FRAUD SCREENING — NOT IF, BUT WHEN
There’s usually more than one way to do something — and this is certainly true for business processes and payments. When deciding how best to process payment transactions, it’s important to make the decision that is right for the business, based on all available information — whether this relates to costs or benefits that can be accurately measured or other business key performance indicators that cannot be so precisely defined and assessed.

1. A QUESTION OF TIMING

While the merits of fraud screening are undoubted, and have been well documented, the decision facing a merchant is not just whether but at what point to introduce fraud screening during the transaction process.

The decision to apply screening before or after bank authorization will have implications for business processes, transaction fees and customer experience. Any move to adopt a different transaction flow process must first be carefully analyzed, as it may have significant financial and customer implications. As well as potential losses to fraud in each scenario, the decision must take into account all fees along the payment chain, ensuring the return on investment remains positive.

Today, ACI works with merchants who fraud screen both pre- and post-bank authorization. Both approaches have positive and negative implications. Factors that will influence the choice include transaction volume, average transaction value, product or service offering, and the sector(s) in which the merchant operates, as well as differences in banking and legal systems across the countries in which the merchant is active.

2. FRAUD SCREENING PRIOR TO BANK AUTHORIZATION

In this scenario, once the customer clicks to purchase, the transaction is screened using business rules and scoring and blacklists prior to bank authorization (whether a 3DS authentication request is carried out or not). Note here that the merchant is managing payment attempts, not confirmed sales. If the transaction is accepted by the fraud screening engine, the customer’s issuing bank may still decline the transaction. The customer is likely to make another attempt. However, if the transaction is declined by the fraud screening mechanism, then it does not go forward to the bank for authorization, delivering savings to the merchant on authorization fees and reversal/refund fees.

It is important to recognize that the merchant must actively manage the customer relationship where a decision to reject the transaction is being made by the fraud screening engine and not the issuing bank.

3. CUSTOMER PERCEPTIONS

There will inevitably be situations where a genuine cardholder will have a transaction denied (what the fraud industry refers to as a “false positive”). In these circumstances, a number of relationships
are involved but, from a merchant perspective, it is critical to protect the customer relationship and online experience. (In this respect, a refusal by the issuer can make life easier for the merchant than one for which he or she must take direct responsibility.) Where a transaction has been refused, whether by bank or merchant, only limited information should be provided to the customer as to why the attempt was not successful, in order to avoid revealing the business rules to fraudsters.

When a transaction is sent for bank authorization prior to the merchant’s fraud screening engine, this can have important implications for the merchant’s costs and reputation. One may ask why authorized orders need to be decisioned in the fraud screening engine, when CV2 and AVS checks will already have been completed and the issuing bank system will have used its own fraud prevention system to assess the risk of each transaction.

The value from a fraud perspective of screening transactions post-authorization is two-fold. First, the data received back from the issuing bank as part of the authorization process is helpful in making the transaction decision — and can make the difference between accepting an order and requiring the order to be challenged for review. More importantly, attempted authorizations can themselves be an indication of fraud — fraudsters commonly practice card testing that includes changing transaction attributes such as email. Collection of all the data from all points in the transaction lifecycle ultimately helps the merchant to better control fraud losses.

It is important to note here that if the issuing bank has authorized a transaction and the transaction is subsequently identified as fraudulent by the merchant or the fraud screening engine, a reversal is required through the acquirer. A transaction reversal not only has cost implications for the merchant. It also has implications for the customer since funds are blocked until the authorization expires or the issuer bank receives the reversal and unblocks the funds.

If settlement has already taken place, a full refund will need to be initiated which can sometimes take a few days to reach the customer’s bank account. As a result, it is essential for the merchant to act swiftly to reverse the authorization of a fraudulent transaction in order to avoid costly interchange fees.

When considering whether to screen pre- or post-authorization, a merchant will need to assess the operational impact of a new transaction flow, potential cost savings and the implications for customer relationships. In addition, the merchant must decide whether he/she prefers to manage confirmed or attempted sales. If, for example, the merchant operates a no-challenge policy — working on a straight accept/deny recommendation — there would be logic in handling fraud screening post bank authorization, when the precise value of the sales being denied is clear.

Ultimately, there is no “wrong” choice. As a general rule, a small merchant with low levels of fraud might find the lower fees attached to the pre-authorization option more attractive. By contrast, a merchant operating in an industry with higher levels of attempted fraud and higher transaction values might seek the more accurate fraud detection provided by better key performance indicators in the post-authorization scenario. Whatever the individual circumstances of the merchant, this is a decision that requires careful thought and planning.
ACI Worldwide®, the Universal Payments® (UP®) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI® to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI’s private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience.