

## White Paper



### Fraud Management in the Online Retail Environment

---

Guneet S Paintal

Almost 28% of all online retailer orders are affected by fraud. The efficiency of the fraud management process thus has a direct impact on ecommerce profitability, operating efficiency and scalability

## Background

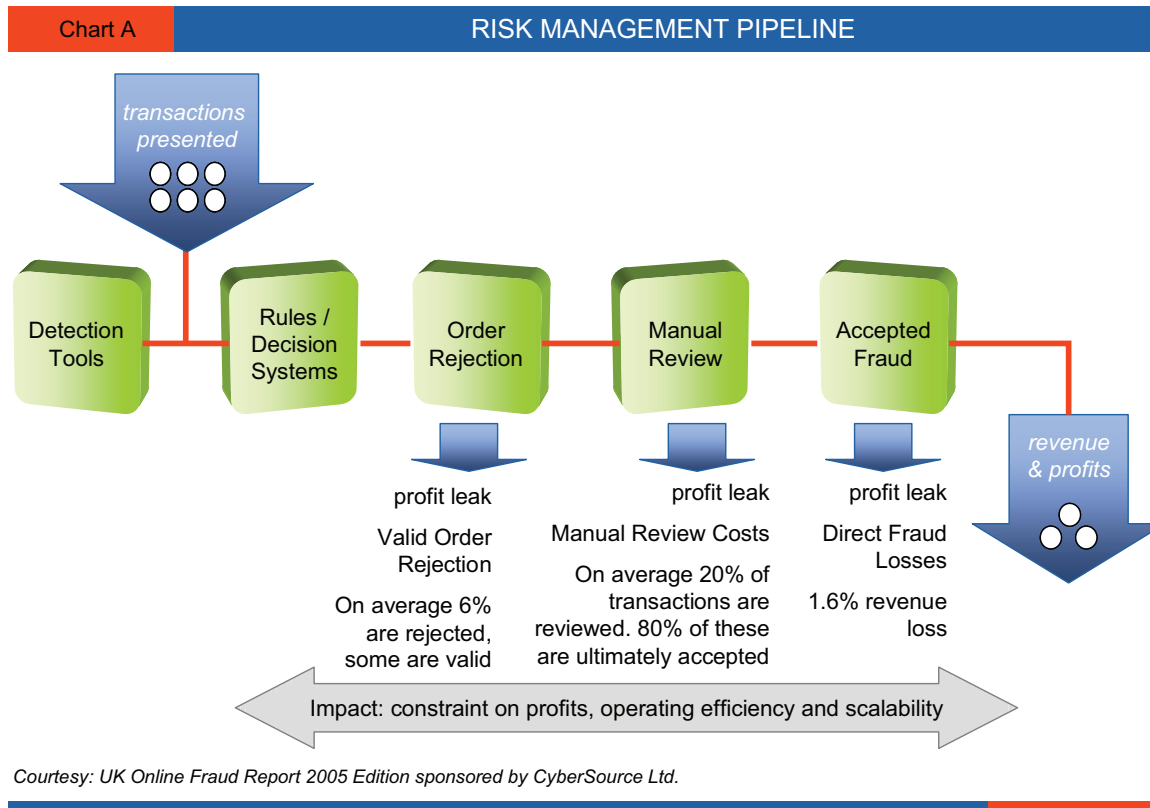
According to a report by Forrester Research, Inc, US online retail sales this year are expected to be around \$211.4 billion. It is also projected that online sales will reach \$316 billion by 2010. This e-commerce growth is expected to account for 12 percent of total retail sales in 2010; up from nearly 7 percent in 2004. This is predicated on the growing population of online shopping households, combined with effective multi channel integration and site improvements from retailers.

