Code groups with corresponding codes

Coding group	Code	Key quotes	
Advanced techniques and approaches	Advanced Modelling Techniques	*Expert 1:*	*"... the models we are using for fraud detection include a lot of xgboost, but also more complex models… "*
		Expert 1:	*"as i mentioned earlier, using the same technology but applying it to transactions or analysing texts in transactions, like in the app fraud example, we think that's a more promising path than relying on assistants."*
		Expert 2:	*"...employing advanced analytics to better understand and adjust for concept drift and changing customer behaviours."*
		Expert 3:	*"… state of the art in ai-based fraud detection is, in my opinion, either a tree-based approach or something similar. For example, isolation forests have a big advantage because they don't require labels for training."*
		Expert 3:	*"… we use a deep learning technique, which is very good at handling new and unseen data…"*
		Expert 3:	*"… large language models outperformed xgboost, which we used to use and were quite happy with… "*
		Expert 3:	*"… we treat each transaction as a word. Just as a large language model tries to predict the next word, we try to predict the next transaction and determine how different it is from the expected one…"*
	Contextual Fraud detection	*Expert 1:*	*"the signals we would look for include the credit card being used in another country, a very high amount being used, a different device id logging in, and so on. As you say, the fact that it's now used in another country might not be suspicious in itself, but if it happens along with other factors, like higher-than-usual amounts, new services or goods being purchased, or a new device id that has never occurred before, it becomes more significant... "*
		Expert 1:	*"the system tells the user things like: this is an alert because the user has never logged in with that device before. It's the first time this device has occurred."*
		Expert 1:	*"it also indicates if the transaction was made abroad while 10 minutes before it was still made in switzerland, suggesting a potential account takeover."*
		Expert 2:	*"you need to take into account the transaction history, the relationships with other counterparties, and additional context like pos information, ip addresses, locations, and channel… "*
		Expert 2:	*"… we build the profile, collect transaction history, and gather all metadata related to the point of sale, among other things."*
		Expert 2:	*"… if a model learns that someone frequently travels between certain locations and suddenly there's a transaction that deviates significantly in amount, timing, or geographic location, it can flag this as an anomaly… "*
		Expert 2:	*"for example, it's typical for germans to travel to mallorca, and such regular travel patterns can be incorporated into the model's understanding… "*
		Expert 2:	*"… if the system logs admin activity, and in the future, you include mobile payments, it's important to track how often and in what patterns users log in."*
		Expert 2:	*"if i suddenly log in from another country at 3:00 am, that's suspicious and valuable context."*
		Expert 2:	*"these details include various fields such as payment type, payment means, e.g., debit transaction, amount, time, counterparty information, and possibly the counterparty bank identifier… "*
		Expert 2:	*"… customer's average transaction volume suddenly increases from €50 to €1500, especially to high-risk countries like afghanistan or iran, we would flag this as suspicious… "*
		Expert 2:	*"… checks the number of cross-border transactions made in the last month compared to the last week or the last three months compared to the last month… "*
		Expert 2:	*"if you weren't making many cross-border transactions and suddenly start making a lot, it will raise the anomaly score… "*
		Expert 2:	*"... There was no country information available. Instead, we had longitude and latitude data. We implemented a very cool feature where we calculated the manhattan distance between the longitude and latitude coordinates and divided it by the time elapsed since the previous transaction... "*
		User 1:	*"even if you are sitting in zurich and you pay somewhere globally, if the settlement of the card transaction is in the philippines, it will immediately create an alert. But technically, it can be like noise because you are visiting or buying something from a site in the philippines."*
		User 3:	*"beispielsweise wenn eine transaktion in zürich und zwei stunden später in são paulo erfolgt, sollte das system die karte automatisch blockieren, da dies mit einer physischen karte nicht möglich ist."*
