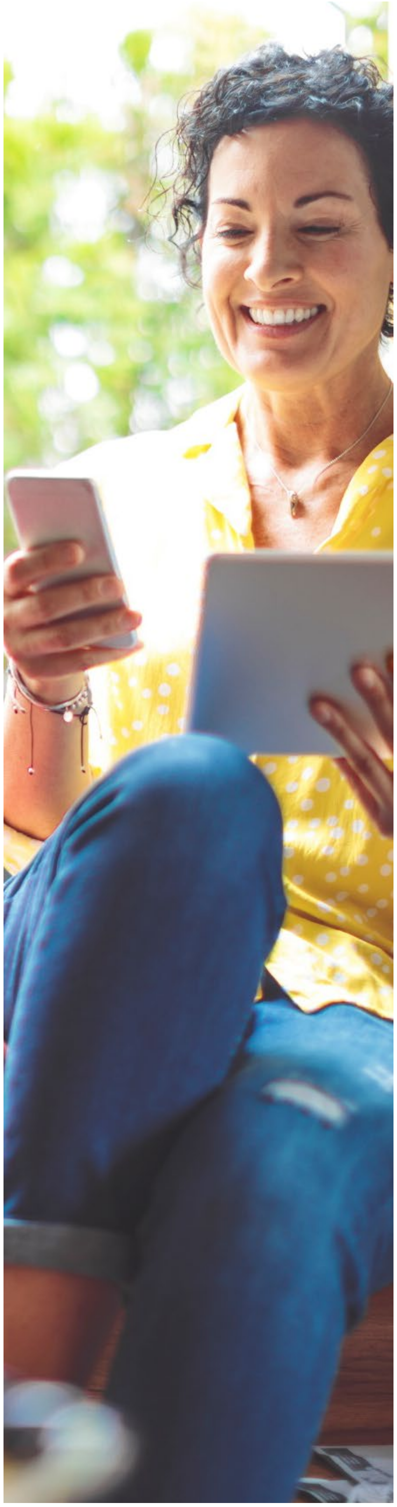
Risk Best Practice Guide
The Customer Challenge Process
A Merchant's Perspective

October 2019

VISA everywhere
you want to be

Contents



Purpose of this Guide

The purpose of this guide is to help your business address first party fraud with a number of recommendations that you may want to adopt to improve processes.

First party fraud cases (where it is known or there is a high suspicion that the genuine customer or a person known to them has carried out the transaction) have become more difficult to identify and manage successfully following the positioning by Regulators where some require an immediate credit to a customer account where fraud is claimed.

Yet there is an expectation that merchants and card issuers undertake a robust customer challenge process.

Identifying and acting upon such incidents maintains compliance with Anti Money Laundering regulations and could drive benefits to all stakeholders in the payments system.

Specifically for merchants it:

- Reduces costs of dispute management
- Reduces dispute volumes and associated fees
- Enhances customer satisfaction and increased transaction volumes

Introduction

If all types of businesses adopt a consistent approach, first party fraud can be marginalized. This guide is designed to recommend proven methodologies that are available for identifying and managing first party losses. It is not intended as a prescriptive "how to" instruction manual but rather a guide to give businesses some ideas as to the options they can consider when approaching this kind of risk. Each business will of course tailor their approach in line with appetite for both risk and customer experience.

Customer Engagement

Initial Contact:

What steps can a merchant take when a customer relationship is first established? As with all types of fraud prevention, initial engagement with a customer is key. If whatever information is collected up front turns out to be counterfeit or suspect and is not spotted at that stage, it becomes the foundation for that person's profile.

It is vital to collect sufficient data to understand who your customer is and recognize how they are interacting with your business. In this light, remember to make sure that your terms and conditions are clear on the data you are collecting and how you will use it, as per the data protection rules that apply to the transaction and your local/country/region laws.

Risk appetite is defined by a company's tolerance for fraud loss and customer experience expectations.

It should include a workable refund policy, subject to specific criteria and be sustainable.

Its implementation should be measured using quantifiable metrics and reporting.

