Fraud Detection and Prevention

Transaction Monitoring Techniques

A/B Testing refers to a method of comparing two versions of a system, process, or application to determine which one performs better, often used in Transaction Monitoring Techniques to evaluate the effectiveness of different fraud detection models, identifying the most accurate and efficient approach to prevent fraud.
Acquiring Bank is a financial institution that enables merchants to accept payments, processing transactions and managing the flow of funds, playing a crucial role in the transaction monitoring process.
Activity Monitoring involves tracking and analyzing user behavior, including login attempts, transactions, and other system interactions, to detect potential security threats and prevent fraudulent activities.
Adaptive Authentication is a security process that adjusts the level of authentication required based on the risk associated with a particular transaction or user, providing an additional layer of security to prevent fraud.
Advanced Persistent Threat (APT) refers to a type of cyber attack where an attacker gains unauthorized access to a system or network and remains undetected for an extended period, often using sophisticated techniques to evade detection.
Alert Management involves the process of generating, managing, and responding to alerts and notifications, ensuring that potential security threats are addressed promptly and effectively.
Anomaly Detection is a technique used to identify patterns or behaviors that are outside the norm, flagging potential security threats and preventing fraudulent activities.
Anti-Money Laundering (AML) refers to the set of regulations and procedures designed to prevent the laundering of illicit funds, requiring financial institutions to monitor and report suspicious transactions.
Application Programming Interface (API) is a set of defined rules that enable different applications and systems to communicate with each other, often used in transaction monitoring to integrate with other systems and share data.
Artificial Intelligence (AI) refers to the use of computer systems that can learn and make decisions like humans, often applied in transaction monitoring to detect and prevent fraud.
Asset Protection involves the use of various techniques and strategies to protect assets from unauthorized access, theft, or damage, including intellectual property, data, and financial assets.
Authentication is the process of verifying the identity of users, devices, or systems, often using credentials such as passwords, biometric data, or smart cards.
Authorization involves the process of granting or denying access to resources, data, or systems, based on the permissions and privileges assigned to users or roles.
Automated Clearing House (ACH) is a network used for electronic funds transfer, enabling the exchange of financial transactions between banks and other financial institutions.
Bank Secrecy Act (BSA) refers to a set of regulations that require financial institutions to report suspicious transactions and maintain records of customer activity, helping to prevent money laundering and other

financial crimes.
Behavioral Analysis involves the study of user behavior, including transaction patterns and system interactions, to identify potential security threats and prevent fraudulent activities.
Biometric Authentication uses unique physical or behavioral characteristics, such as fingerprint or face recognition, to verify the identity of users.
Blockchain is a distributed ledger technology that records transactions across a network of computers, providing a secure and transparent way to conduct transactions.
Business Intelligence (BI) refers to the process of gathering, analyzing, and interpreting data to inform business decisions, often used in transaction monitoring to identify trends and patterns.
Card Verification Value (CVV) is a security feature used to verify the identity of credit or debit card holders, reducing the risk of card-not-present transactions.
Certification Authority (CA) is an entity that issues digital certificates, verifying the identity of users, devices, or systems, and enabling secure communication over the internet.
Cloud Computing refers to the delivery of computing resources, such as storage and processing power, over the internet, often used in transaction monitoring to provide scalability and flexibility.
Compliance involves the process of adhering to regulatory requirements, industry standards, and internal policies, ensuring that transaction monitoring systems meet the necessary guidelines.
Computer Security Incident Response Team (CSIRT) is a team that responds to and manages computer security incidents, such as data breaches or system compromises.
Credit Scoring is a method used to evaluate the creditworthiness of individuals or businesses, assigning a score based on their credit history and other factors.
Cryptocurrency is a digital or virtual currency that uses cryptography for secure financial transactions, often used in transaction monitoring to detect and prevent illicit activities.
Customer Due Diligence (CDD) involves the process of verifying the identity and legitimacy of customers, helping to prevent money laundering and other financial crimes.
Customer Relationship Management (CRM) is a system used to manage customer interactions, tracking customer data, transactions, and communication.
Cyber Attack refers to a malicious attempt to compromise or disrupt the security of a system, network, or application, often using techniques such as phishing or malware.
Data Analytics involves the process of examining and interpreting data to extract insights and meaning, often used in transaction monitoring to identify trends and patterns.
Data Encryption is the process of converting plaintext data into ciphertext, making it unreadable to unauthorized parties, and protecting sensitive information.
Data Loss Prevention (DLP) is a set of strategies and technologies used to prevent the unauthorized transmission or disclosure of sensitive data.
Data Mining is the process of automatically discovering patterns and relationships in large datasets, identifying potential security threats and preventing fraudulent activities.
Data Visualization involves the use of graphical representations to communicate complex data insights and trends, often used in transaction monitoring to identify patterns and anomalies.