		User 3:	*"… gibt es bestimmte muster, die darauf hinweisen, dass eine karte gestohlen wurde und jemand versucht, geld vom konto abzuheben. Das bedeutet häufige transaktionen unterhalb der freigrenze, eine hohe frequenz von zahlungen in einem engen geografischen raum oder auch online. Solche muster kann ein gutes system erkennen."*
		User 3:	*"meiner meinung nach ist es auch wichtig, dass das system muster erkennt, wie zum beispiel von welchen geräten und standorten sich kunden normalerweise einloggen. Die software sollte erkennen, wenn der kunde ein neues iphone kauft oder sich auf einer reise befindet und entsprechend reagieren... "*
	Detection vs Prevention	*Expert 2:*	*"detecting fraud in real-time, at the authorization level, adds complexity because you need to prevent financial damage before it occurs."*
		Expert 2:	*"if you want real-time action, then you focus on prevention. However, if detection after the transaction is the goal, it doesn't have to be done live, and you aren't constrained by performance concerns."*
		Expert 2:	*"detection is generally more accurate not just because you can employ more sophisticated models, but also because you have the full context of the situation… "*
		Expert 2:	*"… it's possible to combine approaches. You could have two models running concurrently, one in real-time that blocks transactions and another that operates on batches, which doesn't aim to block transactions immediately… "*
		Expert 2:	*"… combining preventive and detective aspects is crucial, and incorporating a rule-based approach adds flexibility and quick adaptability."*
		Expert 2:	*"i wouldn't say there's a huge difference in the models themselves, rather, it's about the information the model can access."*
		Expert 2:	*"… in prevention, you need a baseline of data to begin with, while detection starts with a model to gather all the necessary data… "*

		Expert 2:	*"once trained, you can use this model for prevention, provided the model for detection doesn't rely on information that won't be available in real-time… "*
		Expert 3:	*"we just have to configure the system to either block the transaction or alert about the transaction. It doesn't affect how we train the model."*
		User 1:	*"... If you compare it with large corporate banks that have lots of support teams and typically a 24/7 fraud monitoring team, they are able to handle any fraud activity at any time. They usually have much more restrictive and blocking card functionalities in place."*
		User 1:	*"... it has an ultimate impact on resources, prices, and everything. In our setup, it's clearly impossible to go this way, so we really follow the self-service model."*
		User 3:	*"das modell muss sehr präzise sein. Zusammengefasst kann man sagen, dass ein präventiv arbeitendes system schnell und präzise sein muss. Bei der detektiven arbeit sind diese faktoren nicht so wichtig oder nicht so essenziell."*
	Large language Models/transformer	*Expert 2:*	*"... the development of large language models specifically tailored for transaction monitoring is a noteworthy advancement."*
		Expert 3:	*"on the success side, i think large language models will prove quite useful in the future… "*
	Model quality	*Expert 1:*	*"other than that, of course, the model quality must be as high as possible. This means that the cost consideration must be as positive as possible."*
		Expert 3:	*"we look at cases with high, borderline, and low anomaly scores to ensure the model is functioning well… "*
	Model training And techniques	*Expert 1:*	*"we define the features in the feature extraction step, run feature extraction, and then run the actual model training."*
		Expert 2:	*"we then set metrics, like precision or recall, depending on the priority, and enter an iterative loop where we train the model, review our findings as if we were fraud investigators, and adjust based on feedback from the data provider… "*
	Supervised and Unsupervised Learning	*Expert 2:*	*"in my experience, supervised methodologies have worked the best, as we can foresee which patterns we want to train for and know how they should look… "*
		Expert 2:	*"on the other hand, unsupervised methods usually involve anomaly detection. However, data anomalies might just be pure data anomalies and not represent any sort of threat."*
Ai and rule-based approaches	**Ai and Rule-based Approaches**	*Expert 1:*	*"... pure ai-based monitoring system, with the exception of some rules that are very specific and targeted. For instance, if you want an alert for a transaction in a high-risk country, you can and should use a rule for that."*
