

Geo-Blocking Compliance



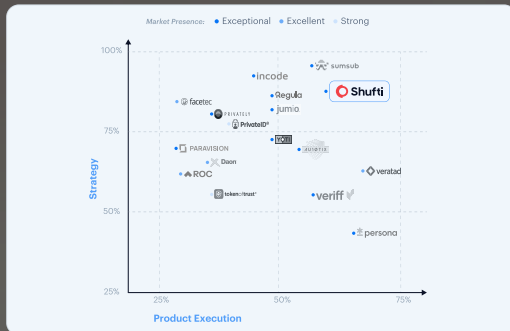
**Blocking Access From Sanctioned and
Restricted Locations**

Industry Recognition 2025–2026

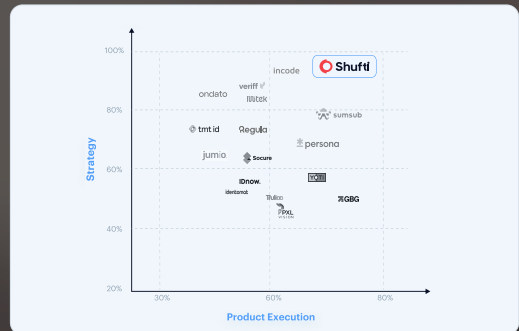
Recognised by leading analyst firms, government bodies and independent research organisations



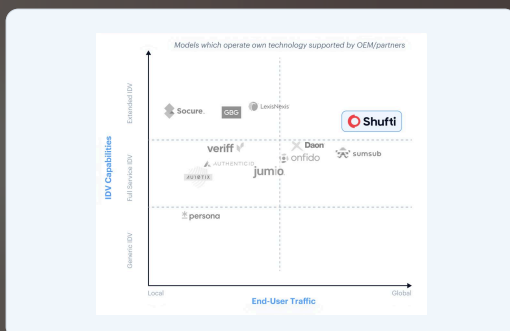
Ranked Exceptional in Liminal's 2026 Age Estimation Index



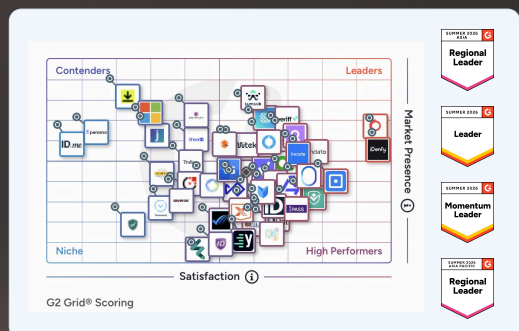
Ranked Exceptional in Liminal's 2026 Age Verification Index



Broadest global reach in the 2025 KuppingerCole Extended IDV report



Recognised as a Leader across four G2 Summer 2026 reports



Differentiated by Gartner on document diversity and country coverage



240+ Countries & Territories

10k+ Document Types

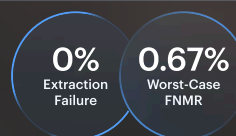


First EU company to achieve iBeta Level 3 Conformance to ISO/IEC 30107-3, with 0% APCR

iBeta Level 3 Conformance
0% APCR



Ranked Top 5 in the DHS RIVR 2025 for identity validation



KJM AGE VERIFICATION



PCI DSS



iBeta L3



ISO 27001:2022



CE+



QG GDPR



SOC2



GDPR



CCPA

What is inside this guide

—	Introduction	03
1	What is geo-blocking compliance?	04
2	Why can't sanctions screening and payment screening cover geo-blocking and how these run together?	06
3	How often does the network location disagree with the document origin?	08
4	How often does the same identity appear in two locations at once?	11
5	What do regulators actually expect?	13
6	How do geo-blocking controls fail?	17
7	What should a defensible location-control programme contain?	20
8	What evidence should you be able to retrieve?	22
9	How Shufti supports geo-blocking compliance	25
—	FAQ	28
—	References	29

INTRODUCTION

Geo-Blocking Compliance: What Regulators Expect and Why Controls Fail

In March 2026, OFAC announced [a USD 1.11 million settlement with TradeStation Securities](#) after failures in its geo-blocking controls allowed customers in then-restricted jurisdictions to execute 481 trades. The lesson for geo-blocking compliance from this enforcement case is clearly that presence of a control does not prove that it works. You need to know whose location it measures, what decision it makes and how you will detect a failure.

This guide is specifically written to answer those questions for compliance, product and engineering teams evaluating their options for different location controls. It draws on US sanctions guidance, EU territorial sanctions and EU MiCA guidance. Your applicable restrictions depend on the legal entity, service, customer and activity involved.

USD 1.11m

Settlement OFAC announced with TradeStation Securities in March 2026.

481

Trades executed by customers in then-restricted jurisdictions.

¹ OFAC, settlement with TradeStation Securities. ofac.treasury.gov/media/935351/download

SECTION 01

What is geo-blocking compliance?



