



Empowering Financial Services with VEDS:

A Vanguard in Fraud Detection and Prevention

As financial services increasingly embrace digital transformation, the imperative for secure, efficient and compliant data sharing has never been more critical. In this digitally-driven era, marked by sophisticated cyber threats and stringent regulatory demands, Vaultree Encrypted Data Sharing (VEDS) empowers financial institutions to securely share and analyse encrypted datasets, unlocking new frontiers in industry-wide fraud detection while driving innovation without compromising data security, sovereignty or veracity.

The Fraught Landscape of Financial Fraud

A recent report by Kroll highlights a 35% increase in unauthorised payment fraud and account takeover (ATO) in 2023 alone. Additionally, KPMG, in their recent 'Global Profiles of the Fraudster' report, revealed that financial services, on average, faced a cost of \$5 million per fraudster. These worrying statistics show two things: the financial sector's battle against fraud is intensifying, and traditional defences or preventative measures are falling short.

Compounding the challenge is the sector's fragmented approach to fraud detection, with critical intelligence remaining siloed due to security and regulatory constraints.

Introducing VEDS: Secure, Collaborative Data Analysis

Vaultree Encrypted Data Sharing (VEDS) is a transformative solution for secure, enterprise-scale data sharing. At its core, VEDS enables different companies to share and merge datasets in an encrypted form, utilising their own encryption keys and Key Management Systems (KMS); VEDS empowers customers to retain complete control of their data at all times.

This approach secures sensitive data throughout the sharing process, meeting the essential requirements for privacy and compliance in the modern, data-driven landscape. Additionally, while customers can choose Vaultree for key management and encryption, there's no requirement for an ongoing licensing commitment, offering flexibility in how they manage and secure their data while ensuring that sensitive data remains secure throughout the sharing process, addressing the critical need for privacy and compliance in today's data-centric world.

Key Features of VEDS

Multi-Key Encryption and KMS Integration

Ensures unparalleled control and security over data, with seamless integration with existing Key Management Systems.

Operational Efficiency:

VEDS's sophisticated encryption processes ensure data remains analytically useful while minimally impacting performance, making it a perfect fit for the fast-paced financial sector.

Central Governance for Secure Sharing:

Simplifies the management of permissions and access controls, granting the data owner full control throughout the entire process. This enhances data governance, streamlining collaborative efforts in fraud detection.

VEDS: A Competitive Edge in Financial Services

Secure, Collaborative Fraud Detection

Encrypted Data Sharing: VEDS leverages Vaultree Data-In-Use Encryption to allow for the sharing and analysis of encrypted datasets. This means that financial institutions can exchange information on fraud patterns without ever exposing the raw data. The data remains encrypted at all times, ensuring that sensitive information is never at risk.

Multi-Key Encryption System: The platform employs a multi-key encryption service, where each participating institution uses its own set of encryption keys and Key Management Systems (KMS). This unique approach guarantees that only authorised users within each organisation can access their data, enhancing security and control over sensitive information.

Collaborative Intelligence: By facilitating a secure environment for data exchange, VEDS enables the creation of a collective intelligence network. Financial institutions can pool their insights to gain a comprehensive understanding of fraud tactics and collaboratively develop more effective detection and prevention strategies.

Trust and Sovereignty: VEDS was built with a 'Zero Trust' model that transforms competitive dynamics within the financial sector, enabling institutions to collaborate on fraud detection while maintaining strict data control and sovereignty. Integrated with Key Management Systems (KMS), VEDS ensures that each participant retains absolute control over their data. This control, combined with ensured data veracity through comprehensive audit logs and granular access controls, lays a strong foundation of trust among collaborating institutions.

Driving Innovation Through Secure Data Utilisation

platform's secure data-sharing capability allows institutions to collaborate on developing new financial products, services, and technologies. By securely pooling datasets, institutions can leverage AI and ML models to uncover insights into consumer behaviour, market trends, and operational efficiencies. This collaborative innovation, grounded in data security and privacy, paves the way for breakthroughs that can reshape the financial services landscape.

VEDS's architecture, designed for seamless integration and scalability, ensures that as collaborative projects grow and evolve, the platform can adapt without compromising performance or security. This flexibility is key to supporting the dynamic nature of financial services, where agility and responsiveness to market changes are critical competitive advantages.

Infrastructure Agnostic Design

VEDS is able to seamlessly integrate across various IT landscapes. This infrastructure-agnostic flexibility allows VEDS to be deployed anywhere within an organisation's architecture, from on-premises systems to cloud platforms like Google BigQuery, without the need for disruptive changes or re-auditing. This adaptability is critical for financial services, where the IT environment can be complex and varied across institutions. By supporting a wide range of infrastructures, VEDS ensures that financial organisations can leverage its encrypted data-sharing capabilities regardless of their existing IT setup, facilitating smooth collaboration and innovation efforts.

organisations can leverage its encrypted data-sharing capabilities regardless of their existing IT setup, facilitating smooth collaboration and innovation efforts.

Cost Efficiency and Regulatory Compliance

VEDS addresses the financial sector's need for cost efficiency and regulatory compliance. By streamlining the data sharing and analysis process, VEDS reduces the operational overhead associated with traditional data protection methods. The platform's compliance with global data protection regulations, including GDPR and FINRA, simplifies the complex landscape of regulatory adherence for financial institutions, allowing them to focus on core business objectives without the burden of compliance risk.

Vaultree Encrypted Data Sharing: Securing the Future of Finance

VEDS not only equips financial institutions with the tools to effectively combat fraud but also opens avenues for secure, collaborative innovation. This dual capability is indispensable in an era where data is both a valuable asset and a potential liability.

To find out more about VEDS and how Vaultree is driving innovation and security in financial services, contact Vaultree today.

Contact Information

For further information, troubleshooting and signposting through Vaultree, please contact:

Solutions Team

solutions@vaultree.com