		Expert 1:	*"on top of the auto-close model and the rules, we have another model that opens alerts for situations that go beyond what the rules can cover. This approach gets close to the quality of a pure ai-based system but still includes the rule component."*
		Expert 1:	*"... easier for them to accept having control over the rules and using an ai system… "*
		Expert 2:	*"exactly, it's possible to combine approaches. You could have two models running concurrently, one in real-time that blocks transactions and another that operates on batches, which doesn't aim to block transactions immediately… "*
		Expert 2:	*"... combining preventive and detective aspects is crucial, and incorporating a rule-based approach adds flexibility and quick adaptability."*
		Expert 2:	*"... combining a rule-based approach is super useful, particularly in cases that would be almost impossible to detect by a model… "*
		Expert 3:	*"for example, if the rule is about a transaction going to high-risk countries like russia or if the transaction was made to the same counterparty for the seventh time in a day, it would be blocked. So, for rules, it makes more sense because it's very quantifiable."*
		Expert 3:	*"... there should be a couple of good rules. Not a lot, because that would just increase false positives, but a couple of good rules should be in place in case the model leaves out something… "*
		User 3:	*"das system sollte so aufgebaut sein, dass es grundsätzlich regelbasiert arbeitet, aber durch die künstliche intelligenz falsch positive ergebnisse erkennt und diese automatisch filtert, sodass sie dem compliance-mitarbeiter gar nicht erst angezeigt werden."*
		User 3:	*"bei hawk:ai nutzen wir bereits künstliche intelligenz zur reduktion von falsch positiven ergebnissen, was ich als eleganten zwischenschritt sehe. Vermutlich wird dies dazu führen, dass man sich stärker auf modelle fokussiert, die auf regeln basieren, aber durch ki dynamischer und anpassungsfähiger sind. In unserem spezifischen fall mit kmus und zahlungsverkehrsfirmen wäre es sinnvoll, ein system zu haben, das auf dynamischen regeln basiert."*
	Complex Fraud detection	*Expert 1:*	*"... if you notice that someone is conducting business with their own company all the time and trying to obfuscate that, it could be a relevant fraud signal… "*
		Expert 2:	*"... those fraudulent ones will likely be so diverse that it becomes difficult for both humans and models to generalize what's happening in each case due to the vast difference in volume."*
		User 1:	*"... the weakness is probably the modern, very fast-evolving methods of card payments. This rapid evolution gives criminals the opportunity to be faster than the measures we implement to secure the money."*
	Real-time Fraud detection	*Expert 2:*	*"... it's about 1000 transactions per second, necessitating rapid processing… "*
		Expert 2:	*"... if a model is very complex and slow, i might avoid it for real-time prevention due to timing constraints."*
	Specific/targeted Rules	*Expert 2:*	*"... if there's a new payment type that the model doesn't support yet, we can quickly add a rule for this case, such as triggering a maximum of two transactions per month… "*
		User 1:	*"there are certain card-related rules defined at country levels. For example, if you pay locally or if you go abroad, all those parameters are predefined in terms of thresholds, right? "*
		User 1:	*"... the most commonly used fraudulent typology or rule breach is activity outside of the cardholder's country… "*
		User 2:	*"... current system is rule-based with no ai in use, making it quite rigid and not flexible… "*
		User 3:	*"... was alle machen, ist der regelbasierte ansatz statisch. Je nachdem, welchen risikoappetit eine firma hat, ergeben sich unterschiedliche herausforderungen."*
		User 3:	*"wenn ich sehr restriktiv bin und streng kontrollieren möchte, um meine risiken im griff zu haben, erhalte ich zwangsläufig sehr viele falsch positive ergebnisse. Diese müssen dann von compliance-mitarbeitern überprüft werden. Dabei weiss man, dass wenn ein mitarbeiter 1'000 transaktionen überprüft und nur eine davon tatsächlich positiv ist, er möglicherweise die restlichen 999 transaktionen weniger gründlich überprüft. Das ist ein grosser nachteil des regelbasierten ansatzes."*
Balancing multiple objectives	**Accuracy**	*Expert 1:*	*"but of course, the model should be as accurate as possible. So that's clear."*
		Expert 2:	*"this way, the system can distinguish between usual and unusual spending behaviours, adapting to recognized patterns like restaurant spending in foreign transactions, and improving its accuracy in fraud detection."*

	Alert handling Efficiency	*Expert 1:*	*"… we determine the number of alerts we can maximally generate for them."*
