Use Case: FinTech Customer Information Protection

The Gramm-Leach-Bliley (GLB) Act imposes data security and data-sharing standards on U.S. businesses that engage in general categories of ‘‘financial’’ activities. In addition, many U.S. states, New York, New Jersey, Connecticut, Massachusetts, and California, have supplemented GLB with the ‘‘money transmitter’’ laws to cover financial technology or “FinTech” companies.

> “Financial companies must…ensure the security and confidentiality of customer information and to protect against unauthorized access to or use of that information, both by third parties and your own employees.”

This means GLB places responsibility for data security directly with the board of directors and for public companies, the Sarbanes-Oxley Act makes the CEO and CFO responsible. With alarming frequency, new reports of serious breaches reveal that concentric or layered security architectures based on detection, protection, and transportation technologies are simply inadequate. In many cases, human error plays the largest role from misconfiguration, fraudulent scams, and even intentional security violations. Making this problem even more complex to solve, leading global Fintech companies are proactively turning to cloud technology in an attempt to meet increasingly stringent compliance regulations. This is not to say historical banking institutions do not face the same security challenges because they both offer Internet-connected customer services and data access to traders and other brokers. Nevertheless, any data breach, no matter how small, can result in direct liability to a company and its officers.

Interoperable with existing security products and processes, the best practice to ensure data protection even after a breach is to encrypt customers’ Personally Identifiable Information (PII) data so that cybercriminals or internal non-authorized users only obtain unintelligible data. Bonafeyed protects PII data with the following data-defined security approach:

- Many Fintech systems proxy access to other systems – those credentials must be kept safe and accomplished with ***Cy4Secure™*** ability to SHA-512 hash users IDs.
- It may be necessary to allow other 3rd party systems/countries to access information - ***Cy4Secure’s*** features diversified encryption keys, multi-factor authentication to share data across other domains.
- KYC information is kept behind ***Cy4Secure’s*** air-gap technology, Bona-Isolator™.
- Individually encrypting data elements keeps information safe between a client and backend applications – the data is always encrypted at a high fidelity within SaaS or application’s database.

By taking these steps, Bonafeyed easily integrates into existing systems – simply take what are existing store procedures or reporting agents on the database server and isolate them as a separate client with restricted permissions. In such a case, if there is a leak or breach, the exposure to the vast amounts of PII data is contained or limited.

With Bonafeyed, when encrypted data is lost, stolen, abandoned, or forgotten, it remains protected, becomes demonetized and permanently inaccessible once keys are deleted or retired ensuring cyber criminals or internal non-authorized users only obtain unintelligible data, which exceeds the requirements of Gramm-Leach-Bliley Act and money transmitter laws!

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.