Another survey of Internet merchants by CyberSource Corp. has projected that online merchants will lose \$3 billion due to fraud. This is up 7% as compared to fraud losses last year. The Merchant Risk Council (MRC), the retail industry's premier association for preventing online fraud, in its most recent survey has revealed two significant trends. Online fraud rates for merchants surveyed are now similar to the fraud rates of brick-and-mortar stores, and fraud spikes and fraudsters' use of increasingly sophisticated schemes keep retailers on alert.

This whitepaper attempts to describe the tools, processes and systems for the detection, prevention and management of online fraud.

Many merchant surveys indicate improving trends such as decrease in online fraud charge back rates and better control of direct costs of online fraud. However these surveys also reveal that the indirect, hidden costs of fraud are extremely high and hitting businesses hard. The costs of fraud management are proving to be as troubling for online merchants as the cost of fraud itself. These costs are associated with the following processes:

- Almost 1.6% of orders result in chargebacks to the merchants due to direct fraud.
- 81% of merchants surveyed (by MRC) named manual review as a method of managing online fraud, making it the preferred tool for fraud prevention. With the projected substantial growth in online sales, it is likely that those merchants relying on manual review will have experienced a significant increase in their operational costs as they attempt to scale the number of review staff with the growth in online sales.
- Since most manual review processes involve customer follow up and validation, it results in inconveniencing the customer as they need to provide more information as well as wait longer for fraud verification and thus delivery of purchased products. This invariably results in lost sales and lower repeat sales. This may even lead to gains by competing retailers with better fraud screens.
- Fraud management also creates another cost in the form of rejecting valid transactions. As per the CyberSource survey, as much as 4.1% of orders are rejected on the suspicion of fraud. Estimates indicate that as much as one fifth of these rejected orders were actually valid leading to the certainty that much valid business is being rejected.



The impact of online fraud casts a larger shadow over profitable ecommerce operations than just the visible direct costs of fraud. Apart from the average direct fraud loss of 1.6% there is almost 6% of orders that merchants decline to process as well as the number of orders being manually reviewed (20%). It thus becomes apparent that between 27% and 28% of merchants orders are affected by fraud. Thus the efficiency of this process has a direct impact on profits, operating efficiency and scalability.

## Fraud Prevention Tools

In order to combat fraud online retailers have the option to use different types of fraud prevention tools and techniques. These can be typically classified into the following categories

- Online payment authorizations of credit cards
- Address Verification Services/Systems (AVS)
- Use of card verification codes (CVV, CVV2)
- Negative files
- Risk Prediction Techniques/Models
- Rules based detection techniques
- Manual reviews
- Verified by Visa / MasterCard SecureCode

There is also a growing trend amongst online retailers to avoid credit card based fraud by actively encouraging and supporting the use of alternate forms of tender. These include outsourced services such as Paypal and the use of gift cards and e-checks.

**Online payment authorizations:** This process ensures that the credit card being used is not lost or stolen. It also makes sure that the card has enough credit balance to pay for the purchase. It cannot however make out that the person using the card is actually authorized to do so.

**Address Verification Services/Systems (AVS):** An AVS check matches the billing address provided by the customer with the billing address on file for that credit card. The customer's address data is submitted together with each payment authorization request. The system responds with a "score" signifying how well the address data matched. This tool when used on its own is not very effective as it may not lead to a match in as many as 40% of the transactions and it is also possible that a fraudster will have the billing address of the credit card, hence nullifying the advantage of such a check.

**Card Verification Codes (CVV, CVV2, CID):** These codes consist of 3 or 4 digit numbers printed on the front or back of credit cards. These codes are required along with the credit card details for authorizations to occur. These codes are not printed on receipts or stored in retailer databases to prevent easy access of the same by fraudsters. This process requires that the card be physically present at the time of the transaction thus reducing card not present fraud scenarios.

**Negative Files:** These files typically define the set of minimum criteria an order transaction must satisfy before proceeding for fulfillment. These consist of lists of known fraudulent data such as email ids, stolen credit card numbers, bad shipping addresses etc. These files are based on past experiences, data mining of fraudulent orders and periodic updates by credit card companies.

