Revisions to the initial design principles

	Adaptive Learning & Continuous Improvement	
DP1	For developers to improve fraud detection accuracy and performance over time for users in the context of evolving transactional behaviours and changing card user habits, **(1) employ real-time learning mechanisms, analyse historical data,** and **(3) continuously integrate user feedback**. Implement constant updating and refinement processes to adapt dynamically to both emerging fraud patterns and normal variations in card user behaviours because this approach ensures the FDS remains accurately tuned to fraudulent activities and legitimate user trends, enhancing the system's reliability in a rapidly changing environment.	For developers to enhance fraud detection accuracy and adaptability for users in the context of evolving fraud patterns and changing cardholder behaviours, employ mechanisms to **(1) regularly update models**, continuously **(2) monitor key performance metrics**, learn from cardholder behaviour patterns, and **(3) incorporate user feedback on fraud alert accuracy**. Implement **(1) distinct processes for constant updating and refinement** using the latest transactional and external data to adapt dynamically. This approach ensures that the FDS remains responsive and accurate while allowing **(1) users to manage critical updates, reducing compliance risks** and maintaining system reliability.
	User-Centric Development & Alignment	
DP2	For developers to create a tailored FDS that aligns with the business model, goals, services, and customer base for users in the context of the FDS development process. **(4) Employ active involvement of end-users** and regular feedback loops. Tailor the system to specific business needs because this ensures the FDS is effective, aligned with strategic objectives, and optimises the cost–benefit ratio for each end-user by meeting their specific goals, such as reducing manual work, increasing efficiency or speed, and enhancing risk management, making optimal use of the available resources.	For developers to create a tailored FDS that aligns with the specific business goals, services, and customer base for users in the context of the FDS development process. Employ active involvement of **(4) end-users, including both managers and operational users**, through regular touchpoints and feedback loops. Tailor the system to meet the unique business needs of each user, ensuring the FDS is effective, aligned with strategic objectives, and optimised according to the cost–benefit ratio. This involves addressing specific goals such as reducing manual workloads, increasing efficiency or speed, enhancing risk and resource management, and **(5) most importantly, protecting cardholders against fraud. (6) Leverage fraud risk assessments and similar tools during development to ensure the model is accurately designed to address the organisation's specific risks and requirements.**
	Comprehensive Data Integration & Quality Assurance	
DP3	For developers to enhance fraud detection accuracy for users in the context of data quality and integrity, **(7) employ thorough data understanding, comprehensive preprocessing techniques, advanced feature engineering, secure data handling, and integration and analysis of various contextual data points** (e.g., time, place, login behaviours, device ID, IP address) because this ensures the model is built on a robust and reliable data foundation, accurately identifying fraudulent activities.	For developers to enhance fraud detection accuracy for users in the context of data quality and integrity, **(7) employ robust data understanding, thorough preprocessing techniques, advanced feature engineering, and continuous integration and analysis of contextual data points** (e.g., time, place, login behaviours, device ID, and IP address). **(8) Implement continuous data quality monitoring to detect and rectify missing or incorrect data fields**, with **(9) an emphasis on critical data points that directly influence fraud detection.** Prioritise the accuracy, quality, and integrity of these data fields to ensure the FDS remains built on a reliable foundation, enabling more informed decision-making and ensuring the accurate identification of fraudulent activities.

DP4	**(10) Hybrid Detection Approach** For developers to enhance detection efficiency and adaptability for users in the context of operational needs, **(10) employ a hybrid approach that integrates AI and rule-based methods. (11) This combination provides flexibility in adjusting detection rules and precision in fraud detection,** leveraging the strengths of both methodologies to improve accuracy and reduce manual review workload. This ensures the system remains effective and responsive to evolving fraud patterns and allows for timely adjustments to changing requirements.	**(10) AI-Driven with Targeted Rules** For developers to enhance detection efficiency and adaptability for users in the context of operational needs, **(10) prioritise an AI-driven approach while selectively integrating rule-based methods. (10, 11) This strategy leverages the superior adaptability and pattern recognition capabilities of AI to handle most fraud detection scenarios, reserving rule-based methods for specific, well-defined cases where AI may not have sufficient labelled data or where straightforward, clear-cut decisions are needed.** This approach ensures the system remains effective, minimises unnecessary alerts, and optimises resources by reducing manual review workloads.
DP5	**Scalability & Flexibility** For developers to maintain long-term usability and effectiveness for users in the context of increasing transaction volumes and evolving fraud techniques, **(12) employ scalable infrastructure, modular system design**, and regular performance assessments because this ensures the FDS can efficiently handle growth, adapt to new fraud methodologies, and remain effective.	For developers to maintain long-term usability and effectiveness for users in the context of increasing transaction volumes and evolving fraud techniques, **(12) employ scalable infrastructure and support modular updates and expansions**. This approach ensures the FDS can efficiently handle growth; adapt to new fraud methodologies; **(13) and maintain accurate fraud detection with minimal false positives, even under high transaction volumes**. Ensure that the system can **(14) easily scale up or down by adding resources as needed**, allowing for seamless adjustments while maintaining system effectiveness.
DP6	**(16) Dynamic & Interactive Explainability** For developers to enable dynamic exploration of data and **(16) interactive explainability features for users in the context of using the FDS**; provide user-friendly, interpretable insights; clear reasoning paths; and confidence levels in the system's decisions because this enhances trust, allows users to understand and validate the system's outputs, and supports effective decision-making in handling fraud cases.	**(17, 3) Transparent & User-Friendly Explainability** For developers to create transparent and **(16) user-friendly data exploration and explainability features in the context of both the development and usage of the FDS and to provide clear, interpretable insights; (15) comprehensive access to relevant data;** and well-documented reasoning paths. **(17) Ensure that the model training process is thoroughly documented and transparent.** Balance the level of detail with user needs to foster trust, support decision-making, and enable users to easily validate the system's outputs.

DP7	**(19) Integrated Preventive & Detective Measures** For developers to enable a strategic shift to combining preventive and detective fraud management for users in the context of comprehensive fraud protection, employ FDS algorithms that **(19) support** both **(18) preventive and detective measures** because this allows the system to use the same well-trained model, ensuring more secure protection for card users and the company.	**(19) Balanced Approach to Fraud Prevention & Detection** For developers to enable a strategic shift towards combining preventive and detective fraud management for users in the context of comprehensive fraud protection, employ FDS algorithms that effectively **(19) integrate** both **(18) preventive measures, such as real-time blocking of potentially fraudulent transactions, and detective measures that facilitate thorough investigation after transactions have occurred.** This **(19) balanced approach ensures** that the system leverages well-trained models to provide secure protection for cardholders and the company, addressing fraud **(18, 19) both proactively and reactively.**
DP8	**Bias Mitigation & Ethical Decision-Making** For developers to ensure fair treatment of all card users and **(22) minimise human bias for users in the context of decision-making processes**, employ algorithms that detect and measure bias, perform continuous monitoring, and conduct regular audits and updates because this ensures decisions are made without undue bias, fostering trust and reliability in the FDS.	For developers to ensure fair treatment of all card users and minimise bias in decision-making processes, **(20) establish clear ethical guidelines for data usage before model development**. Employ algorithms that undergo regular monitoring, and **(21) implement mandatory human oversight to review and validate AI decisions.** Additionally, **(22) ensure that users' judgments are thoroughly reviewed to prevent any bias from influencing the system**. This approach fosters trust, promotes fairness, and ensures decisions are made without undue bias, providing balanced and effective fraud protection.