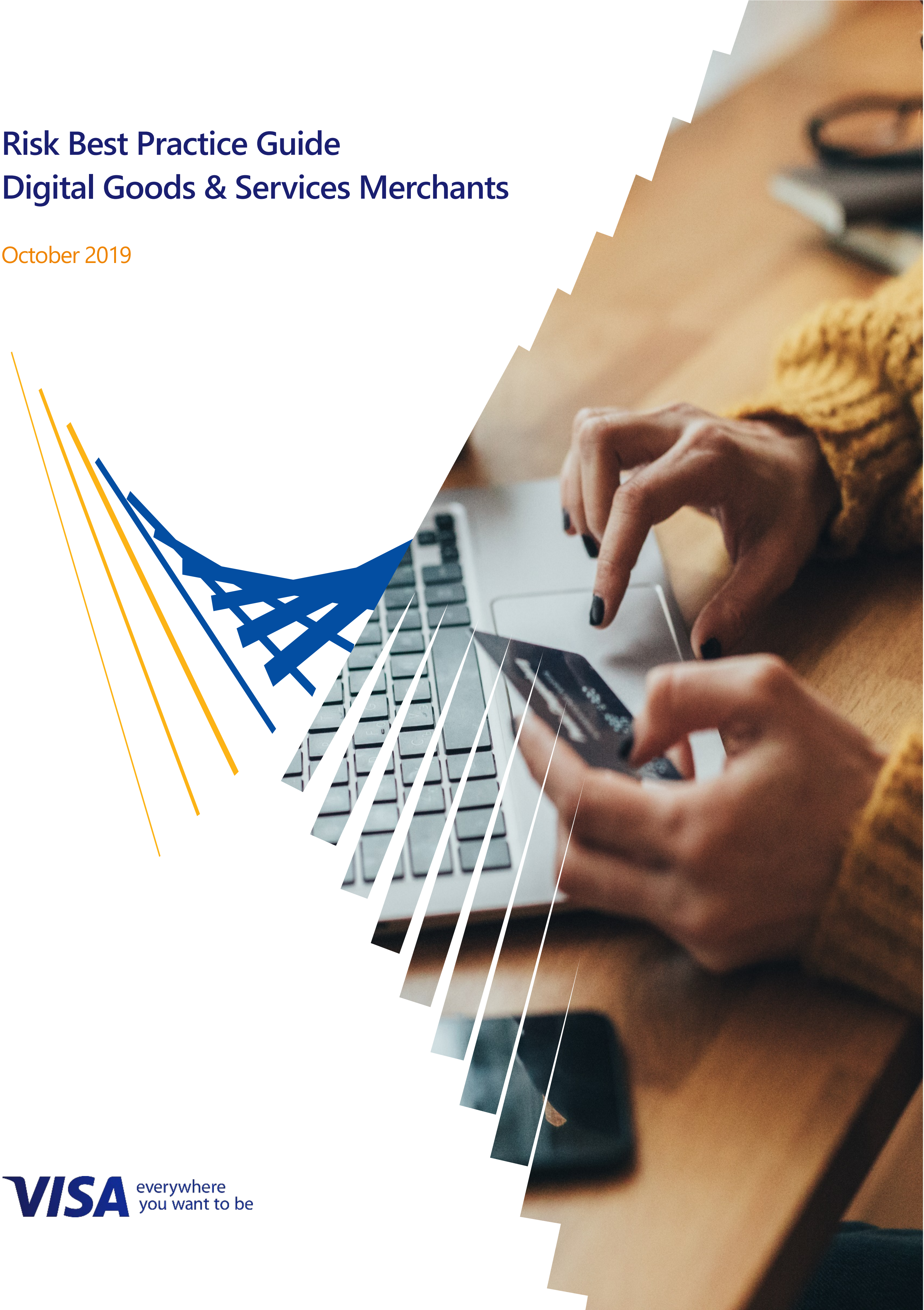
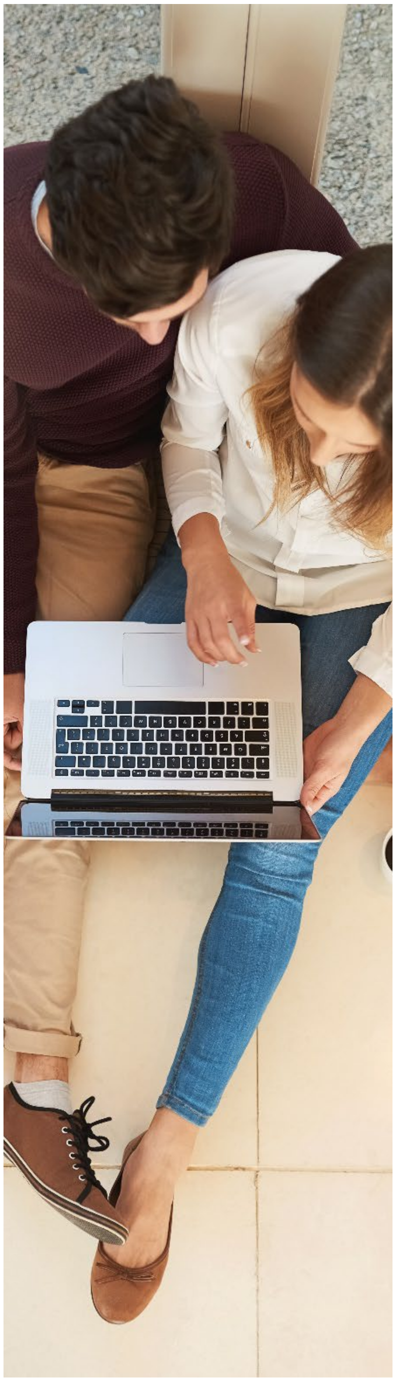
Risk Best Practice Guide
Digital Goods & Services Merchants

