Detailed results of evaluation round of supportive approach

DP	Original DP title & formulation	Feedback summary	Identified issues and needs	Resulting changes	Revised DP title & formulation
DP1	Adaptive learning And continuous Improvement For developers to improve fraud detection accuracy and performance over time for users in the context of evolving transactional behaviors and changing card user habits, employ real-time learning mechanisms, analyze historical data, and continuously integrate user feedback. Implement constant updating and refinement processes to adapt dynamically to both emerging fraud patterns and normal variations in card user behaviors 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.	Expert 1 feedback • Concern about the use of real-time learning mechanisms due to compliance reasons. • Suggests emphasizing the use of the latest data for model updates rather than real-time learning. • Emphasizes that the final decision to apply the updated model should rest with the customer, maintaining their control. Expert 2 feedback • Supports the idea of adaptive learning and continuous improvement. • Suggests adding continuous monitoring of certain metrics like fraud rates, true positives, or false positives. • Emphasizes the importance of metric-based monitoring to track the model's performance over time. Expert 3 feedback • Reinforces the importance of regular model retraining. • Highlights that retraining is crucial for detecting new fraud patterns. User 1 feedback • Agrees with the DP and acknowledges the need for continuous improvement and adaptation to new fraud patterns. • Suggests providing commentary to explain the principle, especially for non-subject matter experts, to avoid overcomplication. User 2 feedback • Fully agrees with the DP, especially the part about enhancing the system's reliability in a changing environment. • Mentions that the system should adapt to individual customer behavior changes, not just general fraud patterns. User 3: feedback • The principle is strong. • Suggests considering the inclusion of tracking losses incurred and maintaining a loss database.	Compliance concerns ! The mention of real-time learning mechanisms might lead to compliance issues. ! The DP should emphasize updating models with the latest data rather than automatic real-time updates. Metric-based monitoring ! Missing focus on continuous monitoring and metric-based tracking to evaluate model performance over time. Clarity for non-experts ! Ep is not quite clear to non-specialists. ! Add commentary or simplify the language. Customer control ! The final decision on the implementation of updates should lie with the customer.	⇒ Replacing "real-time learning mechanisms" with "updating models using the latest data" to avoid compliance concerns. ⇒ Incorporating the suggestion for continuous monitoring of metrics such as fraud rates and true/false positive rates. ⇒ Emphasizing that users retain control over the deployment of model updates. ⇒ Improving the wording of the DP.	Adaptive learning and continuous Improvement For developers to enhance fraud detection accuracy and adaptability for users in the context of evolving fraud patterns and changing cardholder behaviors, employ mechanisms to regularly update models, continuously monitor key performance metrics, learn from cardholder behavior patterns, and incorporate user feedback on fraud alert accuracy. Implement 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 users to manage critical updates, reducing compliance risks and maintaining system reliability.
DP2	User-centric Development and Alignment 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, 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, or enhancing risk management, making optimal use of the available resources.	Expert 1 feedback • Emphasizes the importance of using metrics that align with the business goals the FDS aims to achieve. • Suggests avoiding optimization of metrics that do not directly relate to specific business objectives. Expert 2 feedback • Likes the concept of regular touchpoints with users, especially with those who directly interact with the system, not just managers. • Recommends integrating features that users might currently access outside the system, such as transaction history lookups or google searches, to enhance the system's usability. Expert 3 feedback • Agrees with the necessity of tailoring the FDS to specific client needs, highlighting how different clients may require unique features or data points. • Cites examples where different customer profiles necessitate different fraud detection strategies. User 1 feedback • Stresses that the fundamental principle of the FDS should be card user protection against fraud and other risks. User 2 feedback • Agrees with the importance of reducing manual work but emphasizes that the system's efficiency should be maintained. • Suggests balancing automation with human intervention and maintaining resource efficiency. User 3: feedback • Agrees with the approach. • Highlights the challenge of implementation, which is heavily dependent on specific boundary conditions within an organization. • Suggests the use of tools like fraud risk assessments to ensure that the model accurately addresses the needs of the organization.	User involvement across roles ! Feedback highlights the importance of involving not just managers but also operational users in the development process. ! This ensures that the FDS addresses the practical needs of those who interact with it daily. Card user protection as a core objective: ! The primary goal of the FDS is to protect card users against fraud and other risks. Fraud risk assessment integration ! Inclusion of tools like fraud risk assessments during the development phase can ensure that the FDS accurately reflects and covers the necessary fraud risks specific to the organization.	⇒ Emphasizing the importance of regular touchpoints and feedback loops with all users, including managers and operational users. ⇒ Emphasizing that the protection of card users is one of the main objectives of the FDS. ⇒ Integration of tools such as fraud risk assessments during the development process.	User-centric Development and Alignment 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 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 optimizes the cost-benefit ratio. This involves addressing specific goals such as reducing manual workloads, increasing efficiency or speed, enhancing risk and resource management, and most importantly, protecting cardholders against fraud. Leverage fraud risk assessments and similar tools during development to ensure the model is accurately designed to address the organization's specific risks and requirements.