		User 1:	*"we are responsible every day for resolving such categories of alerts, and as of now, it's purely manual work. It can be perceived as annoying and repetitive because cardholders often have frequently driven methodologies like buying starbucks every morning, cigarettes, or taking an uber for travel. So technically, those transactions and even the timelines of when those transactions happen play a significant role in terms of the quality and the alert result distribution."*
		User 1:	*"technically, the aim is to increase the quality of specific alerts generated, to clearly focus on the appropriate alert. That's what's wanted and needed."*
	Automated Alert closing	*User 1:*	*"we want to initiate ai to help us with this large number of alerts, transactions, and detection methodologies."*
		User 1:	*"if ai could help us get rid of 50% of unnecessary alerts, it would mean that the remaining alerts would be of reasonable and better quality… "*
		User 1:	*"… key is to reduce false alerts and automate more so that you have more time to spend on real cases and other important tasks… "*
		User 2:	*"… without ai implementation, it would be impossible to maintain the alerts, and we would be overdue with all of them… "*
		User 2:	*"… in the future, we hope that the majority of the alerts will be visible in the auto-closed category."*
		User 3:	*"das system sollte so aufgebaut sein, dass es grundsätzlich regelbasiert arbeitet, aber durch die künstliche intelligenz falsch positive ergebnisse erkennt und diese automatisch filtert, sodass sie dem compliance-mitarbeiter gar nicht erst angezeigt werden."*
	Balancing multiple Objectives	*User 2:*	*"i would say it's important to find a balance somewhere in the middle… "*
		User 2:	*"in all of those spectrums, i think that when it comes to fraudulent activity, speed has probably slightly bigger value in this case. From a practical point of view, if you get your card skimmed, for example, and someone has your card details and starts doing fraudulent transactions, speed is probably more important than in other scenarios, such as standard wire transactions. Your goal is to stop the fraudulent activity as soon as possible from its initiation point. I'm not saying that faster is better or more important than the other aspects."*
		User 2:	*"talking about speed, i would not say that it's more important than, for example, detection accuracy. If we created alerts really fast and blocked many cards due to the possibility of transactions being fraudulent, but 99% of them are false positives, that wouldn't be effective. So, balance is important."*
		User 3:	*"es ist ganz klar eine balance. Die geschwindigkeit ist entscheidend, besonders wenn wir von prävention sprechen. Diese muss hoch sein, sonst funktioniert das system nicht. Gleichzeitig wollen wir unseren kunden ein zuverlässiges system bieten. Es darf nicht zu zufälligen kartensperrungen kommen, aber es muss auch in der lage sein, betrugsversuche effektiv zu erkennen und zu verhindern, um finanziellen schaden zu minimieren."*
	Comprehensive Goals	*User 1:*	*"regulators don't know exactly how it should be done. They just want us to closely monitor transactions in the right way, to spot it, identify it, block it, and act accordingly… "*
		User 3:	*"bei den debitkarten geht es bei der betrugsprävention vor allem darum, den kunden und die reputation der firma zu schützen."*
	Limitations of Metrics	*Expert 1:*	*"… a lot of the typical metrics that you would normally use in machine learning break down a little bit if the class imbalance… "*
		Expert 2:	*"i would say it's case-dependent. For the same use case, dataset, and objective, we can compare the same metrics."*
		Expert 3:	*"there is no single best metric… "*
	Necessity for Manual review	*User 1:*	*"… a breach of a specific rule, which is considered fraud-related, immediately highlights the given alert as a potential fraud alert to be reconciled or resolved… "*
	Precision and False positive Reduction	*Expert 2:*	*"… while achieving high precision is important, it's equally crucial to minimize false positives to avoid such issues… "*
		User 1:	*"we want to initiate ai to help us with this large number of alerts, transactions, and detection methodologies."*
		User 1:	*"it must be fast and really, really precise in the detection because that matters."*
	Speed and Efficiency	*User 3:*	*"es ist ganz klar eine balance. Die geschwindigkeit ist entscheidend, besonders wenn wir von prävention sprechen. Diese muss hoch sein, sonst funktioniert das system nicht. Gleichzeitig wollen wir unseren kunden ein zuverlässiges system bieten. Es darf nicht zu zufälligen kartensperrungen kommen, aber es muss auch in der lage sein, betrugsversuche effektiv zu erkennen und zu verhindern, um finanziellen schaden zu minimieren."*
