|  |
| --- |
| **Possible Threat Model (TM) Template:** **Change Payment Account Solution Design Document** |

Step 1: Data Flow Diagram

Using STRIDE and/or Attack Tree approach; these diagrams shown by clicking on the links are very pertinent for the early establishment of the movement of data to and from different trust levels when modeling threats. The diagrams represented by figures have no major changes at the time of writing. The said figures, in practice have all the current sequences for the **Change Payment Account (CPA)** project. At any time, you can click on the link for details.

**[Fig 1.0 CPA DFD](https://drive.google.com/file/d/1xfZlILprFc9CMrzRLrAzr9hp8clpSSDb/view?usp=sharing) -1**

In the second diagram we have a simulation of the process using Microsoft Threat Modeling Tool (MS TMT). The reader is encouraged to read all these, for better understanding of the process. **[Fig 2.0 MS TM Tool CPA DFD](https://drive.google.com/file/d/14FYs4fT7NOt6RlBu4lKUB6fBlTJq58my/view?usp=sharing) -2**

We have taken a defensive approach to make sure that our application is developed with proper security from the inception. This will help us to define and model a secure architecture that follows:

* All the components that make up the system
* Identify assets that need protecting
* Document and rate threats
* **Trust levels – Trust boundaries**

***Entities with different levels of privileges (permissions):*** *Here there is a need to make sure that risk management policies, compliances and regulations are satisfied.*

**Trust boundaries are especially where interactions involve entities with different levels of trust and/or privilege. We established to mitigate the changing interactions between entities, users, and application processes.** Specific privileges (permission) are required for specific access levels. Take for instance a remote server. The permission a local client must bear to access the remote server is not going to be similar for a local server running the same process. We also consider the role of the account that is running the server in both scenarios. Application process could run with a service account as system, local service, network service, standard user with or without elevation. However, for remote services, a standard user without elevation rights is favored in most cases.

***Entities with different levels of privileges (permissions):*** *Here there is a need to make sure that risk management policies, compliances and regulations are satisfied.*

1. **Trust levels – Trust boundaries**

**Trust boundaries are especially where interactions involve entities with different levels of trust and/or privilege. We established to mitigate the changing interactions between entities, users, and application processes.** Specific privileges (permission) are required for specific access levels. Take for instance a remote server. The permission a local client must bear to access the remote server is not going to be similar for a local server running the same process. We also consider the role of the account that is running the server in both scenarios. Application process could run with a service account as system, local service, network service, standard user with or without elevation. However, for remoter service standard user without elevation rights is favored in most cases.