**Risk Prediction Techniques/Models:** Risk prediction model software analyzes data from millions of online sales to extract the profile of fraudulent transactions. Based on these large and historical order samples, the software develops an algorithm to identify fraudulent orders. Every order transaction is evaluated by passing its attributes through this algorithm and a risk score is arrived at. Thresholds of this score can be used to identify orders to reject, review or accept.

**Rules Based Detection:** With rule-based detection software, online merchants define a set of criteria that each order transaction must meet. These criteria are a combination of risk scores, order information (totals, items, fulfillment methods etc.), tender information, customer demographics, geo locations, order history etc. The software will automatically screen incoming orders by these specific criteria and automate the decision to reject, review, or accept the order.

**Manual Review:** This involves the manual review of potentially fraudulent orders by fraud analysts. These analysts review orders and get in touch with customers and payment providers to verify that orders are not fraudulent. This technique should be used in conjunction with risk prediction models and rules based detection. This ensures that the fraud analysts only look at a focused subset of orders having a high likelihood of being fraudulent. While manual review may be viable for smaller merchants with low order volumes, it is not normally a cost-effective or scalable solution for larger merchants with high order volumes or seasonal order peaks.

**Verified by Visa/ MasterCard SecureCode:** These programs enable two parties (card holder and card issuer) to authenticate each other by exchanging electronic passwords before proceeding with an online transaction. When a previously registered password is entered by a card holder and authenticated by the Visa/MasterCard system, the order cannot be charged back due to fraudulent reasons and the merchant is assured of zero liability by the payment providers. Implementation of payer authentication systems can protect merchants from certain chargebacks due to fraud, but this protection may only apply if a merchant can maintain low chargeback levels.

All of the tools mentioned above are complementary to one another, as they each inspect different components of a transaction. The best way to combat fraud is to use layers of fraud protection. These layers of fraud protection can be introduced at different stages within the order lifecycle. These stages can be classified into the order capture business process within the online store front and the order fulfillment business process within the order execution systems.

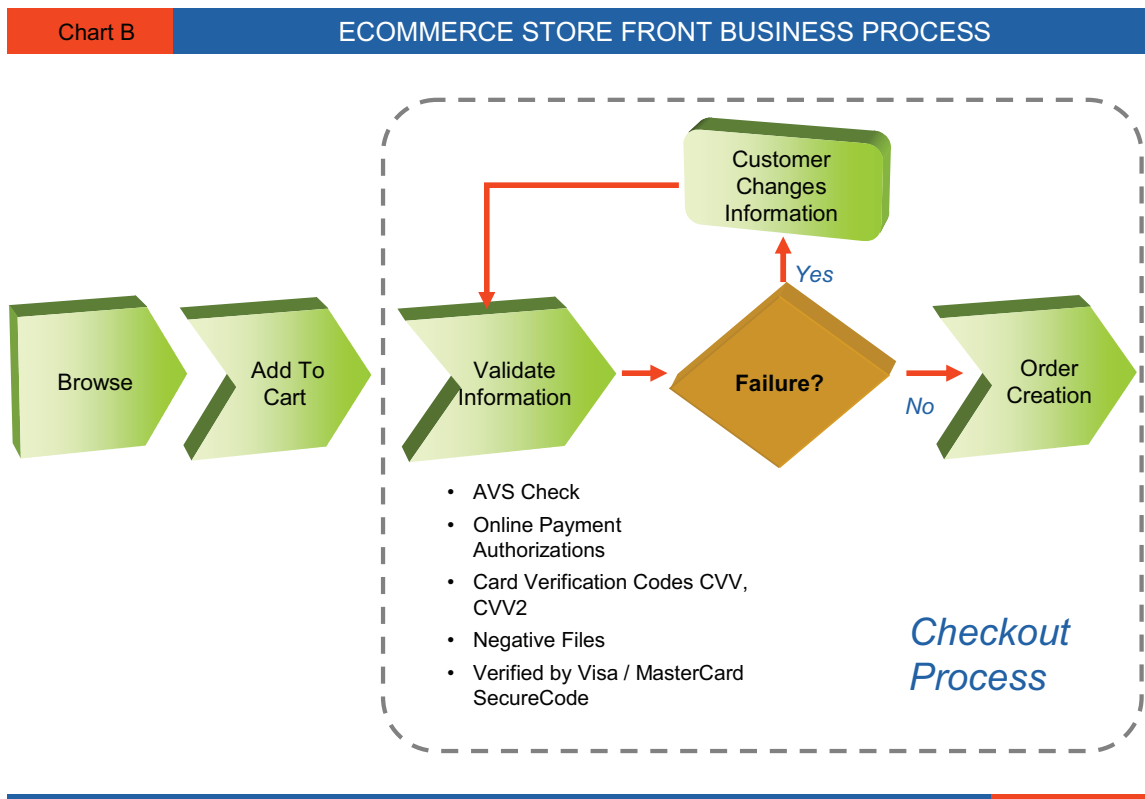
## Ecommerce Store Front Business Process

