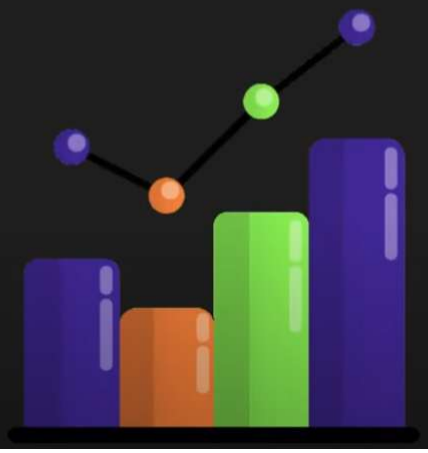
Fraud Classification

- Application level
  - New account frauds
    - Id theft
    - 1st party
    - Old age vulnerable adult attacks
    - Bogus claims
- Transaction Level
  - 3rd party fraud
  - ATO (a/c take over fraud)

Fraud Mitigation

- Rules generation
- Fraud score generation
- Threshold generation



Let's break down the fraud concepts discussed, adding more detail and examples to clarify each point.

I. Types of Fraud:

Fraud is broadly categorized into application-level and transaction-level fraud.

- **A. Application-Level Fraud:** This type of fraud occurs when a fraudulent account is created or manipulated.
- **1. New Account Fraud (using stolen IDs):** A fraudster uses someone else's personal information (name, address, Social Security number, etc.) to open a new account (credit card, bank account, online retail account).

- *Example:* A thief steals a wallet containing a driver's license and credit card. They use this information to apply for a new credit card in the victim's name, running up charges before the victim realizes what happened.
- **2. First-Party Fraud:** The account holder themselves commits fraud. This often involves making purchases with no intention of paying, or deliberately providing false information on an application.
- *Example:* Someone opens a credit card, maxes it out on expensive electronics, and then declares bankruptcy to avoid paying the bill. Or, someone lies about their income on a loan application to get approved.
- **3. Old Age/Vulnerable Adult Attacks:** Fraudsters target elderly or vulnerable individuals, often through scams and manipulation, to gain access to their finances. This can involve romance scams, tech support scams, or pressure to invest in fraudulent schemes.
- *Example:* A con artist calls an elderly person claiming to be from their bank, warning of a security breach. They trick the victim into revealing their account details and then steal their savings.
- **4. Bogus Claims:** A customer makes false claims to get refunds or credits they are not entitled to. This can involve claiming items were not delivered, arrived damaged, or were not as advertised.
- *Example:* A customer orders a product online, receives it, and then claims it never arrived, demanding a refund and getting to keep the product for free.
- **B. Transaction-Level Fraud:** This type of fraud occurs during a transaction, often involving unauthorized access to an existing account.
- **1. Third-Party Fraud (Account Takeover - ATO):** A fraudster gains control of someone else's account (e.g., banking, email, social media) and makes unauthorized transactions. This is often done through phishing, malware, or data breaches.
- *Example:* A hacker steals usernames and passwords from a website. They use these credentials to log into users' bank accounts and transfer money to their own accounts.

II. Fraud Detection Techniques:

Fraud analysts use various techniques to detect and prevent fraud.

- **A. Rules and Fraud Scores:** Analysts create rules to flag suspicious transactions. They also develop fraud scores based on various factors. These scores can be adjusted over time as fraudsters adapt their methods.
- *Example:* A rule might flag any transaction over $1,000 made outside the customer's usual geographic area. A fraud score might combine multiple factors, such as transaction amount, location, and time of day, to assess the risk of fraud.
- **B. Threshold-Based Alerting:** Alerts are triggered when specific thresholds are met. For example, if a customer's spending suddenly increases dramatically, an alert might be generated.