Step 2. Attack Enumeration

The risks are identified from the four (4) DFD Element:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **DFD Elements** | **SPOOFING** | **TAMPERING** | **REPUDIATION** | **INFORMATION DISCLOSURE** | **DOS** | **ESCALATION OF PRIVILEGE** |
| **Entity**  -ECS Faregate; Application Containers (Docker)  -Doppio (back-frontend)  -Okta IDp (tenancy auth) -AWS Cognito (User authentication)  -Kafka (data stream pipeline)  -Snowflakes (data analytics) |  |  |  |  |  |  |
| **Data flow**  User<->  Affiliate website  <->API AFW||Non-API <-> (Loan, Risk service) <-> Doppio Backend <-> Create Account<->DB |  |  |  |  |  |  |
| **Data store**  -NoSQL DynamoDB |  |  |  |  |  |  |
| **Processes**  -AWF microservice s  \*\*Onboarding\*\*  -Affiliate workflow service  -Loan application service  -Risk service  -Doppio |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Identified Risk** | **Risk Description** |
| **Elevation Of Privilege:** Elevation Using Impersonation\* | web Portal (Doppio/API:Payment service) may be able to impersonate the context of Web Member / User in order to gain additional privilege. |
| **Spoofing:**  Spoofing the Mobile Member/User External Entity\* | Mobile Member/User may be spoofed by an attacker and this may lead to unauthorized access to web Portal (Doppio/API:Payment service). Consider using a standard authentication mechanism to identify the external entity. |
| **Elevation Of Privilege:** Elevation Using Impersonation | web Portal (Doppio/API:Payment service) may be able to impersonate the context of Mobile Member/User in order to gain additional privilege. |
| **Repudiation:**  Potential Data Repudiation by web Portal (Doppio/API:Payment service) | web Portal (Doppio/API:Payment service) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Denial Of Service:**  Potential Process Crash or Stop for web Portal (Doppio/API:Payment service) | web Portal (Doppio/API:Payment service) crashes, halts, stops or runs slowly; in all cases violating an availability metric. |
| **Denial Of Service:**  Data Flow HTTPS | API Request Is Potentially Interrupted | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Elevation Of Privilege:**  Web Portal (Doppio/API:Payment service) May be Subject to Elevation of Privilege Using Remote Code Execution | Mobile Member/User may be able to remotely execute code for web Portal (Doppio/API:Payment service). |
| **Elevation Of Privilege:** Elevation by Changing the Execution Flow in web Portal (Doppio/API:Payment service) | An attacker may pass data into web Portal (Doppio/API:Payment service) in order to change the flow of program execution within web Portal (Doppio/API:Payment service) to the attacker's choosing. |
| **Repudiation:**  Potential Data Repudiation by web Portal (Doppio/API:Payment service) | web Portal (Doppio/API:Payment service) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Denial Of Service:**  Potential Process Crash or Stop for web Portal (Doppio/API:Payment service) | web Portal (Doppio/API:Payment service) crashes, halts, stops or runs slowly; in all cases violating an availability metric. |
| **Denial Of Service:**  Data Flow HTTPS | API Request Is Potentially Interrupted | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Elevation Of Privilege:**  Web Portal (Doppio/API:Payment service) May be Subject to Elevation of Privilege Using Remote Code Execution | Web Member / User may be able to remotely execute code for web Portal (Doppio/API:Payment service). |
| **Elevation Of Privilege:**  Elevation by Changing the Execution Flow in web Portal (Doppio/API:Payment service) | An attacker may pass data into web Portal (Doppio/API:Payment service) in order to change the flow of program execution within web Portal (Doppio/API:Payment service) to the attacker's choosing. |
| **Spoofing:**  Spoofing of the Mobile Member/User External Destination Entity | Mobile Member/User may be spoofed by an attacker, and this may lead to data being sent to the attacker's target instead of Mobile Member/User. Consider using a standard authentication mechanism to identify the external entity. |
| **Repudiation:**  External Entity Mobile Member/User External Destination Entity | Mobile Member/User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Denial Of Service:**  Data Flow HTTPS | API Response Is Potentially Interrupted | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Spoofing:**  Spoofing the Mobile Member/User External Entity | Web Member / User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Web Member / User. Consider using a standard authentication mechanism to identify the external entity. |
| **Repudiation:**  External Entity Web Member / User Potentially Denies Receiving Data | Web Member / User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Denial Of Service:**  Data Flow HTTPS | API Response Is Potentially Interrupted | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Elevation Of Privilege:** Elevation by Changing the Execution Flow in Kafka (data stream) | An attacker may pass data into Kafka (data stream) in order to change the flow of program execution within Kafka (data stream) to the attacker's choosing. |
| **Elevation Of Privilege:**  Kafka (data stream) May be Subject to Elevation of Privilege Using Remote Code Execution | web Portal (Doppio/API:Payment service) may be able to remotely execute code for Kafka (data stream). |
| **Elevation Of Privilege:** Elevation Using Impersonation | Kafka (data stream) may be able to impersonate the context of web Portal (Doppio/API:Payment service) in order to gain additional privilege. |
| **Denial Of Service:**  Data Flow HTTPS | API Request Is Potentially Interrupted\* | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Denial Of Service:**  Potential Process Crash or Stop for Kafka (data stream) | Kafka (data stream) crashes, halts, stops or runs slowly; in all cases violating an availability metric. |
| **Information Disclosure:**  Weak Authentication Scheme \* | Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme. |
| **Repudiation:**  Potential Data Repudiation by Kafka (data stream) \* | Kafka (data stream) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Tampering:** Collision Attacks \* | Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases. |

**Chart 1.0** Data from TMT file

Step 3. Mitigation

* It allows us to decide how to address each identified risk
* Update design of code of system, introduce security control, or accept risk.

1. **Spoofing; signature / authentication**
2. **Tampering; file permissions / access controls / hashes or signatures**

**R. Repudiation; Strong authentication, audit, logging**

**I. Information disclosure; access controls, encryption**

**D. Denial of service; availability, quotas, and failover servers**

**E. Elevation of privileges; access controls/authorization**

**[*See the table for Identified risk and their descriptions. There are recommendations there*]**

Step 4. Validation

* Accurately reflects the system/application modeled? **Y  / N**

If N start all over by reviewing the DFD process.