The Chart B illustrates the important activities within this process flow which start with a customer browsing the online store and end with checkout of the shopping cart as the customer purchases the products by providing a form of tender. From a fraud perspective, the tools should be invoked only after the customer has decided to buy the products. This implies that most of the 'front end' fraud checking starts during the checkout process.

The important considerations for invoking these tools during the checkout process are:

- From a marketing perspective, when the customer enters checkout, it implies a significant decision making point. The customer has essentially made the buying decision. It is thus very important for the retailer to design a quick and efficient checkout which can smoothly transition the customer from this intent to buy to the actual purchase. Hence all system interactions need to be quick and efficient.

- The online store business processes are also characterized by the online presence of the customer. The customer continuously interacts with the system and hence can correct 'mistakes' and make changes. This feature can be exploited as real time payment authorizations and AVS checks can make sure that in case the tender information does not match up, the customer can be asked to change their credit cards or their corresponding billing addresses. It is important to note that any changes required to the order or payment information after this point onward, requires the retailer to contact the customer manually thus increasing the costs associated with processing the orders.
- Since a large part of the indirect cost of fraud is associated with the manual review process, hence a funnel based approach needs to be applied for identifying fraud orders requiring this review. This means that the number of orders actually moving through for a fraud review should be reduced and confined to being orders with the highest likelihood of being fraudulent. The mouth of this funnel starts with the checkout process. Hence fraud tools such as negative file checks should be implemented at this point. This process is relatively quick, yet immediately eliminates the obviously 'bad' orders.