DP	Original DP title & formulation	Feedback summary	Identified issues and needs	Resulting changes	Revised DP title & formulation
DP3	Comprehensive Data integration And quality assurance For developers to enhance fraud detection accuracy for users in the context of data quality and integrity, employ thorough data understanding, comprehensive preprocessing techniques, advanced feature engineering, secure data handling, and integration and analysis of various contextual data points (such as time, place, log in behaviours, device id, ip address) because this ensures the model is built on a robust and reliable data foundation, accurately identifying fraudulent activities.	Expert 1 feedback • Agrees that data quality is fundamental and serves as the starting point for everything in fraud detection. • Suggests that the design principle mixes different concepts, such as data understanding, quality, and integrity with secure data handling, which may be a separate topic related to information security. • Recommends separating the concepts of data understanding and secure data handling into distinct principles, as they address different areas of concern. Expert 2 feedback • Strongly agrees on the importance of data quality, noting that many issues in fraud detection arise from data quality problems. • Recommends implementing continuous monitoring to detect issues such as missing data fields (e.g., device id), as missing or incorrect data can significantly impact the effectiveness of the FDS. Expert 3 feedback • Emphasises that certain data fields are crucial for effective fraud detection, though not all fields are equally essential. • Notes that while some fields are helpful, like ip addresses and time, others may not be critical but are still beneficial. User 1 feedback • Agrees with the importance of comprehensive data to safeguard customers and emphasises the need for a preventive and vigilant approach in fraud detection. User 2 feedback • Highlights the importance of having good, reliable data for decision-making, comparing it to gathering evidence in legal cases, better data leads to better outcomes. • Stresses that the system should be capable of handling noise in data and must prioritize high-quality data to ensure accurate and efficient fraud detection. User 3: feedback • Emphasises the importance of "connecting the dots", which refers to effectively integrating and analysing various data points. • Believes that this approach will be helpful in validating decisions and enhancing the model's performance.	Different concepts ! Distinguish between data understanding, quality, and integrity versus secure data handling. Continuous monitoring ! Missing aspect of continuous monitoring for data quality to detect and address missing or incorrect data fields that can compromise the effectiveness of the FDS. Prioritization of critical data fields ! More emphasis on certain critical data fields while recognising that others, while not essential, are still beneficial.	⇒ Refinement of the principle to focus exclusively on data understanding, quality, and integrity. ⇒ Increasing emphasis on continuous monitoring of data quality, especially for critical data fields, to ensure the effectiveness of the FDS. ⇒ Highlighting the prioritisation of critical data fields that are crucial for effective fraud detection.	Comprehensive Data integration And quality assurance For developers to enhance fraud detection accuracy for users in the context of data quality and integrity, employ robust data understanding, thorough preprocessing techniques, advanced feature engineering, and continuous integration and analysis of contextual data points (such as time, place, login behaviors, device id, and ip address). Implement continuous data quality monitoring to detect and rectify missing or incorrect data fields, with an emphasis on critical data points that directly influence fraud detection. Prioritize 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	Hybrid detection approach For developers to enhance detection efficiency and adaptability for users in the context of operational needs, employ a hybrid approach that integrates ai and rule-based methods. 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, responsive to evolving fraud patterns, and allows for timely adjustments to changing requirements.	