- *Example:* A customer typically spends around $100 per week on their credit card. If they suddenly make a $5,000 purchase, an alert is triggered for review.
- **C. Key Factors Used to Detect Fraud:**
- **1. Billing and Shipping Address Discrepancy:** If the billing address (where the credit card statement is sent) and the shipping address (where the goods are delivered) don't match, it's a red flag.
- *Example:* A fraudster uses a stolen credit card to buy a laptop and has it shipped to a different address than the cardholder's.
- **2. BIN Match Issues:** The Bank Identification Number (BIN) identifies the issuing bank and country. If the BIN's location doesn't match the shipping or billing address, it's suspicious.
- *Example:* A credit card issued by a bank in Canada is used to make a purchase with a shipping address in Brazil.
- **3. VPN Usage:** Virtual Private Networks (VPNs) can mask a user's IP address, making it harder to track their location. Fraudsters often use VPNs to hide their tracks. Sudden changes in IP address or multiple transactions from different countries in a short time can indicate VPN usage and potential fraud.
- *Example:* A user's IP address suddenly changes from the US to Russia, then to China, all within a few hours, while making online purchases.
- **4. IP Address Changes:** Similar to VPN usage, frequent or unusual changes in IP address can be a sign of fraud.
- *Example:* A user typically accesses their online banking from an IP address in their home city. If they suddenly start accessing it from multiple IP addresses in different countries, it's suspicious.
- **5. Demographic Changes:** Unusual changes in a customer's purchasing patterns can also be a sign of fraud.
- *Example:* A customer who typically buys groceries and household items suddenly starts purchasing high-end electronics or jewelry. Or, as mentioned in the original text, a senior citizen suddenly starts buying gaming consoles. This could indicate account takeover or identity theft.

These are just some of the many techniques used in fraud detection. The field is constantly evolving as fraudsters develop new methods, and analysts develop new ways to counter them.

Let's delve deeper into payment fraud, exploring the various types, methods, and prevention strategies with detailed examples.

I. What is Payment Fraud?

Payment fraud occurs when someone makes an unauthorized or illegitimate transaction. This can be intentional (e.g., using a stolen credit card) or unintentional (e.g., accidentally clicking on a phishing link).

II. Types of Payment Fraud:

- **A. Credit Card Fraud:** Unauthorized use of someone else's credit card information to make purchases.
- *Example:* A thief steals a credit card and uses it to buy electronics online.
- **B. Debit Card Fraud:** Similar to credit card fraud, but the funds are directly withdrawn from the cardholder's bank account.
- *Example:* A scammer obtains a debit card number and PIN and uses it to withdraw cash from an ATM.
- **C. Bank Fraud:** A broader category that includes various fraudulent activities targeting banks and their customers. This can include loan fraud, check fraud, and account takeover.
- *Example 1 (Loan Fraud):* Someone uses a fake identity and false financial documents to obtain a loan, with no intention of repaying it.
- *Example 2 (Check Fraud):* Someone forges a check or alters the amount on a legitimate check to steal money from an account.
- **D. Mobile Wallet Payment Fraud:** Unauthorized use of a mobile wallet (e.g., Apple Pay, Google Pay) to make purchases.
- *Example:* A thief steals a phone and uses the owner's unlocked mobile wallet to make purchases.

III. How Payment Fraud Happens (Methods):

- **A. Phishing:** Deceptive emails, text messages, or websites that trick individuals into revealing personal information (passwords, credit card details, etc.).
- *Example:* A person receives an email that looks like it's from their bank, asking them to click on a link and verify their account details. The link leads to a fake website that steals their information.
- **B. Skimming:** Illegally copying data from a credit or debit card using a skimming device, often attached to ATMs or point-of-sale terminals.
- *Example:* A scammer installs a skimmer on a gas pump. When someone swipes their card, the skimmer captures their card information.
- **C. ID Theft:** Stealing someone's personal information (name, Social Security number, date of birth, etc.) to open accounts, apply for loans, or make purchases in their name.
- *Example:* A hacker steals personal data from a company's database and uses it to open a credit card in someone else's name.
- **D. Chargebacks (Fraudulent):** A customer makes a purchase and then falsely claims that they didn't authorize the transaction to get a refund.