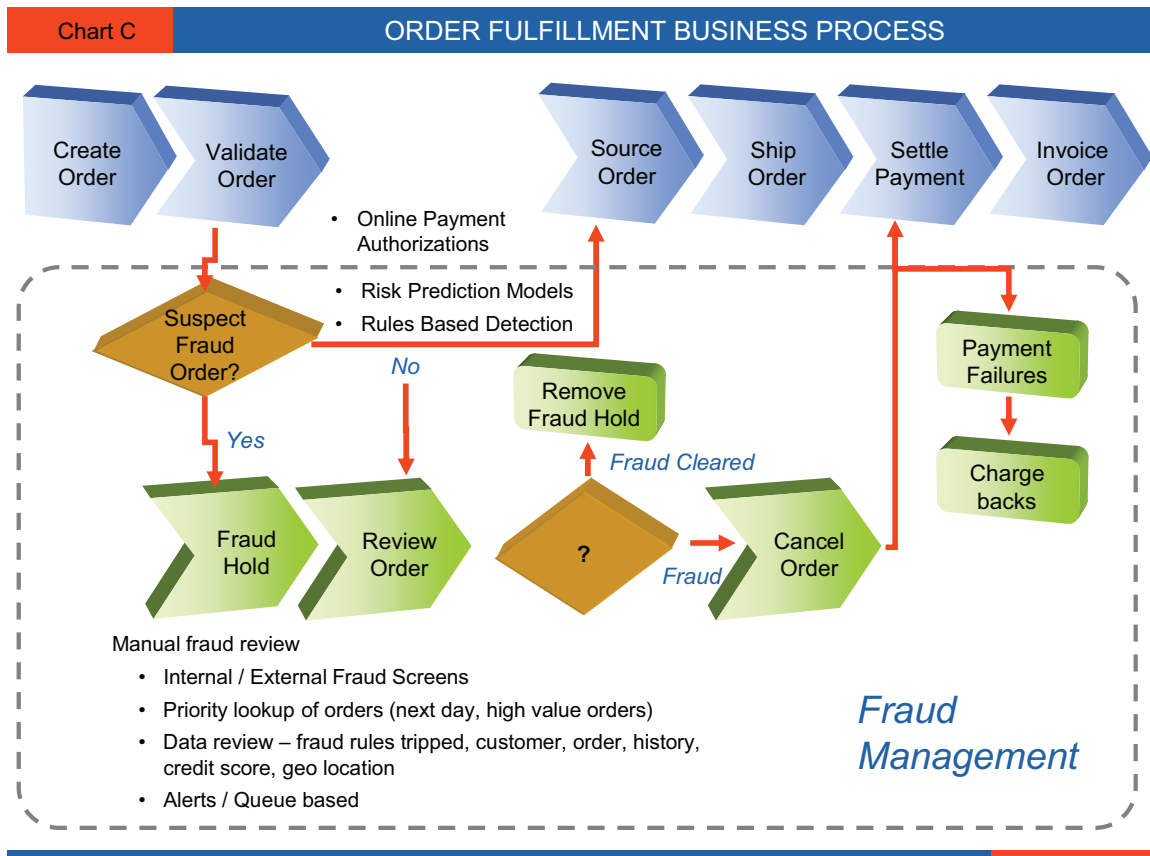
Based on the above considerations the fraud layer at the point of checkout can consist of real time payment authorizations, AVS check, card verification codes, Verified by Visa / Master SecureCode and the negative fraud checks.

The fraud processes associated with credit card payments such as real time authorizations, card verification codes, Verified by Visa / Master SecureCode and AVS check can be combined in the same authorization call to the payment gateways. The data required for the same include card numbers, types, expiration dates, codes and a password associated with the payment programs. The AVS check requires the passing of the billing address associated with the credit card.

The fraud negative check typically uses data such as customer email address, ip address obtained through geo location, shipping and billing address etc. A failure based on these criteria may result in the system preventing the order from being taken or in case of tracking purposes, allow the order to be created and then cancelled thus creating a persisted record of the transaction.

## Order Fulfillment Business Process

As illustrated in the Chart C, the order fulfillment business process ranges from the creation of the order to the ultimate shipping out and invoicing of the order. The order validation process is the activity dedicated to the fraud related processes.



The objectives of the fraud processes during this phase of the order lifecycle are:

- Reduce the number of false positives to avoid loss of sales due to unverifiable cancels and customer ‘insult’.
- Reduce the percentage of orders requiring manual review to a manageable 3-10% without an increase in chargeback rates.
- Increase the efficiency of the manual review process to improve fraud review turn around times.

These objectives can be achieved through a combination of fraud screens. At this stage the most effective and efficient techniques involve the use of rules based decision making and a risk prediction model. This is also the stage at which a comprehensive and efficient manual review process by fraud analysts is required.

As described earlier, the risk prediction models generate a risk score using an algorithm based on analysis of millions of history order transactions. This risk score is an important input to the fraud rules engine. Apart from the risk score, the rules engine also uses a series of order and customer data. This includes the price of items, order totals, tender types, customer demographics and item fulfillment methods (for e.g. in store pickup and home delivery orders have higher incidence of fraud). The rules engine has a series of custom rules defined which compare each of the above input parameters as well as a combination of the same against threshold values and automate the decision to accept, review or reject the orders.