* Are mitigations in line with policies and risk management? **Y  / N**

If N start all over by reviewing the mitigation steps.

|  |
| --- |
| **Legend:**  **S** – Spoofing, **T**- Tampering, **R**- Repudiation, **I** - Information disclosure, **D** – Dos or Ddos, **E-** Escalation of privilege.  This is a shift-left or defensive approach to managing threats: The aim is to build security into applications; proactively making attack vectors ineffectual. This has the potential to reduce many risks and many efforts giving to risk management since residual risk will become a minimalism; if not completely averted. |

1. **Risk Assessment Methodology**

Each risk is assessed individually and is assigned a risk score based on an evaluation of the likelihood and impact of the risk on assets. -In the case the asset is **Change Payment Account** Application.

* **Likelihood (Likelihood is scored from 1 to 5 as follows):**

Likelihood Description Summary

**a. Improbable (1)**

Has never happened before and there is no reason to think it is any more likely now

**b. Unlikely (2)**

There is a possibility that it could happen, but it probably won't

**c. Likely (3)**

On balance, the risk is more likely to happen than not

**d. Very Likely (4)**

It would be a surprise if the risk did not occur either based on past frequency or current circumstances

**e. Almost certain (5)**

Either already happens regularly or there is some reason to believe it is virtually imminent

**II. Impact (Impact is scored from 1 to 5 as follows):**

Consideration is given to the qualitative and quantitative measures:

-Impact Level

-Impact Areas

-Impact Rating

General Description

* -Effect on Customers
* -Financial Cost
* -Health and Safety
* -Damage to Reputation
* -Legal, Contractual and Organizational Compliance

1. **Negligible (rated 1)**

No effect; Very little or none; Very small additional risk; Negligible; No implications

1. **Slight (rated 2)**

Some local disturbance to normal business operations

Some Within acceptable limits

Small risk of not meeting compliance

1. **Moderate (rate 3)**

Can still deliver product/ service with some difficulty

Unwelcome but could be borne

Elevated risk requiring immediate attention

In definite danger of operating illegally

1. **High (rated 4)**

Business is crippled in key areas

Severe effect on income and/or profit

Significant danger to life

Operating illegally in some areas

1. **Very High (rate 5)**

Out of business; no service to customers

Crippling, the organization will go out of business

Real or strong potential loss of life

Severe fines and possible imprisonment of staff

**III. 3.0 Risk Score**

The overall risk score is calculated by multiplying the scores for Impact and Likelihood

**(I x L)** ----- fn. 1

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **LIKELIHOOD** |  |  |  |  |  |  |  |  |  |
| Almost certain | **5** | 5 | 10 | 15 | 20 | 25 |  |  | High |
| very likely | **4** | 4 | 8 | 12 | 16 | 20 |  |  |  |
| Likely | **3** | 3 | 6 | 9 | 12 | 15 |  |  | Medium |
| Unlikely | **2** | 2 | 4 | 6 | 8 | 10 |  |  |  |
| Improbable | **1** | 1 | 2 | 3 | 4 | 5 |  |  | Low |
|  |  | **1** | **2** | **3** | **4** | **5** |  |  |  |
|  | **IMPACT** | Negligible | Slight | Moderate | High | Very high |  |  |  |

Likelihood vs Impact heat map for scoring

The risk assessment below is based on the Risk Assessment Methodology (above) used by the

Information Security Team. The excel spreadsheets that follow clearly show the mappings and scores.

**IV. Risk Assessment**

Heat map non-activated



Heat map activated

**{Residual Risk** = Inherent Risk – Impact of risk controls}

We define **residual risk** as the risk after successful mitigation or risks after controls are put in place to thwart occurrence of such risks.

We define **Inherent risk** as the risk before any successful mitigation or risks before controls are put in place to thwart occurrence of such risks.

**Impact of risk controls** refers to how the controls makes negligible the probable harm any threat agent could bring by exploiting any vulnerability on the asset or critical tools of the business and business continuity.