October 2019



VISA everywhere you want to be

Contents



Purpose of this Guide

This guide is for digital merchants (this includes but is not limited to providers of digital content, games etc. and merchants who sell goods using a digital sales model — airlines, hotels, railways etc.) to support how they manage and mitigate payment risks within their business when supplying digital goods or services. It covers policies, procedures and functionality currently in successful use by digital merchants today and recommendations based on Visa's global payment industry experience.

This guide is intended to operate as a valuable planning tool and fulfilment guide for merchants throughout any stage of the eCommerce life cycle. It is focused upon helping eCommerce merchants to maintain a secure infrastructure for payment card transactions. However, processing dynamics differ by country and geography and merchants should ensure that the capabilities and approach described here reflect their own risk appetites and operating models.

Introduction

Merchants offering digital goods or services will often offer multiple payment options through various providers. Diverse payment channels mean the job of managing risk is complex and proportionately harder to administer whilst, in the online environment, speed is of the essence giving little time to undertake risk assessment. For example, an order for a digital download typically requires immediate fulfilment if consumer demands and customer experience aspirations are to be satisfied. This leaves little opportunity for any form of manual review and therefore requires automated risk management technology to balance speed, efficiency and the identification and avoidance of fraud risk.

Criminals working in the online channel will target weak fraud controls, detection models and other risk mitigation offerings. A good place to start therefore is to ask whether your business is a likely target. Do you understand the scope of and reasons for a fraudster targeting your digital merchant business? Do you believe your controls are as robust as those of your competitors? Does your approach create exploitable weaknesses?

The following chapters highlight the risks from the online sales environment and gives some guidance on how risks can be mitigated or suppressed. The more you understand and recognize the different risks that arise from your business model and sales channel, the better you will be at fine-tuning your business policies, operational practices, fraud prevention tools and security controls.

Understanding the Risks

Fraud attacks against digital goods and services have a unique flavor that mark them out against attacks on physical goods. They are susceptible to automated attacks/bots (devices or software that execute commands, reply to messages or perform routine tasks) sometimes combined with mobile wallets which allow complex manipulations and high-volume activity, or payment orders.

There are Various Risks to be Managed, Some Obvious, Others with Greater Subtlety:

- Theft or misappropriation of digital goods/services — direct loss of digital assets
- Adverse Economic impacts upon digital environments — particularly game mechanics and in-game marketplaces leading to damaged experience or gameplay
- First party fraud — including buyer remorse, family fraud, etc.
- Account takeover — where an account relationship is taken over by a third party (which can be easily confused with first party fraud)
- Card testing — where a bad actor is using your merchant account to test card numbers, leading to use of bandwidth for no return and often creating issuer reactions which will damage wider approval rates
- Data compromise — the theft of card data (and other confidential customer information) — that can lead to customer compromise, fraud at other merchants, Public Relations issues as well as substantial fines

These risks, if crystalized, are likely to result in direct costs in terms of chargebacks, higher acquirer fees, scheme compliance fees, deterioration in authorization approval rates, regulator/legal costs and in some cases direct impact on the public perception of your business reputation and brand.

There are a host of other risk factors including; code manipulation, defacing of sites/assets and denial of service attacks. Whilst these fall outside of the scope of this document, due consideration should be given to them and adequate defenses put in place to mitigate.

Risk Mitigation and Fraud Prevention

To protect your business, you need to implement fraud detection and prevention measures within a reliable risk management system that supports robust consumer and device negative files with intelligent transaction controls that make sense for your business environment. You should recognize that data harvesting, processing and storage must, under the terms of Global Data Protection Regulations (GDPR) be only for legitimate reasons that may include asking the purchaser for direct consent. As such, Visa recommends obtaining legal advice in this respect.

Your organization should have a working knowledge of the risks that exist within payments and specifically the fraud and chargeback risks associated with digital trading as well as being well versed in risk management approach and appetite.

You can implement all of the controls you need to deter fraud, minimize customer disputes, and protect your site from hacker intrusions, but they will not necessarily prove fully effective without proper employee training and a clear and consistent risk methodology. Training your employees in digital business risk management particularly those operating, defining or supporting the sales functions allows them to act as your first line of defense.

Onboarding

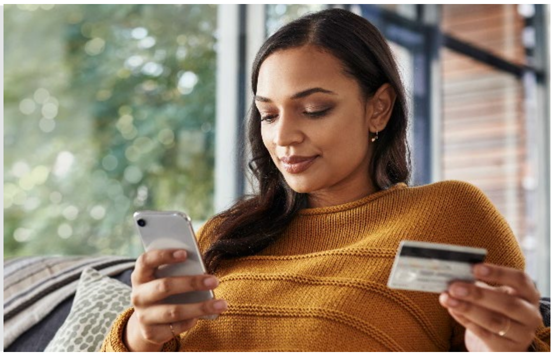
The customer onboarding process is likely to be the first point at which a fraud can be identified. If you do not have strong processes in place, you are opening the door to nefarious characters straightaway. There are numerous online services and manual checklists available to help take the risk out of onboarding checks; as a business, you need to decide what works best for you. At a minimum:

- Look to collect enough data to understand who your customer is and recognize how they are interacting with your business. Uniquely identifying relationships allows you the opportunity to understand whether they are attempting to appear as multiple customers to work around controls and allows you the option to exclude the customer from your services if you ever determine their intentions are malicious. 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.
- Statistical models can be used to recognize risk attributes in the application process and be part of any risk management approach.
- Much of the data required for new entity scoring will be available to you direct. But third-party data sources in real-time can provide a valuable uplift to help you correctly evaluate new business (email address validation, known bad devices or IP addresses, derived device data footprint and device data fingerprint et al. will all support improved risk capability).
- Evaluate where an applicant is using a disposable email address intended to drive anonymity, as these can be indicative of a poor consumer profile. These email services will have no billing relationships, and often no audit trail nor verification that a legitimate customer has opened the account.

- Validate IP location, or longitude and latitude coordinates where captured with the card issuance location and the billing address if available. Any mismatch may be entirely genuine, but will mostly indicate an increased potential risk, or at least an anomaly worthy of further investigation.
- Match data with that stored in your negative files (to prevent as far as possible bad actors who have previously attacked you through First Party Fraud and/or chargebacks returning).
- Employ a robust account registration and access process to ensure that secure authentication takes place for the first, or each unique, transaction on an account, and make it clear to the customer why you are doing this. The additional data entry slows down fraudsters and creates appropriate friction to high velocity use.

Deriving context from available data using as many data sources as appropriate will create more obstacles for fraudsters to navigate and overcome, but digital merchants should be mindful of striking a balance between risk management and inconvenience to the genuine customers. A small inconvenience to the customer at the start of the process provides layers of validation, verification and authentication that helps protect the relationship from account takeover.

> The sales arm of any business may dislike the introduction of potential consumer friction, but this perceived inconvenience is often considered by the consumer as a reassurance. A small inconvenience is offset by the time, effort and cost of recovering a relationship from an account takeover situation.



Transaction Fraud Detection

Today, there is a variety of fraud-screening technologies and best practices that can help you assess the risk of a transaction and give assurance that you are dealing with a legitimate customer. Fraud screening tools can be developed internally or acquired from third parties, and should include:

Detection Models:

You should look to deploy a statistically based/machine learning detection system to monitor risk in your environment potentially based upon scorecards, neural networks or similar. Necessary sophistication will be determined by the size and nature of your business. In the simplest form, statistical models can be developed and deployed quickly and efficiently. Some digital companies already have the skill sets to deploy an appropriate payment risk model (for example, pricing and behavioral models within online games often require similar skill sets) and whilst never trivial to deploy, do not need to be anywhere near as complex as is sometimes assumed.

If you are not quite ready to deploy a statistical model, then you can significantly reduce risk exposure by using transaction controls to identify high-risk behavior. These controls should consider your environment and will differ based on how and what you sell, but would typically include:

- An assessment of how customers move across your website, app and game — do the speed, order and actions look like normal behavior? If not, challenge the customer about what they are doing and why, and block usage if the answers do not tally with your records or are not forthcoming.
- An examination of concentration of use by country, IP, device, user ID and payment card — does this look reasonable behavior, do concentrations look realistic?
- Third party checks when taking orders from sponsored links and looking at whether the volumes are in line with expectations.
- Summarizing the value of spend being accumulated — is this going to be your best or your worst customer? Whilst there is a tendency to allow high velocity customer spend, a validation can be useful in helping a customer stay within their spending limit.

These types of controls help determine when an individual customer or transaction should be subject to greater control or scrutiny.

Customer Velocity Controls:

- Set review limits based on the number and value of transactions approved within a specified time. These limits should be set lower for new than those for long-term customers with a solid purchasing and payment track record. Adjust velocity limits as customers build a history with your business to fit either their individual profile or the average across your whole business.
- Ensure that velocity limits are checked across multiple characteristics including telephone number, email address and device profile.
- Modify transaction controls and velocity limits based upon the transaction risk. Vary transaction controls and volume, value and throughput limits to reflect your risk experience with selected products, download locations and customer purchasing patterns.
- If you operate a business model that allows your customers to undertake repeat transactions, employ a process whereby after a predetermined number of transactions or an aggregate that adds up to a predetermined value, you obtain an out of band authentication (e.g. an SMS text message) with your customer to verify the payment usage is still intended and good.
- If the person who loads a payment card or similar credential is likely to be different from the user of your goods/services — ensure that you provide advice to the cardholder not the user. This will allow expectations to be met and protect you against future claims that transactions were not authorized. Ideally, allow the cardholder to set limits based on their preference — with you as a merchant setting the maximums allowed.
- Always send the CVV2 value in the authorization message (unless it is a permitted Visa exception) and where available do an address verification. Where the response to an address and/or CVV2 data check is negative, do not complete the transaction and be aware of repeated attempts using incremental data this being a potential sign of an enumeration fraud attack.

Transaction Controls:

- 3DS2, fully supported by Visa and compliant with PSD2 regulations in Europe provides a means of Strong Customer Authentication and the opportunity to share far more information about the transaction with the card issuer that will enhance authentication decisioning and ultimately authorization approval rates.
- Behavioral Biometrics — block and/or detect bots or device manipulation by bad actors by monitoring navigation cues, time-on-page cues, noncustomary behavior and other activity that reveals a change in consumer interaction and cadence and/or nonhuman conduct. For the latter, a 'Captcha' or similar challenge/response process can be implemented.
- Orders can originate from a desktop, tablet, smartphone or other internet enabled device. Don't employ the same controls for all transactions, employ a multilayered approach employing screening technologies that are customized for the unique attributes of each channel to optimize results.
- Where you have deployed statistical detection models/machine learning technologies these will help you go beyond mere detection and prevention. They enable you to take it to the next level: predicting emerging fraud threats in limited information scenarios, such as first-time fraud.
- Record all key elements of confirmed fraudulent transactions such as: names, email and IP addresses, device ID's, customer identification numbers, encrypted passwords, telephone numbers, Visa card numbers used (being mindful of maintaining adherence to PCI Data Security Standards).

  Use this to establish and maintain an internal negative file. This valuable information should be used to protect you from fraud perpetrated by a person, persons or organized criminal groups that have previously committed fraud against your business.
- Monitor accounts for dormancy and consider employing a policy of revoking or reducing access to an account and (where applicable) refunding any unused assets to the customer. Dormant accounts are often maintained in preparation for a concerted future fraud attack.

Indicators of high-risk transactions will inevitably differ between business types, but often include:

⏱	Unusually large orders or multiple orders for identical or similar items for the same or different relationship profiles over a short period of time
VISA	Multiple transactions on the same card or from the same device or location in a short period of time, a potential sign that the criminal is maximizing the available funds until the account is blocked by the issuer
VISA	The use of multiple cards from the same purchaser could indicate testing through use of account generating software or a batch of compromised cards

The Transaction Review Process

Once a high-risk transaction is identified, it is very important to establish an effective response.

This could require an additional authentication based on previously loaded or behavioral data, a further validation via a customer mobile or email address, an additional issuer authentication via 3DSecure or similar or result in a referral to a member of staff for manual review. You should always look to deploy verification procedures that address both the need to identify fraud and the need to leave legitimate customers with a positive impression of your company.

Know what time your transactions settle and ensure all detection reviews occur before this time, as otherwise you will clear known bad transactions and are likely to see far more complex recovery controls and operational costs.

Set an effective threshold to determine which suspect transactions to review. The manual review of transactions is time consuming and costly, and in general only needed for higher risk transactions. However, this depends upon your risk performance and risk appetite.

Understanding Declines

It is important to understand why an issuer may make a decline decision. Whilst issuers differ in the declines they produce, typically the volume of declines (whether the decline codes indicate this to you or not) will fall in the following order (most common reason first).

Credit Risk ↓	• Has the customer got any money? • Are they overdrawn or over agreed/acceptable limit?
Card Status ↓	• Was a card with this number ever issued? • Is the card active? Does it have a fraud block? • Has the customer activated the card?
Wrong Details ↓	• What details have been input into the system? • What about other details? CVV2, 16 digit PAN, Expiry date?
IT Glitch ↓	• Micro outage • Could be on issuer, acquirer, processor, scheme
Fraud Check	• Detection processes

As a business, there are a number of things that need to be considered as to why you may be seeing high decline rates and what you can do to mitigate this:

Issue	Action
Are you in the right MCC?	Speak to your acquirer/PSP
Does your merchant name make sense?	If you trade as 'sPLot' and submit transactions as 'SUPERB PRODUCTS LO', expect disputes/fraud chargebacks
Are you sending the right data?	Expiry date, CVV2, MCC, consistent MID et al
Are you being used as a test merchant for purchased cards?	Allowing test transactions causes erratic issuer behavior. Some will just decline. Ensure controls are in place to detect testing
How much fraud are you taking?	What is your detection/uplift approach? Below 20 bps* you will tend towards optimal approvals Above 30 bps expect increasing declines Above 50 bps you can rely on a worse approval rate *Bps = basis points
Care re attempts policy	Too many attempts can create volatile issuer reaction and may in some cases be treated as a denial of services (DDOS) attack

There may be situations where you believe that a fraud claim has emanated from a transaction completed by your customer or a member of their family; and not a third party. This is commonly known as 'friendly fraud', or more accurately, First Party Fraud. There is essentially no consumer victim because the consumer or a person with actual or implied permission from the consumer completed the transaction. In any event, this should be considered a criminal offence whoever carried it out because of the misrepresentation involved.

To help merchants better manage and avoid being a victim of First Party Fraud, Visa has developed another best practice guide on this subject which should be read in conjunction with this and the others referred to at the end of this document.

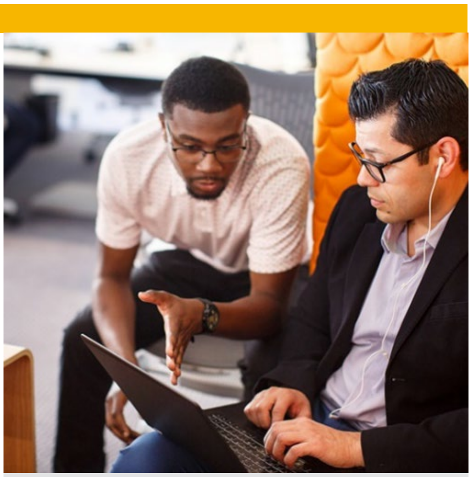
Dealing with Disputes

For your business, a dispute translates into extra processing time and cost, a narrower profit margin for the sale, and possibly a loss of revenue. Inevitably, at some point, customers will have a query about a transaction, this could be because they do not recognize it on their statement or they have an issue with the goods or services provided.

For example, a merchant that acts in its own right but also provides on behalf of services needs to be very clear whom they are processing for and the services provided so there is no doubt in the cardholders mind what a charge to their account is related to.

Check with your acquirer that the data that goes to the card issuers leaves no element of doubt as to what business it has come from.

To minimize losses, implement an adequate chargeback tracking system, have procedures in place to avoid unnecessary chargebacks, and develop a thorough understanding of representment rights. Visa highly recommends implementation of its Visa Merchant Purchase Inquiry (VMPI) product, Visa Merchant Purchase Inquiry is a plugin to the 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 and potentially resulting in the more commonly known 'chargeback'.



Using the Visa Merchant Purchase Inquiry plugin can significantly help with reducing costs related to disputes for both merchants and issuers. Contact your acquirer for more information in this respect.

Where you are satisfied that fraud is either conducted by your customer (first party) or that your customer has attempted to use stolen payment details to purchase from you, then measures should be taken to stop the goods/services provided. Where possible an attempt should be made to recover funds from the individual who took the service. Implement a policy to terminate a customer relationship, withdrawing the digital assets/services provided on evidence of fraud, and not allow that customer to become a serial offender.

Care should be taken however, to recognize where you offer an ongoing service that a third party has not circumvented your own account relationship (Account Takeover) where the genuine customer may be correctly confirming that the he/she did not complete the transaction because the account relationship has been taken over by a third party.

Merchants offering an ongoing account relationship with stored payment credentials should be very alert to account takeover attempts and ensure that account takeover is managed differently as it is possible to destroy a relationship with a good customer and incur significant costs to no effect.

More details on handling disputes can be found in the materials referenced at the end of this document as well as details of onboarding customers and how to obtain fraud data from your acquirer if your business does not already receive it.

Some Wider Hygiene Factors to Consider

- Systems Security — Review PCI DSS security requirements to ensure web application compliance and security around authentication, web session management, and security procedures. PCI DSS Version 3.2.1 (May 2018) provides guidance to secure web applications against threats and vulnerabilities and to prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens
- Establish ways to assist customers who forget their passwords, but always look to use two-factor authentication and as far as possible avoid use of static data
- Provide instant feedback to Internet customers when their required data fields are incorrect or incomplete, such as clear syntax or logical construct errors.
- Clearly publicize on your merchant statement narrative, within apps (especially at the point of purchase), on customer facing web pages et al contact details for customer queries and your refund policy
- Use browser cookies (with the appropriate customer consent or due legal reason to comply with GDPR regulations) or similar to maintain active user sessions, but once a session expires, request that the user log in again, regardless of the computer being used
- If the issuer approves a transaction, send an email order confirmation. This practice enables you to check the validity of the customer's email address. If the email address is invalid, research the situation to determine if it is a legitimate order. You can also minimize customer disputes by sending an email confirmation that reminds the customer of the approved purchase and provides details about it
- If declined, your procedures should specify how to handle the situation with the customer, such as obtaining corrected information, obtaining other means of payment or cancelling the order. Explain the consequences of failing to make appropriate payment
- Track decline rates to determine improving and deteriorating trends to allow you to determine if action is required. If you only receive generic decline codes, contact your acquirer and request they provide the full responses provided by issuer. Whilst not perfect, it will allow you to better manage the transaction and your customer interface and at the same time potentially boost acceptance rates.

Management Information and Key Performance Indicators

Robust management information (MI) combining current performance and trends should be critical to everything you do. Without regular up to date MI showing the core trends in fraud performance you will be working in the dark. For more details and guidance, refer to Visa's guide to managing fraud in the CNP environment.

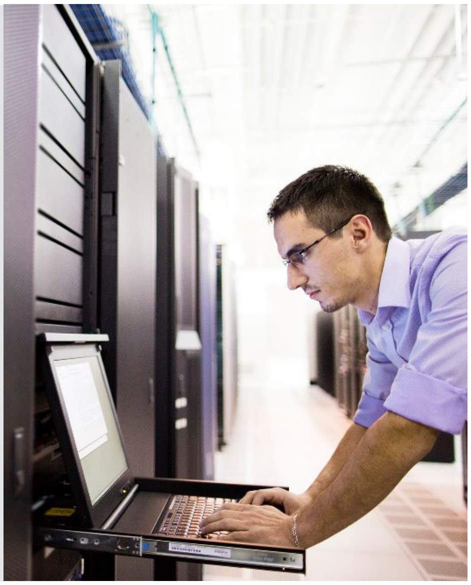
Protect Your Merchant Account from Intrusion

Unauthorized persons are gaining entry to merchant accounts via shopping carts or payment gateway processor systems. These intruders are attacking digital merchants using weak or generic passwords. Once compromised, intruders then emulate the merchant and begin processing transactions, without the true merchant's knowledge.

- Ensure integrity of your systems and connections to payment gateway service providers
- Have effective logging of all user activity to alert of possible fraud scenarios
- Choose a payment gateway that supports a multifactor authentication
- Ensure passwords are appropriately robust and changed frequently
- Enroll for real time alerts provided by payment gateways
- Ensure security of endpoints by maintain up to date patches released and virus/malware controls to any machine used to access your payment gateway

Merchants should ensure risk governance over their service providers by maintaining a strong technology risk management processes. They should ensure that their suppliers have a risk mitigated and compliant infrastructure in line with applicable standards such as PCI-DSS. *see page 10*

Merchants must refer to Visa security guidance as published on the website. **visaeurope.com/receiving-payments/security/**



Visa Services and Solutions

Visa can provide services and solutions that will enhance your risk management capabilities, these include:

3DS 2.0 is a fundamental upgrade of the global standard for card authentication. The benefits it brings include:

- Use of Risk Based Authentication utilizing a significantly increased number of transaction and customer data elements to securely authenticate the majority of transactions without the need for the customer to complete a challenge. This is known as frictionless authentication.
- Full compatibility with mobile and native app environments allowing mobile browser and in-app transactions to be authenticated through a seamless user experience, even when a challenge is required.
- Integration with the merchant checkout user experience, including merchant branding options to further ensure a seamless customer journey
- Compliance with the PSD 2 regulations.

Visa Transaction Advisor is a solution for merchants, gateways or acquirers to identify low risk transactions; risk intelligence delivered in real time before authorization to determine if SCA exemptions apply. Available through 3DS 2.0 or an API.

Cardinal Consumer Authentication enables rules-based authentication solutions for merchants prior to authorization; merchants can create customized, adjustable rules

Visa Tokenization Services is a complete, integrated set of tokenization tools: Visa Token Vault, Token Management and Visa Risk Manager

Visa Merchant Data Secure is a point to point encryption services for acquirers and merchants

Visa Merchant Purchase Inquiry (VMPI) is a plug in tool that allows merchants to have a system to system interface with issuers who are reviewing a cardholder's claim; and prevents disputes escalating to chargeback

Cybersource

Decision Manager is a risk scoring and rules based engine that enables merchants to detect fraud in real time, recommend and test rules as well as manage suspicious cases.

Risk Management Services is a performance improvement, customized fraud rule configuration within Decision Manager on a one time or continual basis. Screening management providing deeper, manual reviews of subset of risky transactions through Case Management portal in Decision Manager

Token Management System is a service for merchants to manage various network, acquirer and proprietory token schemes for merchants, both digital and POS

Account Takeover Protection is a service that helps merchants identify high risk users at account creation and login, and monitors for suspicious account changes for card on file customers.

Contact your Visa representative
for more information on the above.
In addition, you may choose to contact your acquirer who may be able to offer alternative or additional services.

Closing Thoughts

If you choose to outsource your risk management, there are plenty of systems and services available. However, Visa strongly recommends getting legal advice regarding any contract with a third-party supplier, especially in respect of liability for losses.

The migration of payments from the physical to the online world continues at a pace. Criminals will always attempt to profit through the exploitation of weaknesses in the payments ecosystem. They are effective at identifying merchant businesses with a strong defense and those that offer attack vector opportunities.

As such, the merchants with vulnerable security systems and processes will bear a higher proportion of overall fraud loss, poorer approval rates, higher costs and increased customer experience issues. An investment in risk control is very much an investment in the continuing success of your business.

Further Reading

This guide provides a broad range of best practices for consideration by all merchants providing digital goods and services and should be read in conjunction with the other Visa publications detailed below;

Visa Best Practice Guides
(available from your Acquirer)

- Managing Fraud in the CNP Environment
- First Party Fraud — The Merchant Perspective
- Recurring Transactions

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

- Verified by Visa (3DSecure)
- Visa Merchant Purchase Inquiry
- Visa Transaction Adviser

A variety of risk merchant solutions are available through Cybersource (a wholly owned Visa subsidiary) and can provide further information about the services and solutions available if this would be of interest, please visit www.cybersource.com.

For any other information, please contact **fraudmanagement@visa.com.**

These materials and best practice recommendations are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Recommendations should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of the materials, best practice recommendations, or other information, including errors of any kind, contained in this document.