An accept decision translates into a successful outcome of the order validate step and allows the order fulfillment process to continue. Almost all orders not accepted come back with a review decision. This typically results in an order being put on fraud hold and an alert being raised for a fraud analyst. This also triggers the initiation of the manual fraud review business process.

In order to prioritize the review of such orders, the alerts may be raised to different queues. For e.g. orders with next day or second day shipping require to be reviewed first. As a large part of the fraud management cost is associated with the manual review process, hence it is important to provide the fraud analyst all the information required in a summarized and efficient

manner. This information includes tender related details including provider phone numbers for tender verification, risk scores, fraud rules tripped etc. An analyst may need to contact the customer to verify her identity and potentially ask for changes in payment types etc. This implies that the analysts must have the capabilities to make tender related changes on the order and hence the ability to authorize in real time.

Based on the review process, the analyst may decide to reject the order. This results in the order cancellation process. This must tie back to the cancellation of inventory, refund of the customer’s payment type (if charged) and customer communication related to the cancellation and the refund. In case the analyst is successful in verifying the order, it is removed from fraud hold and allowed to proceed for order fulfillment. The analyst must also be provided the capability to escalate the order. This requires the ability to assign the fraud alert to escalation queues or other level 2 analysts.

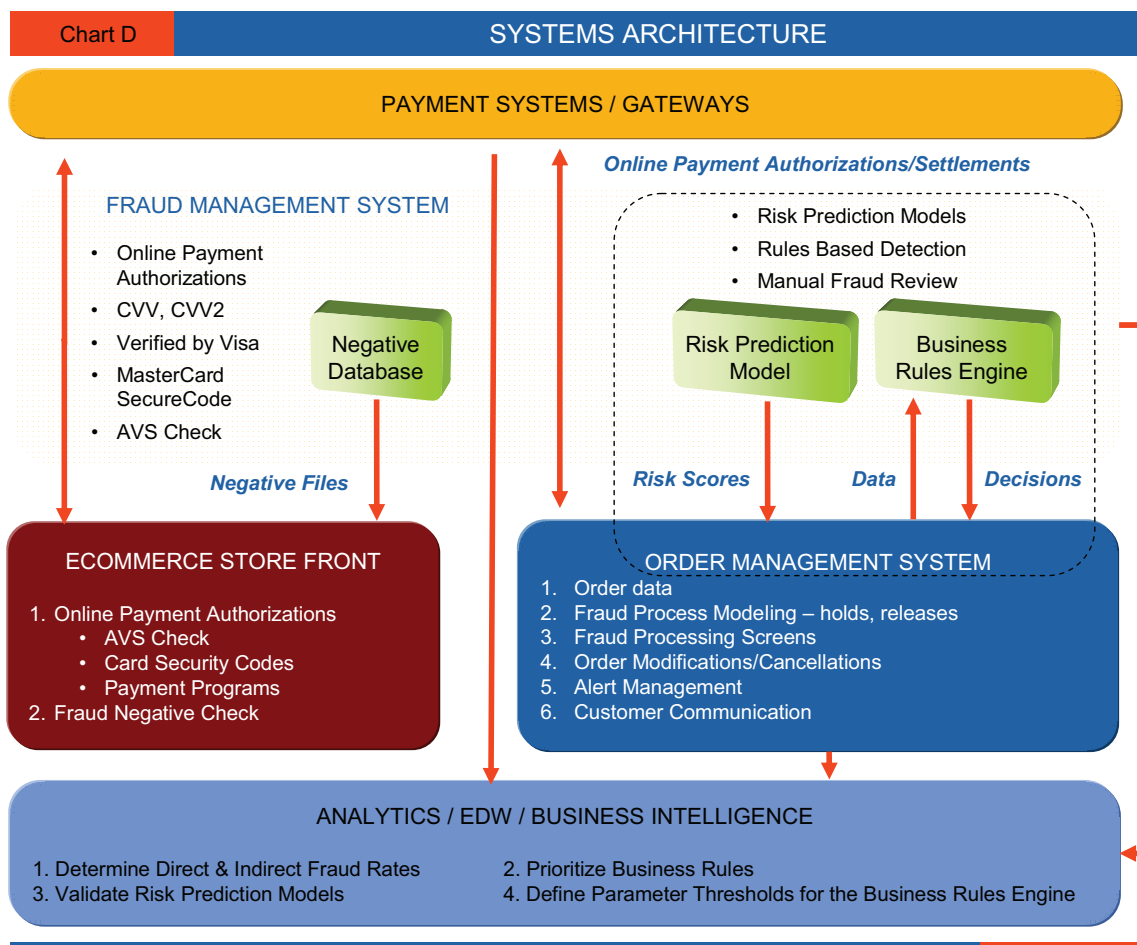
Despite the multiple fraud screens, some orders which are fraud cleared are fraudulent in nature and these results in chargebacks to the online merchants by the credit card companies. The process to handle these chargebacks also is an important feature of the fraud management process.