Bias and ethics	**Bias and Discrimination Risk**	*Expert 1:*	*"i would also say what becomes more and more important, and i think it's particularly important in a fraud context, is the whole topic of fairness. Is your model discriminatory? For fraud, where you are blocking transactions, the model really should be fair because it affects people's lives."*
	Bias Mitigation	*Expert 1:*	*"we also perform bias testing to see if the model has any biases built in."*
		Expert 2:	*"therefore, having clear explainability in one place helps avoid these biases… "*
		Expert 3:	*"bias usually occurs when you have labelled data, but it can also happen with unsupervised learning… "*
		Expert 3:	*" … another type of bias can be seen in b2c versus b2b transactions. If most of the transactions are b2b, the model becomes biased towards high-frequency or high-volume transactions with large customers and transactions with the same counterparty… "*
		Expert 3:	*"to combat this bias, we train different models for b2c and b2b transactions… "*
	Ethical Considerations	*Expert 3:*	*"… If we use country as a feature, why not race? It's kind of the same thing. Felix said we should be able to use it because the model is not biased; it's just using statistics. However, i pointed out that if the model declines a transaction because the person is black, it wouldn't look good on the case manager... "*
	Human Decision Bias	*Expert 2:*	*"this can bias the investigator because they might see a 100 euro transaction and assume it's fine, simply because humans are naturally inclined to avoid extra work… "*
		Expert 2:	*"the model could automatically consider cross-border transactions, frequency, volume, and other factors, avoiding human bias."*
		User 3:	*"bei vielen falsch positiven ergebnissen besteht das risiko, dass die mitarbeiter irgendwann nicht mehr alles richtig überprüfen… "*
Customer involvement And business strategy	**Business Strategy**	*Expert 1:*	*"… understanding the business model of the customer and the types of fraud that could occur for them is crucial because it varies based on the business model… "*

Adaptation	**Adaptation**	*Expert 2:*	*"it really depends on what the client wants. Some clients may prioritize predictive and preventive measures, while others might focus more on detection… "*
		Expert 3:	*"… a customer might have specific requirements that influence how we adjust the model… "*
		User 3:	*"… was alle machen, ist der regelbasierte ansatz statisch. Je nachdem, welchen risikoappetit eine firma hat, ergeben sich unterschiedliche herausforderungen."*
	Cost-benefit	*Expert 1:*	*"what we do is usually contrast the "cost" the model incurs for the customer versus the benefit. By "cost," i mean the number of alerts it produces. Every alert is a cost for the customer, because if it's a false alert, they will have to work on it and close it, which takes time. On the other hand, we can estimate how many fraud cases we can catch with the model and also how many we can catch that rules can't catch. This allows us to estimate the benefit from a monetary perspective for the customer."*
		Expert 1:	*"… customer with a very small team of analysts who work on the alerts, they will naturally prioritize having a low number of false positives… "*
		Expert 3:	*"some clients don't have enough budget, so they might say that our fraud or anomaly detection system opens an alert and then the agent has to check and go through them to see if it's a good alert or not… "*
	Customer Involvement	*Expert 1:*	*"we aim to involve the customer as early as possible to ensure the model aligns with their expectations."*
		Expert 1:	*"usually, we give them all of this information, how many alerts we are generating for this threshold, how many of them are false positives, how many fraud instances we can detect, and all of that. They can then make the decision in the end."*
		Expert 2:	*"some clients may prioritize increasing accuracy, while others might focus on speed or efficiency"*
	Customer Resistance	*Expert 1:*	*"… most of our customers are not ready for a fully ai-based system… "*
		User 3:	*"zudem hoffe ich auf eine grössere akzeptanz und weniger risikoaversion, um die innovation in diesem bereich voranzutreiben."*
	Customer-centric Development	*Expert 1:*	*"… understand from the customer, first of all, what their pain points are at the moment, like where is the need for a fraud detection model, and what specific challenges they are facing… "*