Expert 1 feedback • Strong preference for ai, highlighting its superiority in most cases except for specific black-and-white scenarios. • Sees a limited role for rules, mainly for bootstrapping ai when labelled data is not available. • Suggests that the DP should place a heavier emphasis on ai rather than a balanced 50/50 split between ai and rules. Expert 2 feedback • Supports the use of a hybrid system but emphasizes that rules should be applied carefully to avoid spamming the system with too many cases. • Advocates for using rules primarily for edge cases and to adjust models when a rule becomes noisy, thereby transitioning those scenarios into the ai model. Expert 3 feedback • Highlights the necessity of rules in situations where there is no labelled data, particularly in anomaly detection. • Agrees that rules will always play a critical role, especially for binary or clear-cut situations. User 1 feedback • Points out that ai could significantly reduce unnecessary alerts, providing a more efficient approach to fraud detection compared to the current rule-based methods. • Supports the use of ai to enhance the relevance of alerts, particularly in preventing redundant alerts in straightforward situations. User 2 feedback • Emphasizes the importance of balancing ai and rule-based methods, noting that each approach is necessary in different scenarios. • Believes that a hybrid approach is essential to adapting to changing transactional activity and ensuring comprehensive fraud protection. User 3 feedback • Agrees with the principle but points out a tension between the need to save resources and the accuracy of fraud detection results.	Emphasis on ai superiority ! Several experts emphasize the superiority of ai in most fraud detection scenarios. ! Except for specific clear-cut cases where rules may be more appropriate. ! Need for a stronger emphasis on ai rather than an equal balance between ai and rule-based methods. Selective application of rules ! Rules should be applied selectively, primarily in situations where there is no labelled data. ! Or for specific edge cases that do not require frequent adjustments.	⇒ Strengthening the emphasis on the supremacy of ai in most fraud detection scenarios. The role of rule-based methods should be more focused on specific, clear-cut cases rather than an equal balance between ai and rules. ⇒ Recommending rules for selective application, particularly in situations where there is no labelled data or for edge cases that do not require frequent adjustments.	Ai-driven with Targeted rules For developers to enhance detection efficiency and adaptability for users in the context of operational needs, prioritize an ai-driven approach while selectively integrating rule-based methods. 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.

DP	Original DP title & formulation	Feedback summary	Identified issues and needs	Resulting changes	Revised DP title & formulation
DP5	Scalability And Flexibility For developers to maintain long-term usability and effectiveness for users in the context of increasing transaction volumes and evolving fraud techniques, 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 remains effective.	Expert 1 feedback • Fully agrees with the principle but suggests adding a focus on latency. • Emphasises that real-time processing speed is critical in fraud detection, particularly for blocking transactions promptly. Expert 2 feedback • Strongly supports the need for scalability. • Notes that scalability is essential for handling peak loads, like during black friday, to prevent system breakdowns under high transaction volumes. Expert 3 feedback • Agrees with the importance of scalability, highlighting the need to manage increased transaction volumes as clients grow. • Stresses the connection between scalability and the ease of updating models as fraud patterns evolve. • Mentions the current approach of adding more nodes as transaction volume increases, which demonstrates flexibility. User 1 feedback • Emphasises the goal of minimising false positives while maintaining relevant alerts, and notes that scalability is crucial to this process. • Mentions the need for efficient setups that can adapt to unpredictable customer behaviour. • Acknowledges that scalability is desired, but also points out the challenges in implementation, advocating for flexible methods to achieve it. User 2 feedback • Agrees that scalability is a common requirement and stresses that the system must be adaptable to varying customer base sizes. • Highlights the importance of the system's ability to handle different volumes while maintaining flexibility and effectiveness. User 3 feedback • Agrees with the principle.	Flexibility in scaling ! As transaction volumes increase, the system should scale seamlessly, potentially by adding more nodes or through other flexible methods to prevent the system from becoming overloaded or less effective. Connection between scalability and model updates ! Scalability should relate to the ease of updating models as fraud patterns evolve. Balancing scalability with effective fraud detection ! It lacks the balance between the scalability of the system and its ability to maintain relevant and accurate fraud alerts, minimising false positives without overlooking potential threats.	⇒ Adjustment of the DP to stress the need for flexibility in scaling the system, ensuring that as transaction volumes grow, the FDS can scale efficiently, whether through adding nodes or other scalable infrastructure solutions. ⇒ Making it clear in the DP that scalability should be linked to the ease of updating models. ⇒ Emphasising in the DP that while scalability is crucial, it must not come at the expense of the system's ability to accurately detect and prevent fraud.	