## Systems Architecture

The previous section illustrated the business process impacts of fraud management. This section translates these impacts into a feasible systems architecture definition. The objectives of this section are

- Identify the systems responsible for implementing the fraud management process.
- Identify the responsibilities of each of these systems based on best practices.

The Chart D below attempts to summarize the impacted systems and responsibilities associated with them



## *Ecommerce Store Front*

The online store front is a customer facing application. We have determined that the checkout process must support online payment authorizations, an AVS check, card verification codes, the payment programs for Visa/MasterCard and a fraud negative check. The credit card related interfaces can be invoked at the same time as the AVS check. The fraud negative check may involve a different interface to a fraud management system.

## *Payment Gateways*

There are potentially two different approaches associated with implementing a payment gateway for an online channel. These are based on the use of a commercial or custom built internal payment gateway.

- In case a commercial gateway is being used, there are standard APIs available to access the various payment related services such as authorizations (includes AVS check, card verification codes and Verified by Visa/MasterCard SecureCode), settlements, chargebacks, balance lookups etc. Since both the online store front end and the backend order management systems need to access these services, some amount of duplication is required in interfacing these systems to the gateways. The impact of the duplication is mitigated due to the presence of standard APIs of the commercial gateways.
- In case of a custom built or existing internal payment gateway, there maybe enhancements required to handle the new features such as Verified by Visa/MasterCard SecureCode etc. In order to reduce TCO, a payment abstraction layer may need to be built so that common services can be accessed by both the front end as well as the order management system.

## *Fraud Management System*

The fraud management system must have the following important features.

- Business rules engine to allow the setup and maintenance of custom business rules.
- Transaction processing APIs which allow multiple parameters as input, the ability to evaluate these parameters against the defined business rules and as a result provide as output the decision to accept, review or reject the order transaction.
- The ability to setup and maintain fraud negative lists.
- A risk prediction model or algorithm to provide a risk score based on historical data. It is possible that a single software may not be able to provide these capabilities. In such scenarios real time interfaces to an online risk prediction service (third party ASP model) may be required to determine the risk score which could then be used as an input to the business rules engine.
- A workflow engine to model the fraud business process. Another alternative is to build the workflow within the order management system (OMS). The details are as below.
- Fraud review screens for the fraud analysts to review the order information and the rules tripped. As above, the alternate approach could be to build these on the OMS.
- The ability to record and store authorization and settlement data for credit cards. This ability can be used to reconcile chargebacks from the payment providers against the original order transaction.

