Microsoft

Online Transaction Risk Management Guide

Last updated: July 2023

Disclaimer:

As a Microsoft partner in the Cloud Solution Provider (CSP) program, you're responsible for your customers' purchases and use of our services.

It's important that partners monitor and address anomalous activities from their customers.

Microsoft may send partners notifications if we detect suspicious activities, but it's critical that partners use additional methods of monitoring to help detect anomalous customers' behavior.

Online risk management

- Introduction
- Onboarding customers best practices
- Customer post purchase best practices
- Microsoft notifications

Introduction

Microsoft takes online transaction risk management seriously and partners should do the same to mitigate business risks.

To support partners, Microsoft is sharing a set of recommendations to manage risks when working with customers online.

While Microsoft is committed to supporting partners, partners remain financially responsible for fraudulent purchases by their customers and/or customers' non-payment of purchased services.

Online risk management basics

Risk exposure to be mitigated

- **"Abuse of Service":** Customers or bad actors who use cloud services in violation of Microsoft's Acceptable Use Policy.
- **"Theft of Service":** Customers who demonstrate they have no intention to pay for consumed services, use stolen payment instruments, provide false billing information, and/or default on outstanding balances.

Examples of possible service abuse

- Spamming
- Hacking
- DDOS attacks
- Crypto-mining
- Malware distribution
- Pirated subscriptions resale

Examples of theft of service*

- Transactions that don't occur in person.
- Misrepresented identities.
- Services provisioned and used with no intention of payment.
- Automated account creation and purchasing by bad actors.

**Theft of service may be higher in emerging markets/high risk regions.*

Online risk management best practices

Microsoft recommends partners implement the following throughout the lifecycle of the customer relationship

Onboard new customers

- Establish personal relationships with customers, when possible (for example, contact by phone).
- Look for better ways to verify customers' credentials and background (Credit Bureaus/ Business Commercial Report Agencies).
- Use multi-factor authentication (MFA) during sign-up to minimize exposure to robotic account creation and purchasing.
- Require customers to monitor and secure their tenants by following security best practices.
- Manage and track identities using services such as digital identity services.
- Assess customer financial strength through rigorous credit card fraud detection systems.
- Establish a clear collections policy. Detail collections processes and when access to subscriptions will be affected by nonpayment.

Manage customers accounts

- Implement a process to quickly receive, review, act on, and respond to Microsoft notifications.
- Work with customers to understand their cloud usage business needs and set appropriate monitoring thresholds. (For example, partners can set a monthly Azure spending budget in Partner Center.
- Monitor customer activity logs regularly to help detect fraud early.
- Take quick action when suspicious activities are detected.
- Avoid giving customers full administrative access to subscriptions without first implementing risk mitigation controls.

Manage customer billing

- Request prepayment prior to initial transactions and billing.
- Don't accept high-risk payment instruments (such as pre-paid cards or stored-value cards).
- Monitor customer payments and aging accounts receivables. Aggressively enforce standardized dunning processes for late payments or nonpayment.

Suggestions for customer onboarding best practices

SMS (Text) verification

During the sign-up process end customers are presented with a “Proof that you are not a robot” page which initiates a customer verification via SMS (Text).

Using an SMS verification solution helps partners mitigate the risk of customer sign-ups occurring via robotic methods and/or bad actors being able to easily create multiple accounts (for example, fake sign-ups)

During the sign-up process, partners may choose to confirm a person is on the other end of the transaction by requiring the customer to provide a mobile number to which a one-time passcode will be sent via SMS

Additionally, SMS verification can also be used as part of a multi-factor authentication (MFA) sign-in process for established customers

End user identity management

Here are best practices to mitigate the risk of identify fraud

One way to manage and track a customer's identity is by using a Digital Identity Service

A digital identity is a unique signature of an individual user and/or device at the other end of an online transaction

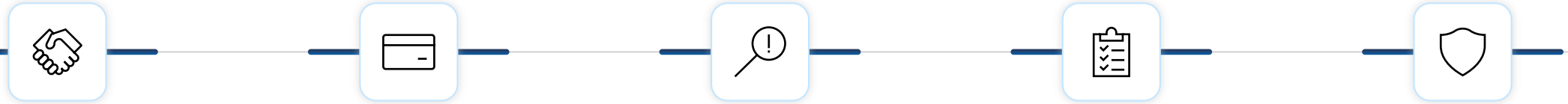
Digital Identity Services allow partners to better identify customers beyond simple identifiers such as an email address, physical address, etc.

Using third-party tools, partners can validate the identity of customers and identify potential bad actors

Know your customer

It is important that partners take additional steps to verify the identity and financial strength, when possible, of individuals and companies that want to purchase online services.

Best practices are



Build personal relationships with customers, for example: contact by phone, meet in-person, etc.

Require a credit card during sign-up; do not accept stored-valued cards or pre-paid credit cards as a payment method

Implement rigorous credit card fraud detection systems to ensure the customer presenting the payment instrument is an authorized user

Review financial reports from credit bureaus

Validate customers' credentials and background in trusted places like Business Commercial Report Agencies, etc.