Device Fingerprinting is a technique used to identify and track devices, such as computers or mobile devices, based on their unique characteristics and attributes.
Digital Certificate is a digital document that verifies the identity of a user, device, or system, and enables secure communication over the internet.
Digital Forensics is the process of collecting, analyzing, and preserving digital evidence, often used in transaction monitoring to investigate and prosecute cybercrimes.
Digital Identity is a set of attributes and characteristics that define an individual or entity in the digital world, often used in transaction monitoring to verify identities and prevent fraud.
Digital Signature is a type of electronic signature that uses cryptography to authenticate the identity of a user or device, and ensure the integrity of digital documents.
Disaster Recovery involves the process of restoring systems and data in the event of a disaster or major disruption, ensuring business continuity and minimizing downtime.
Distributed Denial of Service (DDoS) is a type of cyber attack that overwhelms a system or network with traffic, making it unavailable to legitimate users.
E-commerce refers to the buying and selling of goods and services over the internet, often using online payment systems and transaction monitoring techniques.
Electronic Fund Transfer (EFT) is a type of transaction that transfers funds from one account to another, often using electronic payment systems and networks.
Encryption Key is a secret code used to encrypt and decrypt data, protecting sensitive information from unauthorized access.
Error Detection involves the process of identifying and correcting errors, such as data entry mistakes or system glitches, to prevent fraudulent activities.
False Positive is a type of error that occurs when a legitimate transaction is flagged as suspicious or fraudulent, often resulting in unnecessary reviews and delays.
Financial Institution (FI) is an organization that provides financial services, such as banking, investments, and insurance, often subject to regulatory requirements and transaction monitoring guidelines.
Fraud Detection involves the use of various techniques and strategies to identify and prevent fraudulent activities, such as transaction monitoring and anomaly detection.
Fraud Prevention is the process of preventing or mitigating fraudulent activities, often using a combination of techniques, such as authentication, authorization, and encryption.
Geolocation involves the use of geographic data to identify the location of users, devices, or transactions, often used in transaction monitoring to detect and prevent fraud.
Identity Theft is a type of crime that involves the theft or misuse of personal identifying information, such as names, addresses, or social security numbers.
Information Security (InfoSec) refers to the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction.
Insurance is a type of financial protection that covers individuals or businesses against losses or damages, often used in transaction monitoring to mitigate risks.
Intelligent System is a type of system that uses artificial intelligence and machine learning to make decisions