## *Order Management System*

The important activities performed by the OMS to facilitate the fraud management process are

- As in the case of the online store front, the OMS must provide the ability to interface with the payment gateway for real time authorizations, AVS checks, card verification codes, payment programs etc. This is based on the assumption that order and tender modifications are managed in the OMS.
- The order related information required as input by the fraud rules engine is supplied by the OMS. This implies that the OMS must have services to invoke the appropriate fraud APIs and act on the decisions provided by the rules engine.
- Based on the directives provided by the rules engine, the OMS must have the ability to put the order on hold and transition to the fraud business process. It should also have the ability to restart the order fulfillment process based on

an accept decision from the rules engine or the fraud analyst.

- The OMS ideally should provide workflow capabilities to model the fraud business process flow. This could also include fraud review screens, ability to generate alerts and manage fraud related queues.
- The fraud review process can result in changes to the order including cancellations (for fraudulent orders), changes in payment types (new credit cards provided by customer) etc. If these modifications are managed within the OMS, then it should provide the user interface to make these changes as well as manage the backend processes of de allocating inventory, refunding the customers money etc.
- In case the OMS manages the customer related communications (emails etc), hence it should also be able to manage the communication associated with payment and fraud related problems.

## Data Warehousing Systems (EDW) / Analytics

It is very important to have a data warehousing strategy associated with a fraud management implementation. The important functions to be performed by such a system are described below.

- The EDW needs to pull data from the fraud management system and the OMS.
- The extent of the fraud problem faced by an online retailer can only be determined through analysis of order history data. This helps determine the direct and indirect fraud rates.
- The validity of the business rules can be verified by using the EDW. They can also be prioritized based on analysis done on the EDW data.
- The risk prediction models are only as good as the history data provided. These models must be continuously validated and updated based on data pulled by the EDW system.
- The thresholds for the rules engine can be validated using the EDW.

## Conclusion

Although online retailers are becoming more confident with the handling of direct fraud, there is a growing dissatisfaction at the increasing costs associated with risk management, manual review and the rejection of potentially valid orders.

There is no 'silver bullet' solution to the problem of managing and reducing costs of online fraud. Efficient management of online fraud involves a toolkit based approach combining a series of fraud prevention tools and techniques to maximize operational efficiency and sales conversion, while minimizing the fraud risk.

A 'holistic' fraud solution impacts multiple order lifecycle phases. A comprehensive business process analysis of the ecommerce store front and OMS processes must include the strategy to handle fraud related activities. This white paper also highlights important considerations and best practices which should be kept in mind while defining these processes and implementing the associated systems.

### About the Author:

Guneet S Paintal is a principal consultant with the Supply Chain Management (SCM) practice at Infosys Ltd.

## References

1. Online Fraud Rates Approaching Fraud Rates at Card-Present Retail According to 5th Annual Survey by Merchant Risk Council  
[http://www.merchantriskcouncil.org/press.php?p\\_press\\_id=24](http://www.merchantriskcouncil.org/press.php?p_press_id=24)
2. Merchants are Using More Tools More Effectively, to Combat Online Fraud, According to Annual Survey by the Merchant Risk Council  
[http://www.merchantriskcouncil.org/press.php?p\\_press\\_id=15](http://www.merchantriskcouncil.org/press.php?p_press_id=15)
3. UK Online Fraud Report 2005 Edition sponsored by CyberSource Ltd  
[www.the-logic-group.com/Downloads/UK\\_Fraud\\_%20Report\\_2005.pdf](http://www.the-logic-group.com/Downloads/UK_Fraud_%20Report_2005.pdf)
4. Order-Review Efficiency Rises for Online Sellers, But So Does Fraud  
<http://www.digitaltransactions.net/newsstory.cfm?newsid=1161>



For more information, contact [askus@infosys.com](mailto:askus@infosys.com)

### About Infosys

Many of the world's most successful organizations rely on Infosys to deliver measurable business value. Infosys provides business consulting, technology, engineering and outsourcing services to help clients in over 30 countries build tomorrow's enterprise.

For more information about Infosys (NASDAQ:INFY), visit [www.infosys.com](http://www.infosys.com).