Suggestions for customer post purchase best practices

Know your customer

It is the best practice to implement usage monitoring for services even if those services are not billed by consumption, especially for consumption billed service such as Azure where billing occurs after usage.

- Building on the “know your customer” strategy, partners should work closely with customers to understand the fundamental business needs of their cloud services usage.
- Avoid giving customers full admin access to subscriptions without first implementing risk mitigation controls, such as the best practices in this guide.
- Use the Microsoft Azure Management Portal and available usage reporting to monitor customer-level usage for the various business needs of the customer.
- Subscribe to new security alerts which is one of the many ways Microsoft supports partners in securing their customers' tenants. Alerts should be investigated and remediated quickly. If necessary, partners can suspend affected Azure resources or Azure subscriptions to mitigate an issue.

Billing

In the Cloud Solution Provider program, Microsoft does not bill the end-customer. The partner is required to set up and process billing.

Partners should implement the following in their billing process

Secure payment(s) upfront in advance of billing by requesting customers submit pre-payments to fund their account activity

Avoid accepting high-risk payment instruments such as pre-paid or stored-value cards as the amount on the cards cannot be verified and may not be enough to cover customer purchase costs

Closely monitor customer payments and aging accounts receivable, aggressively enforce standardized dunning processes for late or non-payment, including suspension of subscriptions and services until payments on outstanding balances are received

Microsoft notifications

Microsoft notifications

Microsoft has implemented a notification service and it is crucial that partners keep email addresses associated with subscription administrators regularly updated.

- Partners should develop and implement processes to quickly receive, review, act on and respond to Microsoft notifications as necessary

- If Microsoft detects unusual activity, Microsoft will send notifications to partners in the following scenarios:
  - When subscriptions are suspected of or determined to be violating the Acceptable Use Policy for Online Services, and/or;
  - When subscriptions are associated with suspicious activity (such as fraud/piracy) and pose an immediate risk to Microsoft, partners, and/or customers

- Customers notifications will be sent in the Azure portal via Azure Service Health blade. Learn how to set up alerts here

- General Abuse email notifications: Emails will be sent from azsafety@microsoft.com to subscription admins and owners: Add this email to your safe sender list

Partners should use additional methods to detect anomalous usage and suspicious activities and not rely solely on Microsoft notifications.

Acceptable Use Policy enforcement

- As part of their agreement with Microsoft, partners and their customer are expected to comply with the Acceptable Use Policy as set forth in the Online Services Terms.
- When Microsoft detects or is otherwise made aware of partner or customer activity that we confirm or otherwise suspect violates the Acceptable Use Policy, we will take enforcement steps.
- Violation(s) of the Acceptable Use Policy may result in suspension of Online Services – suspension may be immediate, if required, otherwise we will notify partners requesting action be taken and/or of enforcement actions already taken by Microsoft.

Notifications and expected actions

Microsoft will make reasonable efforts to notify partners if a subscription associated with their customer is showing risky or suspicious activities.*

Partners should evaluate customers who are found to be in violation of the Acceptable Use Policy to determine if they pose any additional risks to their business.

Risk event	Notifications and/or expected actions**
Activities which poses an immediate risk to Microsoft, partners, and/or customers	• Microsoft will **NOTIFY partner via Azure portal or Partner Center portal** of the high-risk subscription • Partner must **INVESTIGATE** and **SUSPEND** all other customer subscriptions of the customer account if it is determined by the partner to be **fraudulent** • Microsoft may **DISABLE high-risk** subscriptions immediately***
Ongoing suspicious security activities	• While is the partner's responsibility to implement and maintain fraud prevention and detection risk controls, Microsoft may NOTIFY partner, via email, of the suspicious activity • Microsoft may **DISABLE high-risk** subscriptions if no action is taken by the partner • In the future, Microsoft may offer additional tools and/or detection capabilities for partners
Violation of Acceptable use policy	• Microsoft will **NOTIFY partner via email** of the violation • Partner will **SUSPEND the offending asset and respond** to Microsoft's notification within 48 hours or the next business day • Microsoft may **DISABLE high-risk** subscriptions if no action is taken by the partner

*Partners should not rely exclusively on Microsoft notifications but use additional methods of monitoring to detect anomalous customers' behavior.

**Email notifications will be sent to the listed administrators of the subscription. Partners should ensure that email contact information is updated regularly.

***Certain violations may result in immediate suspension and/or disablement of the offending subscription.

When partners detect suspicious usage

- Partners are financially responsible for fraudulent purchases by their customers and/or customers' non-payment of purchased services; therefore, they should implement fraud prevention and detection risk mitigation controls such as the suggestions outlined in this Online Transaction Management Guide.

- If a partner proactively detects suspicious activity, they should immediately investigate and take appropriate actions to mitigate risk
  - Investigation may include reviewing the customer's account log-in activity, invoice payment history, frequent changes in payment instruments and/or previous subscription usage patterns, as suggested as best practices previously.
  - Mitigation actions may include remediation of compromised identities, cleanup of compromised resources and strengthening of security posture (read more).

- Partners can also submit a Service Request via Partner Center if they have additional questions or concerns about suspicious activity.

Microsoft