		Expert 2:	*"… the most challenging aspect is understanding how much risk a customer is willing to take."*
		Expert 3:	*"… the customer tells us their specific goals and areas of focus."*
		Expert 3:	*"… if a client has specific needs, like dealing with crypto transactions which are few, we train a separate model just for those transactions… "*
	Resource Constrains	*User 1:*	*"… it needs much more time than compliance officers have. It takes more resources from you because it creates many more alerts than necessary… "*
		User 2:	*"… without ai implementation, it would be impossible to maintain the alerts, and we would be overdue with all of them… "*
Data quality And integrity	**Comprehensive Data**	*Expert 1:*	*"… integrating it with databases that provide information about company shareholder structures, relationships between people and companies, and similar details."*
		Expert 2:	*"traditional systems often exclude such details, focusing only on transactions. But if we enrich transaction data with login information or other relevant details, it significantly improves the accuracy and reliability of fraud detection."*
		Expert 2:	*"it's a combination of all these different data points that ensures the system is effective in the end…"*
	Data integrity	*Expert 2:*	*"you shouldn't have missing information that might lead you to incorrectly determine a transaction is not fraudulent when it actually might be… "*
		Expert 2:	*"data mining has greatly improved by providing richer context to transactions, enriching the datasets that were previously limited in scope."*
	Data quality	*Expert 1:*	*"… model can only be as good as the labels provided… "*
		Expert 2:	*"regarding the guidelines and best practices, the most important aspect is data quality… "*
	Data Understanding	*Expert 2:*	*"it's crucial to understand the transaction language of the dataset."*
		Expert 3:	*"… first step is to understand the data and extract the features from it… "*
	Exploratory Data analysis	*Expert 1:*	*"then, we conduct an exploratory data analysis, where we closely examine the data."*
	Feature Extraction	*Expert 1:*	*"the first step would be feature extraction. We have a feature store at hawk:ai with many different fraud signals registered."*
		Expert 3:	*"even if they do, the difficult part is not creating the ai system, the challenging part is obtaining the right features for the system… "*
	Labelling	*Expert 1:*	*"… importance of having a very good long-term process in place that allows you to capture the right labels… "*
		Expert 2:	*"if we have the chance to obtain fraud labels, then our approach can be completely different and more effective… "*
		Expert 3:	*"… most data are unlabelled because for rule-based systems, an agent can label data by validating whether the rule worked. However, for anomaly detection in money laundering or fraud, we generally lack labels… "*
	Limited data	*Expert 3:*	*"limited data is another challenge. For instance, my first project with amnis involved very little initial data, which was troubling… "*
Explainability and Transparency	**Explainability and user-friendly Explanations**	*Expert 1:*	*"another important area is explainability."*
		Expert 1:	*"the system tells the user things like, "this is an alert because the user has never logged in with that device before. It's the first time this device has occurred." it also indicates if the transaction was made abroad while 10 minutes before it was still made in switzerland, suggesting a potential account takeover. It will note if the amount is unusually high and similar factors. We present this in human-readable text, providing a prioritized list of reasons why it considers the alert to be fraudulent. Additionally, where applicable, we visualize the flow of funds."*
		Expert 2:	*"… having proper explanations is as important as finding fraudulent activities. There are infinite features we can use, but they need to be translatable to plain language."*
		Expert 2:	*"… It's crucial that the information is clearly specified when working on cases. This ties back to what i mentioned in some previous questions. You shouldn't have missing information that might lead you to incorrectly determine a transaction is not fraudulent when it actually might be."*
		User 1:	*"… the ideal or successful fraud detection system should learn from behaviours, be explainable, and be traceable."*

		User 1:	"you need to show them easily and explain how the machine is set up, how the result was gained, and why… "
		User 2:	"explainability and traceability for why something happens or was decided are really important for compliance."