Day-to-Day Management

It is recommended that regular contact be maintained with customers, which includes the following:

- A clear understanding of the products and services your business provides
- Advice notices when payments are being made and a clear merchant name is used that makes sense to your customer when they see it on their statement. The customer should have no sense of doubt as to who they have transacted with
- If you have third parties lodging account details for use by others, e.g. parent or child — set up alerts aimed at the parent's phone/account to confirm spend and set spend breaks. This can help prevent situations where a member of the customer's family, is making high volumes of repeat purchases that could become a future claim by that customer that they did not carry out or authorize those transactions. A simple check via SMS, email or through another form of communication around what has been bought and where it has been delivered to will alert a customer to potential abuse of their payment details
- It is vitally important that your payment page clearly states exactly what the customer has purchased and any items relating to what has been purchased and any that the customer has chosen to decline
- A complaints procedure must be communicated that is clearly visible to customers and easy to follow on how to seek redress if there is a problem

Managing Change

Changes to customer profiles are an everyday occurrence; however, they can also be a risk indicator. Monitoring changes will allow insight to preparatory actions designed to facilitate a future fraud or account takeover.

- Be sensitive to device ID changes where previous customer contact details, accessed using another device ID, are being altered. Double authentication when changes occur are strongly recommended. For ecommerce, the use of biometrics can be an option.
- If you believe there is fraud or an account takeover, don't clear transactions until you validate. If you process and then refund this is a suboptimal process and will both increase costs and the probability of error

Disputes

From an operational cost perspective, it may not be viable to investigate every dispute and as such, your business may want to consider a threshold below which immediate refunds are made. Rules for handling customer disputes need to be clearly defined and should be designed with the key aim of closing a case during first contact to avoid a chargeback scenario and the operational cost of any follow up calls.

It is recommended that calls be recorded and customers after discussion are always given the option to call back and withdraw their claim at any time hereafter.

Initial customer engagement concerning an unrecognized transaction should establish how and when it was carried out by providing additional information to differentiate between:

- A transaction the customer simply does not recognize
- A dispute where the customer has an established relationship with you;
  i.e. this customer has made a similar purchase with you in the past
- A fraudulent transaction

This is best accomplished by developing some simple scripting or question/answer combinations to drive the call/interaction based upon the transaction details available. Can more information be provided to enable recognition of the transaction and allow immediate closure of the claim? What does the statement narrative say, and could this be misinterpreted? Does the date and processing time of the transaction differ to that appearing on the customers' statement?

Then consider the following:

- Does the customer have a history of previous transactions?
- If so, what is different about this transaction to the previous one that has not been challenged?
- What other information do you have about the transaction? For example, has it been completed using the same device I.D. and IP address as previous ones?
- Could a third party have had access to the customer's payment details and completed the transaction on their behalf? E.g. the immediate family?
- Compare and challenge where appropriate, the customers' use of your mobile application and/or online account service to the time the fraud was reported; a log in and out of the application or online account during a month when transactions claimed to be fraud start at the beginning of the month would be highly suspicious.
- Was the disputed transaction completed in store and completed using Chip and PIN and the customer is claiming non-receipt of goods?

Considering all of these factors, does the transaction meet the criteria for refund? If not, what aspect of the transaction is being challenged?

Time now to make a decision:

- Does the customer's version of events make sense?
- Is the fraud claimed viable based upon what you have been told and on your own system data and metrics?
- Are you satisfied that the customer was not complicit in the transaction?
- Have you told the customer that all goods/access will be revoked, and have they agreed?
- Has the customer given you permission to report the fraud to law enforcement for prosecution?

✓ If the answer to all of the above is yes

You should consider refunding the transaction, revoking all goods and services provided under the fraud and take steps to prevent the fraudulent party from touching your systems again.

✗ If you answered no to any of the questions

You should consider rejecting the claim and explain to the customer why that is the case. However, this will need to be tempered by your own customer experience and support model. If you still choose to refund, you should consider all of the above re: revoking goods/services, exiting relationship, etc.

Based on your refund policy, customers should either be informed of an immediate refund, or that further investigation will be necessary before a decision is made. It is very important that this contact with a customer sets their expectations and it is critical that the call is closed leaving the customer in no doubt as to their position.

In the event that a refund is not going to be made, you may want to consider advising the customer that should a chargeback be received it will be challenged and all relevant information will be provided to the card issuer to defend that chargeback. We recommend that you ensure there is clear evidence retained of why a decline decision is made — it must be factual, impartial and should be clearly articulated, and potentially used as defense against a chargeback claim.

