Ekata Identity Network Security & Privacy

Maintaining the privacy and security of personal data is paramount to Ekata. To ensure the privacy of our customers and their sensitive data, the Ekata Identity Network operates on highly obfuscated data. Our industry leading solution enables us to provide the enormous benefit of our data sharing cooperative comprised of our thousands of customers while dramatically reducing our customer’s privacy, regulatory, and security risk.

Data Security and Privacy Protections

All interactions between our customers and Ekata services are encrypted to meet or exceed the Payment Card Industry standards. Within our secure cloud environments, personal information is securely hashed and encrypted using NIST recommended methodologies.

- Encryption in Transit
  - TLS 1.1 or higher
- Personal Information Obfuscation
  - SHA-2 512 hashing
- Encryption at rest
  - KMS managed AES-256

Breach Protection

In addition to strong cryptographic hashing, an additional layer of encryption at the individual field level is employed to prevent lookup table attacks in the event of a breach. Lastly, the full data set is stored encrypted at rest. Both encryption layers are managed via AWS KMS, where the master key is stored within a Hardware Security Module (HSM), and use of its decrypt function is restricted and alarmed.
About Identity Network

The proprietary Ekata Identity Network is derived from historical transactions and feedback data from our global risk conglomerate of thousands of customers. Our Identity Network leverages sophisticated data science and machine learning to provide unique insights that improve the accuracy and predictability of our identity verification solutions.