**Artifact of the practical problem identified in the infrastructure:**

-None

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Description of Risk** | **Impact (I) Score (1-5)** | **Likelihood (L) Score**  **(1-5)** | **Risk Score Explanation** | **Risk Score**  **(I x L)** | **Risk Level**  **(High / Med / Low)** | **Mitigating Controls** | **Implemented control Y/N** | **Residual Risk** | **Residual Risk Level**  **(High / Med / Low)** | **Mitigation Actions** |
| **Elevation Of Privilege:** Elevation Using Impersonation\* | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | STIG to harden systems; IAM, Password manager (Lastpass), Enforce least privilege (just in time access) to reduce standing privileges; Advanced authentication (MFA), Scanner, WAF; Cloud trail to monitor sessions; scanning to continuously monitor vulnerabilities | Yes | If mitigated the risk will be unlikely to occur | Low | Avoid persistent privileges; Implement proper security configurations; Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Spoofing:**  Spoofing the Mobile Member/User External Entity\* | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Use standard/advance authentication mechanism (x.509 certificate, signature; nonce or HMAC) to ID source data store. Okta/Cognito;  Authentication tokens JWT (Encryption, Signature) with mutual certificates, VPN.  Scanners, WAF, Cloud trail. | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Elevation Of Privilege:** Elevation Using Impersonation | 5 | 1 | Risk probability is very likely: impact high | 5 | Medium | Use industry standard/advanced authentication method: Salted sha2 hash with (PBKDF2) for encrypted credentials; secret vault (lastpass). | Yes | If mitigated the risk will be very unlikely | medium | Enforce strong password requirements: Avoid hard coding password in application; MFA |
| **Repudiation:**  Potential Data Repudiation by web Portal (Doppio/API:Payment service) | 2 | 3 | Risk probability is likely: impact slight | 6 | Medium | Use Standard/advanced authentication: mutual certificate, digital: JWT (encryption, signature, nonce or HMAC) ; VPN | No | If mitigated the risk will be almost certain not to occur | High | Not mitigated but will be if we authenticate  source of log before accepting; don’t accept logs from weakly authenticated, or unknown source. |
| **Denial Of Service:**  Potential Process Crash or Stop for web Portal (Doppio/API:Payment service) | 3 | 2 | Risk probability is unlikely: impact moderate | 6 | Medium | Programming for scale by offloading resource intensive process,  Upstream filtering (amazon shield and Cloudflare)  ; Rate limiting for API calls; whitelisting [allow] and blacklisting [deny]; Load balancing; failover, multiple aws availability zones | Yes | If mitigated the risk will be unlikely | Medium | Effective resource consumption without exhaustive requests that locks the systems. |
| **Denial Of Service:**  Data Flow HTTPS | API Request Is Potentially Interrupted | 3 | 2 | Risk probability is unlikely: impact moderate | 6 | Medium | Programming for scale by offloading resource intensive process,  Upstream filtering (amazon shield and Cloudflare)  ; Rate limiting for API calls; whitelisting [allow] and blacklisting [deny]; Load balancing; failover, multiple aws availability zones | Yes | If mitigated the risk will be unlikely | Medium | Effective resource consumption without exhaustive requests that locks the systems. |
| **Elevation Of Privilege:**  Web Portal (Doppio/API:Payment service) May be Subject to Elevation of Privilege Using Remote Code Execution | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Advanced authentication (MFA), Scanner, WAF; Cloud trail | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Elevation Of Privilege:** Elevation by Changing the Execution Flow in web Portal (Doppio/API:Payment service) | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Advanced authentication (MFA), Scanner, WAF; Cloud trail | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Repudiation:**  Potential Data Repudiation by web Portal (Doppio/API:Payment service) | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Advanced authentication (MFA), Scanner, WAF; Cloud trail | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Denial Of Service:**  Potential Process Crash or Stop for web Portal (Doppio/API:Payment service) | 3 | 3 | Risk probability is likely: impact moderate | 9 | Medium | API; Authentication tokens (JWT with Signature); Matcha interface for all access to PostgreSQL; service account with least privilege. | No | If mitigated the risk will be very unlikely to occur | High | Not mitigated but will be if JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA. Although JWTs can be encrypted to also provide secrecy between parties, we will focus on signed tokens. |
| **Denial Of Service:**  Data Flow HTTPS | API Request Is Potentially Interrupted | 5 | 3 | Risk probability is very likely: impact high | 15 | High | Standard authentication to ID data source; VPN | Yes | If mitigated the risk will be almost certain not to occur | medium | Only allow trusted code to log |
| **Elevation Of Privilege:**  Web Portal (Doppio/API:Payment service) May be Subject to Elevation of Privilege Using Remote Code Execution | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Advanced authentication (MFA), Scanner, WAF; Cloud trail | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Elevation Of Privilege:**  Elevation by Changing the Execution Flow in web Portal (Doppio/API:Payment service) | 3 | 2 | Risk probability is very likely: impact moderate | 6 | Medium | Advanced authentication (MFA), Scanner, WAF; Cloud trail | yes | If mitigated the risk will be unlikely to occur | medium | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Spoofing:**  Spoofing of the Mobile Member/User External Destination Entity | 3 | 2 | Risk probability is very likely: impact moderate | 6 | Medium | Whitelisting/blacklisting; Cloudflare; API rate limiting; Fuzzing tool; offloading resource intensive process | yes | If mitigated the risk will be unlikely to occur | medium | Strongly recommend fuzzing the parsers. |
