

Applied Research project

Merrimack College

Data Governance, Laws and Ethics

Amol Gote

9th May 2020

## Data catalog and data capture

ABC is consumer personal loan financing company specializing in loans for dentistry treatments. It connects dentist networks, patients and banks. ABC collects tons of data during the loan application processing and servicing (loan repayment). There are 3 major types of data that ABC collects, customer’s PII Information and Credit history, customer’s identity. There are other 2 categories which are financial transactions for loan repayments and internal logs for API’s and mobile applications which it generates.

## Data Access

ABC is cloud company it leverages best practices from cloud providers AWS in this case to protects their data. Mobile application interacts with back end API’s over HTTPs, all the key PII database columns are encrypted, all identity documents and credit reports are encrypted at rest and stored in AWS S3 buckets. Appropriate security controls are in place for S3 buckets through bucket policies, IAM user and IAM roles. All the API’s implement OAuth token-based authentication, for B2B API’s 2 levels of security mechanisms are in place first IP based filtering and secondly token based authentication. Production database access is very restrictive, only DBA and CSO have access to the data store. Encryption keys are managed through AWS KMS service and are rotated appropriately. Applications logs are managed within AWS VPC and are moved internally to Elastic search/Kibana based solution for issue troubleshooting. Mobile app logs are managed through a third-party service (New Relic). ABC needs to share financial transaction data which is gathered from loan servicer to loan underwriting bank, for that ABC leverages bank provided SFTP site to push the data, this push is through a Cron job.

## Best Practices, Compliance laws and Competitors

ABC finances personal loans, so it must abide by the laws of FTC specifically GLBA and must be complaint with FCRA rules for credit decisioning. GLBA safeguard rules includes PII information must be secured against unauthorized access, all data sharing of consumer data with third parties and banks must be notified to customers, all the data access specifically PII information needs to be tracked and audited. To enable these safeguards, organization need to assign dedicated CISO/CSO, maintain data inventory and classification, all customer data must be encrypted at rest or transmitted over external network. Roles based security must be enabled which guarantees access to authorized individuals. Dispose the data that is not needed for the business operations. Monitor and regularly test safeguards through vulnerability or penetration testing. GLBA also enforces to have risk assessment framework, which identifies risks associated with data breaches and plans to mitigate those risks. FTC also proposes to have an incident response plan. For FCRA compliance, it gives lender access to credit bureau reports but restricts access to others, also other that FCRA rules, individual credit bureaus have their own rules on how the data from the credit reports need to be utilized. ABC is pretty new in this business domain and is competing with lending company CareCredit which has been in business for 30 years, it never had any data breach, there is no publicly available information which states any wrongdoing by CareCredit as far as any laws are concerned.

## Points of excellence and areas of improvement

ABC has lot of protections in place, it encrypts key PII database fields, uses encryption for transport as well as at rest. It shares financial transaction data with its partner banks, with them ABC has contractual agreement signed on the usage of the customer data. It is entirely AWS cloud based so it uses its best practices related to role-based access which encompasses of IAM roles and IAM users. ABC primarily uses S3 for inbound and outbound file transfers, so in either case S3 buckets are protected with IAM users, roles and bucket specific policies. For all IAM policies it follows the principle of granting only the permissions required to perform that task. They have dedicated personnel performing the role of chief security officer (CSO), who has put together a data classification in place, which classifies data as Restricted, Confidential, Private and Public. The reason for this classification was ABC wanted to identify which database fields need to be encrypted. All the encryption is managed by AWS KMS service which ensures the key rotation. Database access is restrictive and MFA access enabled for root permissions. Despite all these best practices in place there are numbers of areas of improvements. ABC has data classification in place, but it lacks concrete risk framework due to which it lacks mitigation plan against any unauthorized data access. Application logs potentially contains sensitive PII information, API team is logging the entire payload request and response, so anyone who has access to event log / Kibana console can get hold of some of the PII information. SRE team has access to production Kibana logs which is potentially a risk. Data analytics and data science team get access to read only data store of the production database, they get snapshot on certain frequency, in this case SSN is encrypted, but there is PII information first name, last, mobile number, etc. available.