Scalability And Flexibility For developers to maintain long-term usability and effectiveness for users in the context of increasing transaction volumes and evolving fraud techniques, employ scalable infrastructure and support modular updates and expansions. This approach ensures the FDS can efficiently handle growth, adapt to new fraud methodologies, and maintain accurate fraud detection with minimal false positives, even under high transaction volumes. Ensure that the system can easily scale up or down by adding resources as needed, allowing for seamless adjustments while maintaining system effectiveness.
DP6	Dynamic and Interactive Explainability For developers to enable dynamic exploration of data and 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.	Expert 1 feedback • Strong agreement with the principle, considering it a cornerstone for effective fraud detection systems. Expert 2 feedback • Views interactive explainability as supportive but not mandatory. • Emphasises the importance of users having access to all relevant data points within the FDS to avoid inefficiencies caused by switching between platforms. • Highlights the need for comprehensive data availability (e.g., currency conversion rates) within the system to support accurate analysis. Expert 3 feedback • Believes interactive explainability might be overkill for compliance purposes. While useful in research, it may not be necessary for everyday use by fraud investigators. • Suggests that general explanations are important for building trust, but overly detailed or interactive explanations may not be needed for compliance. User 1 feedback • Stresses that the principle is crucial for meeting regulatory and audit requirements. • Highlights the need for balance between relying on ai and ensuring human oversight and understanding of the ai's decision-making process. User 2 feedback • Emphasises the importance of cooperation between developers and users to ensure that the system's features are fully understood and utilized. • Advocates for balancing the importance of end-user needs with what is feasible in terms of cost and development effort, making the user experience as friendly as possible. User 3 feedback • Agrees with the principle. • Adds that it might be necessary to consider regulatory requirements.	Importance of access to relevant data ! Users need access to all relevant data points within the FDS to avoid inefficiencies caused by switching between platforms. ! Comprehensive data availability is crucial to support accurate analysis and decision-making. Balance between detailed explainability and practicality ! While interactive explainability is beneficial, it may be seen as excessive for everyday use by compliance officers and fraud investigators. ! There is a need for a balance between providing detailed explanations and ensuring that the system remains user-friendly and practical for regular use.	⇒ Emphasising that users should have access to all necessary data points within the FDS to facilitate accurate decision-making without the need to switch between different platforms. ⇒ Removing focus on interactivity, emphasising more general, understandable explanations that build trust without overwhelming users with unnecessary details. Focus on what is most useful for user and operational needs.	Transparent And user-friendly Explainability For developers to create transparent and user-friendly data exploration and explainability features in the context of both the development and usage of the FDS, provide clear, interpretable insights, comprehensive access to relevant data, and well-documented reasoning paths. 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	Integrated Preventive and 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 support both 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.	Expert 1 feedback • Initial confusion regarding the distinction between preventive and detective measures. • Agrees with the principle after clarification, emphasising the importance of real-time blocking for fraud prevention. Expert 2 feedback • Highlights the importance of keeping the system up to date with the latest fraud trends and data points to ensure effective preventive measures. • Discusses the challenge of preventive measures being more labour-intensive due to the need for real-time decision-making, compared to detective measures that can rely on historical data. Expert 3 feedback • Supports the integration of preventive and detective measures, emphasising that they should work together. • Provides examples where immediate blocking is necessary (e.g., transactions to sanctioned countries) versus scenarios where detection without immediate blocking is more appropriate. User 1 feedback • Strongly supports the principle, suggesting that proactive fraud prevention should be emphasised. User 2 feedback • Agrees with the principle, acknowledging the need for balance between prevention and detection, and noting that both are equally important in a comprehensive fraud detection system. User 3 feedback • Agrees with the principle.	