- *Example:* Someone buys a product online and then contacts their bank to dispute the charge, claiming they never made the purchase.
- **E. Malware Attacks:** Malicious software that infects devices and steals personal or financial information.
- *Example:* A person downloads a seemingly harmless app that contains malware. The malware steals their banking information and sends it to a hacker.
- **F. Social Engineering:** Manipulating individuals into divulging confidential information or performing actions that compromise security.
- *Example:* A scammer calls someone pretending to be from their IT department and asks for their password to "fix a problem."

IV. Impact of Payment Fraud:

- **A. Financial Losses:** Direct losses for both consumers and financial institutions.
- **B. Reputational Damage:** Loss of trust and customers for banks and businesses.
- **C. Legal Penalties:** Fines and regulatory actions for businesses that fail to protect customer data.

V. Payment Fraud Prevention:

- **A. Chip Cards (EMV):** Credit and debit cards with embedded microchips that make them more difficult to counterfeit.
- **B. NFC (Near Field Communication):** Contactless payment technology that reduces the risk of card skimming.
- **C. Two-Factor Authentication (2FA):** Requiring a second form of verification (e.g., a code sent to a phone) for transactions.
- **D. 3D Secure Cards:** Adding an extra layer of security for online transactions, often requiring a password or code.
- **E. Awareness and Education:** Educating consumers about common fraud schemes and how to protect themselves. This includes being wary of phishing emails, using strong passwords, and monitoring account activity.
- **F. Strong Passwords and Unique Accounts:** Using different, complex passwords for each online account makes it much harder for hackers to gain access even if one account is compromised.
- **G. Monitoring Account Activity:** Regularly checking bank and credit card statements for unauthorized transactions is crucial for early detection of fraud.
- **H. Secure Browsing Practices:** Avoiding suspicious websites and being cautious about clicking on links in emails or messages helps prevent malware infections and phishing attacks.
- **I. Up-to-Date Software:** Keeping operating systems, apps, and antivirus software updated ensures that security vulnerabilities are patched and helps protect against malware.

This is a really comprehensive set of lectures on fraud analytics! Let's break down the key concepts and examples provided, adding further details for clarity.

Lecture 1: Credit Card Life Cycle - Application and Approval

- **Applying for a Credit Card:**
- There are various ways to apply: online, bank branch, airport kiosks, etc.
- The application process involves providing personal and financial information (demographics, income, existing loans, etc.).
- The bank assesses eligibility and suggests suitable credit card products based on the applicant's profile.
- **Behind the Scenes:**
- **Validation:** The bank verifies the applicant's information and checks their existing relationship with the bank.
- **Credit Scoring:** A credit score is calculated to assess the applicant's creditworthiness (likelihood of repaying debt).
- **Fraud Scoring:** A fraud score is generated to evaluate the risk of fraudulent activity or default.
- **Third-Party Checks:** The bank may consult credit bureaus to obtain the applicant's credit history and background information.
- **Decision:** Based on the gathered information, the bank approves, declines, or puts the application under review.
- **Upselling/Downselling:** The bank may offer a higher-tier card (upsell) or a lower-tier card (downsell) based on the risk assessment.

Lecture 2: Third-Party Products and Interfaces

- **Why Third-Party Products?**
- Banks use third-party products and services to address specific challenges and risks, such as fraud prevention and identity verification.
- These services provide valuable insights and data from across different institutions, enhancing the bank's ability to protect itself and its customers.
- **Key Third-Party Products and Services:**
- **Strategy Management Teams:** Analysts who develop rules and scoring systems to assess transactions and applications for risk.
- *Example:* A rule might be created to block transactions from a specific merchant known for fraudulent activity.
- **Credit Bureaus:** (e.g., TransUnion, Equifax, Experian) Provide credit reports and scores that help banks assess an individual's creditworthiness.

- **Identity Verification Agencies:** (e.g., UIDAI in India) Verify the identity of individuals to prevent identity theft and fraud.
- **Document Management Systems (DMS):** Securely store and manage customer documents (e.g., identification, loan applications).
- **AI and Machine Learning (ML):** Used to analyze large datasets, detect patterns, and identify potential fraud more accurately and efficiently.

