The solution creates a comprehensive transaction trail between parties. The solution tracks and timestamps various information from the moment data is submitted to when it is completely verified, such as IP addresses; user information and geo-location. Programmatic third party penetration testing and vulnerability assessments are in place.