***Online Fraud Detection***

**1. What is Fraud?**

Fraud essentially involves using deception to dishonestly make a personal gain for oneself / or crate a loss for other.

The term “fraud” Commonly includes activities such as theft, corruption, embezzlement, money laundering, bribery and extortion.

**2. Different Kind of Fraud?**

Fraud can mean many things and result from many varied relationships between offenders and victims.

* Crimes by individuals against consumers, clients or other business people, e.g. misrepresentation of the quality of goods; pyramid trading schemes
* Employee fraud against employers, e.g. payroll fraud; falsifying expense claims; thefts of cash, assets or intellectual property (IP); false accounting
* Crimes by businesses against investors, consumers and employees, e.g. financial statement fraud; selling counterfeit goods as genuine ones; not paying over tax or National Insurance contributions paid by staff
* Crimes against financial institutions, e.g. using lost and stolen credit cards; cheque frauds; fraudulent insurance claims
* Crimes by individuals or businesses against government, e.g. grant fraud; social security benefit claim frauds; tax evasion
* Crimes by professional criminals against major organizations, e.g. major counterfeiting rings; mortgage frauds; ‘advance fee’ frauds; corporate identity fraud; money laundering
* E-crime by people using computers and technology to commit crimes, e.g. phishing; spamming; copyright crimes; hacking; social engineering frauds.

**3. Producting customer’s confidential Information**

Any business that stores personal data such as customer’s payment card information is responsible for keeping that information secure .This is true of online business as well as brick and mortar organizations.

Data breaches produce unwelcome publicity that can have a severe negative impact on a retail organization’s brand and reputation.

**Payment Card Industry Data Security Standard (PCI-DSS)**

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary [information security](https://en.wikipedia.org/wiki/Information_security) standard for organizations that handle branded [credit cards](https://en.wikipedia.org/wiki/Credit_card) from the major card schemes including Visa, MasterCard, [American Express](https://en.wikipedia.org/wiki/American_Express), [Discover](https://en.wikipedia.org/wiki/Discover_Card), and [JCB](https://en.wikipedia.org/wiki/Japan_Credit_Bureau). The PCI Standard is mandated by the card brands and administered by the [Payment Card Industry Security Standards Council](https://en.wikipedia.org/wiki/Payment_Card_Industry_Security_Standards_Council). The standard was created to increase controls around cardholder data to reduce [credit card fraud](https://en.wikipedia.org/wiki/Credit_card_fraud).

Payment Card Industry Data Security Standard (PCI-DSS), which is a set of obligations mandated by card networks to help protect consumers’ personal information. These PCI requirements pertain to how the data is stored, accessed, and handled by a business. Organizations that store account information are required to certify that they are in compliance with PCI standards. This certification process, which must be done periodically, can be expensive and time-consuming.

**Card Not Present**

Whenever a [Transaction](https://www.2checkout.com/ecommerce-glossary/transaction-settlement) is completed and the cardholder (or his or her credit card) is not physically present to hand to the seller.

A **card not present transaction** (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC) is a [payment card](https://en.wikipedia.org/wiki/Payment_card) transaction made where the cardholder does not or cannot physically present the card for a merchant's visual examination at the time that an order is given and payment effected, such as for mail-order transactions by mail or over the [telephone](https://en.wikipedia.org/wiki/Telephone) or [Internet](https://en.wikipedia.org/wiki/Internet).

Card not present transactions are a major route for [credit card fraud](https://en.wikipedia.org/wiki/Credit_card_fraud), because it is difficult for a merchant to verify that the actual cardholder is indeed authorizing a purchase.

The [Address Verification System](https://www.2checkout.com/ecommerce-glossary/address-verification-system) is one way that the card associations encourage sellers and banks to monitor for fraud in CNP Transactions.

**Address Verification System**

A service used to verify a card holder's billing address. A system created and maintained by Visa, the Address Verification System was designed to prevent fraudulent activity by allowing a [Merchant](https://www.2checkout.com/ecommerce-glossary/merchant) to verify whether a credit card's given address matches the address in the [Card Issuer's](https://www.2checkout.com/ecommerce-glossary/issuing-bank) system. This system is especially useful in situations where a buyer and a merchant do not complete their Transaction in person but online.

**Tools for Detecting and Preventing Fraud Transactions**

**1).Automated transactional risk scoring**

Specific logic and settings can help to distinguish normal purchase behavior from risky transactions. Fraud risk is calculated based on multiple data factors and assigned a numerical score for each transaction. The scores, which serve as relative risk indicators, determine “next steps” for that transaction according to a merchant’s preferred operating procedures.

Additionally, you need to be able to identify transactions for which the cost of an additional verification may be higher than the potential fraud loss. You need to decide whether your policy for such transactions should be to be processed without any further verification or to be rejected.

**Fraud Scoring**

Fraud scoring models are used to identify and rate the highest-risk [card-not-present transactions](http://blog.unibulmerchantservices.com/9-steps-to-processing-card-not-present-transactions) that need to be additionally verified. They can pick up patterns of fraudulent activity and can differentiate these patterns from legitimate transaction activity. A numeric value (a score) is calculated for each transaction, reflecting the probability that it may be fraudulent.

**How Is a Fraud Score Calculated?**

Each transaction’s fraud score is a sum of the points the model assigns for various high-risk elements. Such elements typically include the following:

* Geo location taken from the IP address.
* Anonymous IP address.
* AVS result code.
* Time of day the order is placed
* Type of merchandise.
* Shipment method.
* Sale’s amount.
* Evidence of previous fraud on this card account.
* Number of computers that have placed orders with this card account.
* Different shipping and billing addresses.
* Mismatch between time zone and geo location.
* Length of time as a customer.
* ZIP codes.

**How to Use a Fraud Scoring Model**

Your fraud scoring system should allow you to

* Identify multiple orders placed with the same shipping address, but with different cards. This may indicate that criminals have stolen several card numbers.
* Identify orders for an unusually high count of a single item.
* Check if multiple orders are placed from the same IP address.
* Check the card numbers – if they vary by only a few digits, these numbers may be software-generated.
* Identify orders with the same card number, but different expiration dates. Often criminals who have stolen a card number don’t know the expiration date, so they will keep trying to guess it.
* Account for the fact that most [fraudulent e-commerce](http://blog.unibulmerchantservices.com/how-to-handle-potentially-fraudulent-e-commerce-transactions) orders in the U.S. are placed between midnight and 2 a.m.

**2) Real-time categorizing and resolution**

Transactions with risk scores exceeding certain thresholds—determined by either the merchant or the fraud solution provider—can be automatically placed into different categories for further action. Generally, a transaction is either immediately accepted or rejected—but it can also be flagged for manual review if it falls somewhere between those two categories. Depending on the fraud solution provider, this categorization process may require manual efforts to synchronize with the authorization, settlement, and fulfillment procedures.

**Powerful fraud management capabilities**

* Determine what levels of risk are acceptable for various products, order profiles, shopping behaviors, and other combinations of factors
* Adjust rules and logic as needed, based on evolving fraud patterns
* Streamline administrative processes during the entire life cycle of a transaction.