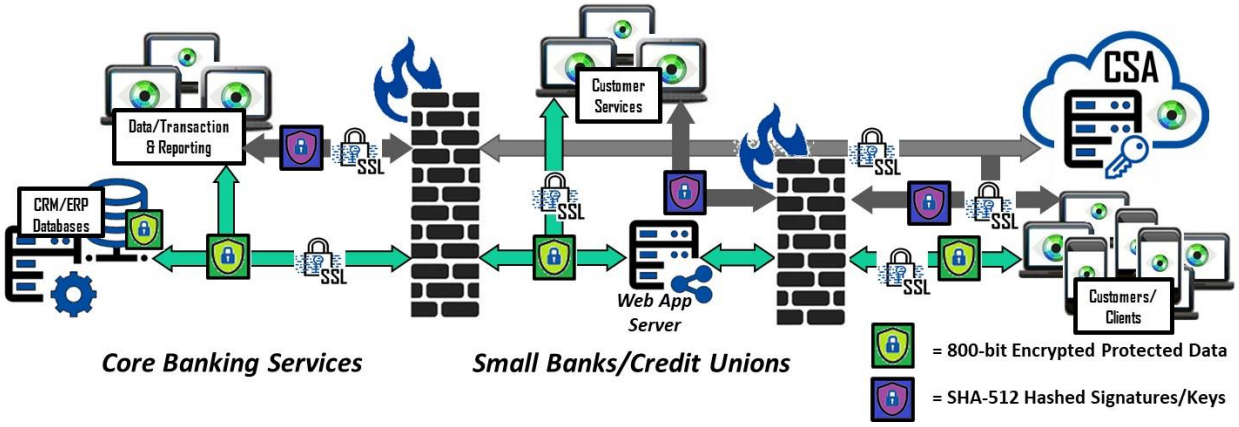
Use Case: Small Banks, Community Banks, and Credit Unions

The financial and banking services sector faces almost triple the number of cyberattacks than any other industry today. Core banking solutions help banks reduce operational and support expenses, provide real-time transaction processing, and manage bank accounts by aggregating CRM, ERP and management functions into a centralized database. Infiltrating these back-end processes present cybercriminals multiple opportunities to profit through ransomware and brokering of stolen data.

On or about October 2020, American Bank Systems, a service provider to US banks and financial institutions, was attacked, confronted with ransomware, and subsequently, 53 GB of data leaked. The cyberattack impacted ABS' clients including small banks, community banks and mortgage companies. The challenge is financial institutions must protect all "nonpublic personal information" relating to current and former customers under the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act. Verizon's 2020 Data Breach Investigations Report found, "The majority of attacks in this sector are perpetrated by external actors who are financially motivated to access easily monetized data stored by the victim organizations" and the top vulnerability is web applications using stolen credentials followed by a misconfiguration of IT. The fact is once the perpetrators acquire access to the databases, they obtain banking records with PII, loan, customers' Tax ID or SSN information.

Applying Bonafeyed's Data Defined Security to banking services, core computer backend databases can safeguard data with field and columnar level data encryption while allowing banks and customers to securely access the data using their existing systems. This ensures in the event of a breach monetary exploitation of the bank's and client's data is not possible. In other words, querying the databases would only yield encrypted data that has no value.



Bonafeyed also protects banking data on less complicated security systems over mobile devices by simply taking existing store procedures or reporting agents on the database server and isolate them as a separate client with diversified decryption. In such a case, if there is a leak or breach, the exposure to the vast amounts of PII records is 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 cybercriminals or internal non-authorized users only obtain unintelligible data.

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