## Maintaining excellence and rectification in areas of improvements.

ABC should continue with cloud based best practices that they incorporated in their processes an infrastructure, but there is scope for improvement in certain areas. Apart from having data classification they should do impact analysis of the data loss against for each of the classification. They have classified database attributes which is their main data source as Restricted, Confidential, Private and Public, there is no impact analysis (High/Medium/Low) against confidentiality, integrity and availability. NIST framework-based data classification needs to be defined. Below are some of the categorization and classification along with its impact.

|  |  |  |
| --- | --- | --- |
| Data classification levels | Description | Examples |
| Public | Publicly Available data | Number of loans generated, company performance. Profit and loss statements of organization |
| Private | Information available within organization | Internal communications, chats emails, application logs |
| Confidential | Customer PII Information | SSN, Name, Date of Birth, Mobile number, Credit reports. |
| Restricted | Highly confidential information that can cause permanent damage to a company and its customers. | Intellectual property (IP), trade secrets |

Table : Data classification levels

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Types (Domain) | | | | Data Classification |
| Customer Personal PII Information | This information is collected through mobile application and is required for loan approval. | | | Confidential |
| Financial Transactions | Monthly repayments made by customer. | | | Private |
| Application Logs | API Logs and mobile application logs | | | Private |
| Identify Information Types | Confidentiality Impact | Integrity Impact | Availability Impact |  |
| Customer Personal PII Information | High | High | Low |  |
| This could have significant impact on customer's trust | This could impact operations and customer support | This information is only required during application processing, later most of data in encrypted. |  |
| Financial Transactions | High | High | High |  |
| Expose customer's financial information | This could impact company's earnings | This impacts reporting, daily financial settlements |  |
| Application Logs | Low | Low | Medium |  |
| As long PII as masked, application do not pose much risks | Logs have very less shelf life, also they are used by application troubleshooting | In case of showstopper application logs become critical. |  |
| Final Domain Categorization | High | High | Medium |  |
| Overall Impact: High | | |  |

Table : Data classification matrix

ABC needs to correct the logging framework and ensure that all the PII fields that are logged are masked especially SSN, bank account numbers. Process of providing read only snapshot of the production data store need to change and need to incorporate data anonymization as part of the process.

# Bibliography

Taggart, C. (2019 Nov 21). GLBA Safeguards Rule updated: FTC defines “financial institutions”. Retrieved

from plantemoran:

[https://www.plantemoran.com/explore-our-thinking/insight/2019/12/glba-](https://www.plantemoran.com/explore-our-thinking/insight/2019/12/glba-safeguards-rule-updated-ftc-defines-financial-institutions)

[safeguards-rule-updated-ftc-defines-financial-institutions](https://www.plantemoran.com/explore-our-thinking/insight/2019/12/glba-safeguards-rule-updated-ftc-defines-financial-institutions)

Groot, J. (2019, July 15). What is GLBA Compliance? Understanding the Data Protection Requirements of

the Gramm-Leach-Bliley Act in 2019. Retrieved from the digital guardian:

[https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-](https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act)

[requirements-gramm-leach-bliley-act](https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act)

Green, A. (2020, March 3). We Need to Talk About Gramm-Leach-Bliley (GLB): The Safeguards Rule Will

Be Changing! Retrieved from[: https://www.varonis.com/blog/we-need-to-talk-about-gramm-](:%20https:/www.varonis.com/blog/we-need-to-talk-about-gramm-)

[leach-bliley-glb-the-safeguards-rule-will-be-changing/](:%20https:/www.varonis.com/blog/we-need-to-talk-about-gramm-)

Experian. *Understanding the Fair Credit Reporting Act.* Retrieved from Experian:

[https://www.experian.com/blogs/ask-experian/credit-education/report-basics/fair-credit-](https://www.experian.com/blogs/ask-experian/credit-education/report-basics/fair-credit-reporting-act-fcra/)

[reporting-act-fcra/](https://www.experian.com/blogs/ask-experian/credit-education/report-basics/fair-credit-reporting-act-fcra/)