	Interactive Explainability	Expert 1:	"we are also experimenting with even more advanced approaches, such as interactive explainability. In this method, users can change certain aspects of the transaction and see how the model outcome would be affected. This helps in understanding the model's decision-making process better... "
	Shap	Expert 3:	"… we use explainable ai plots, such as shap values, to understand how each feature impacts the anomaly score…"
	Transparency	Expert 1:	"i would also add transparency during the model training time because explainability is what you get during model execution time. But you also want transparency regarding how the model was trained, what principles were used, what features were used, and all of that. There must be a proper audit trail of how the model was generated and proper documentation surrounding that."
		User 1:	"it should be transparent about which data the decision is based on. It should be easy for you to understand and trace why it made a particular decision…
		User 3:	"für compliance officers wäre es wichtig, dass diese systeme transparent und nachvollziehbar sind, um deren entscheidungen zu unterstützen."
Learning And feedback Integration	**Changing Customer Behaviour**	Expert 1:	"… changing customer behaviour is actually something that should be alerted for… "
		Expert 2:	"understanding typical behaviour patterns, such as a swiss customer regularly purchasing in switzerland, is crucial… "
	Feedback Integration	Expert 1:	"if we have the chance to obtain fraud labels, then our approach can be completely different and more effective… "
		Expert 2:	"another very useful feature that i would 100% recommend is systematic feedback gathering… "
		Expert 2:	"whether the investigator accepts the case or needs more information, we gather all this feedback… "
		User 1:	"the system then accepts your decision and learns from it. This feedback loop is the second key component. It's critical to take the effort and time invested in the analysis by the human side and incorporate it into the system's learning process. That's the key factor."
	Learning And iterative Improvement	Expert 1:	"based on the validation outcome, we most likely go back to the feature extraction step and repeat the process until we achieve a satisfactory result."
		Expert 2:	"we then set metrics, like precision or recall, depending on the priority, and enter an iterative loop where we train the model, review our findings as if we were fraud investigators, and adjust based on feedback from the data provider… "
		Expert 2:	"… models can learn these cross-border behaviours. The models are trained to recognize that people living near borders might frequently cross into neighbouring countries, and this is a normal pattern… "
		User 2:	"the ai itself does not have what i consider one of the most important features, which is the learning ability… "
		User 3:	"hier sehe ich den hauptvorteil von artificial intelligence. Man kann den normalen bereich für einen kunden dynamisch anpassen. Wenn eine transaktion unter den gleichen bedingungen zwei- oder dreimal als gut bewertet wird, kann die software lernen, dass sie wahrscheinlich gut ist."
	Monitoring	Expert 1:	"we also monitor the data going into the model, computing the average feature values… "
		Expert 1:	"… monitoring in place in our application where we track key metrics of the models… "
User interaction And support	**User decision Support**	Expert 1:	"the model really has to give exact reasons for why it made a decision. Only then can we validate the model properly, ensure it really works, and understand how it works. Additionally, it makes the investigation for analysts much faster because they know what aspect to focus on first, rather than just getting an abstract score without any explanation... "
		User 2:	"i would say a must-have feature is that it assists you in decision-making. That's also one of the more important goals… "
	User-friendliness	Expert 2:	"… expandability is crucial. Imagine being an investigator who has to do a lot of clicks and open many windows to get the information needed."
		User 3:	"für uns ist ein system mit einem benutzerfreundlichen interface wichtig, bei dem die künstliche intelligenz im hintergrund arbeitet und nicht prominent dargestellt wird… "
	Visual data Representation	Expert 3:	"we already do something similar for fund flows, showing a tree structure with arrows for amounts coming in from multiple accounts and going out to one account. This could be improved further… "
	Speed and Efficiency	User 1:	"we need to be faster in concluding, resolving, blocking, preventing, and protecting the customer's funds… "
		User 1:	"the core setup needs to enable us to quickly address alerts. The speed is crucial here… "
		User 2:	"in all of those spectrums, i think that when it comes to fraudulent activity, speed has probably slightly bigger value in this case. From a practical point of view, if you get your card skimmed, for example, and someone has your card details and starts doing fraudulent transactions, speed is probably more important than in other scenarios, such as standard wire transactions... "