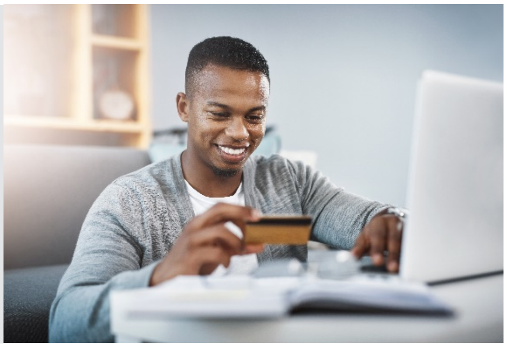
Some merchants choose to add the following disclaimer to any dispute defense "Please make the cardholder aware that should they continue to maintain that this transaction is fraudulent the details will be added to our high risk database. In accordance with (company name) terms and conditions agreed to at the time of the transaction, any future transactions will be at risk of cancellation".

Remember — providing compelling evidence to help defend a dispute is about proving to the issuer that the genuine cardholder was responsible for the transaction. It must be easily understandable to both the issuer and the cardholder and in a way that it proves culpability.

Other Things to Consider

The customer experience during a fraud claim is vital in terms of maintaining a good relationship; after all, if it is a genuine customer you will want to encourage further trade in the future. However, it is just as important not to present the business as a "soft touch", opening it up for increased and inflated claims.

The following things should be considered and the processes that need to be used or developed to facilitate smooth case handling to the benefit of both the business and its customers:



- Consistent application of a clear, easily audited policy will produce less variable outcomes and gives a clear basis for resolving any disputes
- Consider using a written statement in suspicious cases making it clear it may be used as evidence that fraud has been committed against the business and will be handed over to the police
- Handling serial victims/offenders; at what point does a customer move from being unlucky to becoming a first party fraudster? A customer needs to be treated accordingly and recognizing when a customer should be treated as a fraudster will go a long way to helping a merchant define appropriate communications, care and control reactions
- If your business operates a no refund policy ensure this is clearly stated within your terms and conditions and be prepared to challenge 'Credit Not Processed' or 'Merchandize Cancelled' disputes
- Always consider a policy for termination of a customer's account if you are satisfied that they are party to a fraud
- Consider developing a "watch" list for accounts where there is suspicion of first party fraud so all subsequent claims can be fully investigated in spite of other criteria
- Be aware of long-term regular customers processing claims directly with their card issuers without discussing the issue with your business first. Check recent transactions for anything that could indicate an error on their part that they may be trying to compensate for through the dispute system
- Always keep the customer/first-party fraudster appraised of the consequences of their claim whether successful or not. Loss of access to your services may be a major issue to them and they need to realize this is what will happen if you accept their fraud claim at their word
- Ensure you get TC40 confirmed fraud reports from your acquirer and use them to track fraud levels, whether subject to chargeback or not
- Once investigation of a transaction has concluded and you continue to have grounds for suspicion, advise your customers that if they maintain that the transaction is fraudulent you may refuse to transact with them in the future

Summary and Further Information

Clearly, a successful business has to take a certain amount of risk; the key to risk management is agreeing the risk appetite and strategies, policies and processes that underpin them.

The ongoing review and adjustment of those key elements is vital as fraud constantly evolves as the fraudsters look to keep ahead of the game.

Visa Merchant Purchase Inquiry

Visa Merchant Purchase Inquiry is a plug-in to Visa's globally used Visa Resolve Online (VROL) platform. Using Application Programming Interface (API) technology, this solution allows merchants the capability to provide additional data elements to issuers at the beginning of the dispute process in an attempt to prevent disputes from occurring. Using the Visa Merchant Purchase Inquiry plug-in can significantly help with reducing costs related to disputes for both merchants and issuers. It is considered by Visa to be a robust defense against first party fraud. For more information and VMPI and its implementation, please contact your acquirer.

Further Reading

Visa Best Practice Guides
(available from your Acquirer)

- Recurring Transactions
- Managing Fraud in the CNP Environment
- Digital Goods & Services Merchants

Visa Risk Tools
Visa provides a number of risk tools to help merchants manage fraud risk as shown below, and to obtain more information regarding risk tools, please contact your acquirer for more details.

- Visa Secure (3DSecure)
- Visa Transaction Adviser

A variety of risk merchant solutions are available through Cybersource (a wholly owned Visa subsidiary). For more information, please visit **www.cybersource.com.**

For further advice or information, please contact your Visa Account Manager.