| **Repudiation:**  External Entity Mobile Member/User Potentially Denies Receiving Data | 2 | 2 | Risk probability is unlike: impact slight | 4 | Low | Standard authentication method ( CA mutual certs, signature, TLS) | No | If mitigated the risk will be unlikely | High | Not mitigated but will be, if we implement authentication method for sensitive data. |
| **Denial Of Service:**  Data Flow HTTPS | API Response Is Potentially Interrupted | 2 | 2 | Risk probability is unlike: impact slight |  | Low | Limit API calls, use quota, failovers, Enroll in dos protection (cloudflare filter dos traffic)  Include a disaster recovery plan to, ensure efficient comms,  mitigations and recovery. Maintain current Antivirus,  Install firewall, evaluate security settings to avoid wrongful  implementations, User security best practices. | Yes | If mitigated the risk will be unlikely to occur | Low | Slow networks must be investigated; especially when access to sites fails. |
| **Spoofing:**  Spoofing the Mobile Member/User External Entity | 3 | 2 | Risk probability is likely: impact slight | 5 | Medium | Multi Factor Authentication including IP, connection should be authenticate validated with unique session IDs,  Mutual certificates, , authentication protocols (IPsec, TLS); domain authentication (LDAP). | Yes | If mitigated the risk will be unlikely | Medium | Implement effective KYC to thwart attackers with both user and application authentication. |
| **Repudiation:**  External Entity Web Member / User Potentially Denies Receiving Data **(1 )** | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Advanced authentication (MFA), Scanner, WAF; Cloud trail | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Denial Of Service:**  Data Flow HTTPS | API Response Is Potentially Interrupted | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Advanced authentication (MFA), Scanner, WAF; Cloud trail | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Elevation Of Privilege:** Elevation by Changing the Execution Flow in Kafka (data stream) | 3 | 3 | Risk probability is likely: impact moderate | 9 | Medium | API; Authentication tokens (JWT with Signature); Matcha interface for all access to PostgreSQL; service account with least privilege. | No | If mitigated the risk will be very unlikely to occur | High | Not mitigated but will be if JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA. Although JWTs can be encrypted to also provide secrecy between parties, we will focus on signed tokens. |
| **Elevation Of Privilege:**  Kafka (data stream) May be Subject to Elevation of Privilege Using Remote Code Execution | 2 | 3 | Risk probability is very likely: impact high | 6 | Medium | Standard authentication to ID data source; VPN | Yes | If mitigated the risk will be almost certain not to occur | Medium | Only allow trusted code to log |
| **Elevation Of Privilege:** Elevation Using Impersonation **(0)** | 5 | 1 | Risk probability is very likely: impact high | 5 | Medium | Use standard auth mechanism (x.509 certificate, signature; nonce or HMAC) to ID source data store. Okta/Cognito;  Authentication tokens JWT(Encryption, Signature) with mutual certificates, VPN. | Yes | If mitigated the risk will be unlikely | Medium | Certificate, Signature and GRC should be implored as a part of authentication mechanism. Deprecated Security configuration and related systems must be Updated or replaced. |
| **Denial Of Service:**  Data Flow HTTPS | API Request Is Potentially Interrupted\* | 3 | 2 | Risk probability is unlikely: impact moderate | 6 | Medium | Programming for scale by offloading resource intensive process,  Upstream filtering (amazon shield and Cloudflare)  ; Rate limiting for API calls; whitelisting [allow] and blacklisting [deny]; Load balancing; failover, multiple aws availability zones | Yes | If mitigated the risk will be unlikely | Medium | Effective resource consumption without exhaustive requests that locks the systems. |
| **Denial Of Service:**  Potential Process Crash or Stop for Kafka (data stream) | 3 | 2 | Risk probability is unlikely: impact moderate | 6 | Medium | Programming for scale by offloading resource intensive process,  Upstream filtering (amazon shield and Cloudflare)  ; Rate limiting for API calls; whitelisting [allow] and blacklisting [deny]; Load balancing; failover, multiple aws availability zones | Yes | If mitigated the risk will be unlikely | Medium | Effective resource consumption without exhaustive requests that locks the systems. |
| **Information Disclosure:**  Weak Authentication Scheme \* | 3 | 3 | Risk probability is likely: impact moderate | 9 | Medium | Scanner (burp’ engagement tools; Fuzzing), WAF; Salted hash-sha2 (PBKDF2) of encrypted credentials; secret vault (lastpass). Disable setting not needed; proper system and security configurations | Yes | If mitigated the risk will be unlikely | Medium | Enforce proper data protection of AuroraDB (mySQL ,PostgreSQL) forestalls most attackers assault to read information not intended for disclosure |
| **Repudiation:**  Potential Data Repudiation by Kafka (data stream) \* | 1 | 3 | Risk probability is likely: impact negligent | 3 | Low | Advanced authentication (MFA), Scanner, WAF; Cloud trail | Yes | If mitigated the risk will be unlikely to occur | Low | Regular scanning and monitor user behavior to stop authentication/authorization bypass. |
| **Tampering:** Collision Attacks \* | 2 | 3 | Risk probability is likely: impact slight | 6 | medium | SHA2 | Yes | If mitigated the risk will be unlikely | medium | Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases. |

5.0 Approval Recommendation

*We identified a service account (*adv-affiliate-workflow)*. However, it is not clear what role the service account has in the AuroraDB (*backoffice\_change\_payment\_account\_request*). It is not very clear which is the right database table.* We should identity the right database to ascertainimmediate mitigation making sure that the service account be given *‘db\_read’ or ‘db\_write’ privilege as best practice for* ***Change Payment Account (CPA)****.*

Secondly, we noticed another risk directed to unverified integrity of data as they traverse the Matcha Lead 2.0 process architecture. The system architecture and host instances are clear. The CPA Solution design documents traverse other application including (Matcha engine). Matcha Lead 2.0 application does not transform information: This means that any sensitive (PII) information is encrypted, and transferred with TLS 1.3 which seems not to be good enough. However, to mitigate threat of data tampering. It is pertinent that we ascertain existence of a control that will help HM confirm data integrity e.g HMAC shared secret, file integrity checker and copy-on-write file (snapshot of logs or DB).

Other threats or vulnerabilities found in the architecture will be mitigated by using relevant controls and enforcement actions. This will reduce the overall risk score thus justify the production of the application moving forward. -None of the finding will go unresolved.

The security risks associated with the use of ***Change Payment Account (CPA)*** have been assessed by threat modeling team, and appropriate mitigation actions or controls have been identified. Based on successful completion of the mitigation actions and implementation of mitigation controls, the threat modeling team judges the overall residual level of risk, to be acceptable for continued use of the ***Change Payment Account (CPA)***within the HM organization.

This Report will be reviewed by the delegates of HM, and risks reassessed for any future major releases of the ***Change Payment Account (CPA)***software and for any minor releases that impact security.

The use of ***Change Payment Account (CPA)***will be subject to Information Security Policies as applicable to all staff and all systems within HM.

Appendix

|  |  |
| --- | --- |
| **CVE-2021-38153** | Some components in Apache Kafka use `Arrays.equals` to validate a password or key, which is vulnerable to timing attacks that make brute force attacks for such credentials more likely to be successful. Users should upgrade to 2.8.1 or higher, or 3.0.0 or higher where this vulnerability has been fixed. The affected versions include Apache Kafka 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1, 2.2.2, 2.3.0, 2.3.1, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, and 2.8.0. |
| **CVE-2021-4190** | Large loop in the **Kafka** dissector in Wireshark 3.6.0 allows denial of service via packet injection or crafted capture file |
| **Fig 1.0 CPA DFD** | <https://drive.google.com/file/d/1xfZlILprFc9CMrzRLrAzr9hp8clpSSDb/view?usp=sharing> -1 |
| **MS TM Tool CPA DFD** | <https://drive.google.com/file/d/14FYs4fT7NOt6RlBu4lKUB6fBlTJq58my/view?usp=sharing> -**2** |