Clarity on terminology ! There was initial confusion regarding the distinction between preventive and detective measures, indicating a need for clearer definitions within the DP. Integration and balance between preventive and detective measures ! It is important that preventive and detective measures are seamlessly integrated and that a balanced approach ensures comprehensive protection against fraud.	⇒ Defining clearer preventive and detective measures, ensuring a shared understanding among all stakeholders. ⇒ Focusing on the integration of preventive and detective measures, ensuring both are balanced and equally prioritized to provide comprehensive fraud protection.	Balanced approach To fraud prevention And 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 integrate both preventive measures, such as real-time blocking of potentially fraudulent transactions, and detective measures that facilitate thorough investigation after transactions have occurred. This balanced approach ensures that the system leverages well-trained models to provide secure protection for card users and the company, addressing fraud both proactively and reactively.

DP	Original DP title & formulation	Feedback summary	Identified issues and needs	Resulting changes	Revised DP title & formulation
DP8	Bias mitigation And ethical Decision-making For developers to ensure fair treatment of all card users and 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.	Expert 1 feedback • Stresses the importance of context when considering bias, noting that the impact of using potentially biased data fields (e.g., gender, nationality) varies depending on the model type. • Argues that for models like false positive reduction, the impact of bias is less severe because human review follows automated decisions, allowing for correction of any bias. • Emphasises that higher standards against bias must be applied in models used for account openings or preventive measures where discrimination could have significant real-life consequences. Expert 2 feedback • Emphasises the importance of setting ethical boundaries for data usage before model development begins to avoid ethical conflicts for data scientists. • Highlights the necessity of human oversight to ensure ai decisions are reviewed and validated by humans, as ai systems might inherently have biases similar to human ones. Expert 3 feedback • Acknowledges the challenge of minimising bias while recognizing that certain necessary features, like country, can introduce bias. • Suggests training specialized models for different transaction types or customer groups to reduce bias and improve model accuracy. User 1 feedback • Reinforces the importance of human judgment, emphasising that humans should have the final say in determining whether an alert is legitimate, acknowledging that machines can sometimes detect patterns better than humans. User 2 feedback • Expresses concern about the balance between fairness and practical risk management, suggesting that while equal treatment is important, the system must also recognize different risk levels among customer groups. • Raises the issue of potential bias from compliance officers, which could undermine the effectiveness of the ai system if fraudulent behaviour is wrongly classified as non-fraudulent. User 3 feedback • Agrees with the principle.	Ethical guidelines for data usage ! Set clear ethical boundaries for data usage before model development to prevent the introduction of bias in the system. Mandatory human oversight ! Ensure that ai decisions are subject to human review to maintain fairness and prevent biased outcomes. User bias ! Addressing the potential bias of users whose judgements have a direct impact on the ai system. Any bias at this stage can undermine the effectiveness of the fraud detection system.	⇒ Emphasising the importance of establishing ethical guidelines for data usage in fraud detection systems to avoid bias. ⇒ Incorporating mandatory human review of ai decisions and ensure that users' judgments are also subject to scrutiny to prevent any bias from influencing the system. ⇒ Incorporating continuous monitoring and regular audits to identify and eliminate any biases in both the ai system and the human decision-making processes.	Bias mitigation And ethical Decision-making For developers to ensure fair treatment of all card users and minimise bias in decision-making processes, establish clear ethical guidelines for data usage before model development. Employ algorithms that undergo regular monitoring and implement mandatory human oversight to review and validate ai decisions. Additionally, ensure that users' judgments are thoroughly re-viewed 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.