and take actions, often used in transaction monitoring to detect and prevent fraud.
Internet Protocol (IP) is a set of rules that govern the communication between devices over the internet, often used in transaction monitoring to track and identify users.
Intrusion Detection System (IDS) is a system that monitors network traffic for signs of unauthorized access or malicious activity, often used in transaction monitoring to detect and prevent cyber attacks.
Intrusion Prevention System (IPS) is a system that blocks or prevents malicious activity, such as hacker attacks or malware, often used in transaction monitoring to protect systems and data.
Know Your Customer (KYC) is a set of regulations and guidelines that require financial institutions to verify the identity and legitimacy of customers, helping to prevent money laundering and other financial crimes.
Machine Learning (ML) is a type of artificial intelligence that enables systems to learn and make decisions based on data and experience, often used in transaction monitoring to detect and prevent fraud.
Malware is a type of software that is designed to harm or exploit systems, often used in cyber attacks to steal data or disrupt operations.
Merchant is a business or individual that accepts payments for goods or services, often using online payment systems and transaction monitoring techniques.
Mobile Payment is a type of payment that uses a mobile device, such as a smartphone or tablet, to initiate and complete transactions.
Money Laundering is the process of concealing or disguising the source of illicit funds, often using financial systems and transactions to make the funds appear legitimate.
Network Security involves the use of various techniques and strategies to protect networks from unauthorized access, use, or malicious activity.
Online Banking is a type of banking that uses the internet to provide financial services, such as account management, bill payment, and fund transfers.
Online Payment System is a type of system that facilitates online payments, often using payment processors, gateways, and transaction monitoring techniques.
Payment Card Industry Data Security Standard (PCI DSS) is a set of regulations and guidelines that require merchants and financial institutions to protect sensitive payment card information.
Payment Gateway is a type of system that facilitates online payments, often using payment processors and transaction monitoring techniques.
Payment Processor is a type of company that handles payment transactions, often providing services such as payment processing, settlement, and reporting.
Phishing is a type of cyber attack that uses social engineering to trick users into revealing sensitive information, such as passwords or financial data.
Predictive Analytics involves the use of statistical models and machine learning to predict future events or trends, often used in transaction monitoring to detect and prevent fraud.
Public Key Infrastructure (PKI) is a set of technologies and policies that enable secure communication over the internet, using digital certificates and encryption.
Real-Time Gross Settlement (RTGS) is a type of payment system that settles transactions in real-time, often used in high-value or time-sensitive transactions.

Risk Management involves the process of identifying, assessing, and mitigating risks, often used in transaction monitoring to prevent fraud and minimize losses.
Secure Sockets Layer (SSL) is a type of encryption protocol that protects data in transit, often used in online payment systems and transaction monitoring.
Security Information and Event Management (SIEM) is a type of system that monitors and analyzes security-related data, often used in transaction monitoring to detect and prevent cyber attacks.
Security Token is a type of token that represents a security or asset, often used in online payment systems and transaction monitoring.
Social Engineering is a type of cyber attack that uses psychological manipulation to trick users into revealing sensitive information or performing certain actions.
Structured Query Language (SQL) is a type of programming language that manages and manipulates data in relational databases, often used in transaction monitoring to detect and prevent fraud.
Suspicious Activity Report (SAR) is a type of report that flags suspicious transactions or activities, often used in transaction monitoring to prevent money laundering and other financial crimes.
System Integration involves the process of combining multiple systems or applications to create a cohesive and efficient workflow, often used in transaction monitoring to provide a comprehensive view of transactions.
Transaction Monitoring involves the use of various techniques and strategies to monitor and analyze transactions, often used to detect and prevent fraudulent activities.
Transaction Risk Assessment involves the process of evaluating the risk associated with a particular transaction or user, often used in transaction monitoring to prevent fraud and minimize losses.
Two-Factor Authentication (2FA) is a type of authentication that requires two forms of verification, such as a password and a biometric scan, to ensure secure access to systems and data.
User Entity Behavior Analytics (UEBA) is a type of analytics that monitors and analyzes user behavior, often used in transaction monitoring to detect and prevent insider threats and cyber attacks.
Virtual Private Network (VPN) is a type of network that encrypts and protects internet traffic, often used in transaction monitoring to provide secure and private communication.
Whitelisting involves the process of approving or allowing specific users, devices, or transactions, often used in transaction monitoring to prevent fraudulent activities.
Wire Transfer is a type of payment that uses a network of banks and financial institutions to transfer funds, often used in high-value or time-sensitive transactions.
XML (Extensible Markup Language) is a type of programming language that manages and manipulates data in a structured and standardized way, often used in transaction monitoring to exchange data between systems.