Lecture 3: Post-Approval Process

- **Record Setup:**
- **Customer Record:** Stores personal information (name, contact details, employment, etc.).
- **Account Record:** Contains credit card specific information (account number, credit limit, transaction history).
- **Card Record:** Manages information related to the physical card itself.
- **Account Setup:**
- **Batch Processing:** Multiple applications are processed together in batches.
- **Real-Time Processing:** Accounts are set up immediately upon approval.
- **Card Setup:**
- The physical card is produced and sent to the customer along with a welcome kit.
- The PIN is generated and sent separately for security.

Lecture 4: Key Terminologies in Fraud Analytics

- **Card Life Cycle Terminologies:**
- **Customer:** The person making the purchase.
- **Merchant:** The seller providing the goods or services.
- **Issuing Bank:** The bank that issued the customer's credit/debit card.
- **Acquiring Bank:** The bank that processes the payment for the merchant.
- **Card Associations:** (e.g., Visa, MasterCard, RuPay) Facilitate transactions between issuing and acquiring banks.
- **Transaction Flow:**

1. Customer initiates a purchase.
2. Merchant sends transaction details to the acquirer.
3. Acquirer forwards the request to the card association.
4. Card association routes the request to the issuing bank.
5. Issuing bank authenticates and authorizes the transaction.
6. Funds are transferred from the customer's account to the merchant's account.

- **On-Us vs. Off-Us Transactions:**
- **On-Us:** Both customer and merchant have accounts at the same bank.
- **Off-Us:** Customer and merchant have accounts at different banks.
- **Card Present vs. Card Not Present:**
- **Card Present:** Physical card is used at the point of sale (POS).
- **Card Not Present:** Card details are entered manually, typically for online transactions.

Lecture 5: 3DS vs. Non-3DS Transactions

- **3DS (Three-Domain Secure):**
- Requires cardholder verification (e.g., password, OTP) during online transactions.
- Examples: Verified by Visa, MasterCard SecureCode.
- Reduces fraud risk and shifts liability from the merchant to the card issuer in case of fraud.
- **Non-3DS:**
- No additional verification step.
- Higher risk of fraud for the customer.
- Merchant is liable for fraudulent transactions.

Lecture 6: Role of a Fraud Analyst

- **Monitoring:**
- Tracks key performance indicators (KPIs) like transaction count, amount, alerts, claims, etc.
- Monitors application flow across different channels.
- **Threshold Generation:**
- Sets thresholds based on historical data and trend analysis using statistical methods (mean, standard deviation, IQR).
- Thresholds are updated periodically to adapt to changing fraud patterns.
- **Alerting:**
- Uses visualization tools (e.g., Tableau, Power BI) to create dashboards and set up alerts.
- Automated alerts are triggered when thresholds are breached.
- Alerts are reviewed and investigated by analysts.
- **Rule Generation:**
- Collaborates with the strategy team to develop rules for identifying and preventing fraud.
- Rules are incorporated into dashboards for automated alerting.

Lecture 7: Case Study - Fraud Rule Creation

- **Scenario:** Multiple customers report unauthorized transactions from a specific merchant (ABC).
- **Investigation:**
- Monitoring analyst identifies a spike in transactions and suspicious patterns related to merchant ABC.
- Strategy analyst investigates further, reviews customer disputes, and analyzes fraud scores.
- **Rule Creation:** A rule is created to flag transactions from merchant ABC with high fraud scores, requiring additional verification from the customer.
- **Implementation:** The rule is implemented to prevent future fraudulent transactions while minimizing false positives.
- **Evaluation:** The effectiveness of the rule is monitored and adjusted as needed.

This series provides a comprehensive overview of fraud analytics, covering key concepts, terminologies, and processes involved in detecting and preventing fraud. The practical case study demonstrates how fraud analysts use data analysis and rule generation to protect customers and businesses from financial losses.