Geo-blocking, also written as geo blocking, restricts access to a platform or service using geographic information. In a compliance programme, it applies the firm's rules for restricted locations and records how those rules were enforced. The applicable legal restrictions determine which customers, services and activities the control must cover.

A firm may need location controls for three reasons:



Sanctions

to prevent activity prohibited under applicable sanctions, taking account of relevant exemptions and authorisations.



Licensing

to keep regulated services within the markets and activities the firm is permitted to serve.



Product restrictions

to restrict a particular service or instrument in an otherwise supported market.

Start with a policy approved for your entity and products. Record which countries or regions are restricted, which actions are affected, the legal or business basis, any authorised exceptions, and who maintains each rule. A geolocation provider's default country list cannot answer those questions for you and can't make you compliant without customizing them as per your own requirements.

SECTION 02

Why can't sanctions screening and payment screening cover geo-blocking and how these run together?

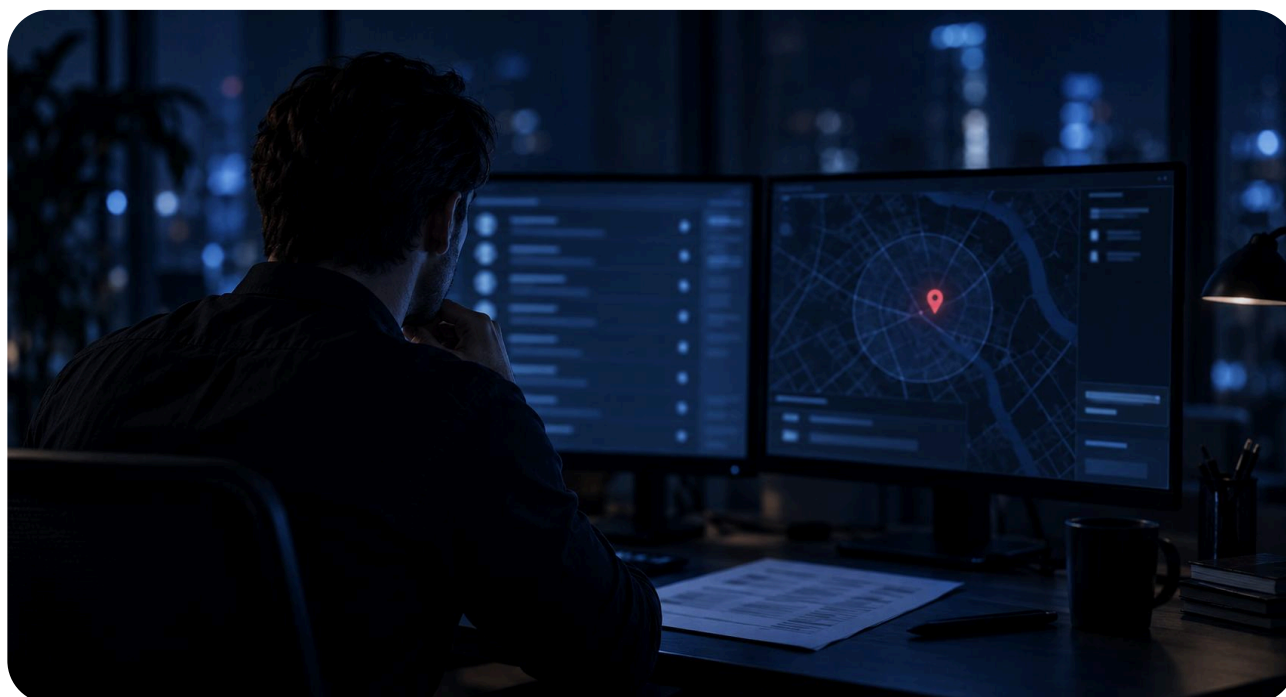
Sanctions screening answers questions about whether a person's name appears in any sanctions list whereas payment screening looks for mention of any restricted location in details accompanying a transaction. But both do not answer where a person is physically present at the time of using or accessing a service. You need to ensure all of these controls work simultaneously for comprehensive compliance with applicable regulations.

To prevent access/use of your products/services from a prohibited or restricted location, establish physical presence using IP, device location, GPS, Wi-Fi positioning and cellular or other network signals where available and appropriate. These checks may run at onboarding, login or transaction initiation, depending on the service and applicable restriction.

For an incoming or outgoing payment, assess the parties and the transaction's geographic connections. Relevant data that can be used for that purpose may include originator and beneficiary details, addresses, account or IBAN information, bank identifiers, intermediaries, the payment route or channel and payment purpose. An incoming payment may have no customer device session. An IBAN's country code² identifies the account jurisdiction; it does not establish the beneficiary's current physical location.

A customer may pass a name check while accessing a service from a prohibited location. Conversely, a customer in a permitted location may send a payment involving a restricted beneficiary, bank or destination. Apply the relevant restrictions and authorisations to each decision: permission to access the service does not clear the payment.

Connect sanctions and AML screening³ with customer-location checks and payment controls through named owners, shared escalation rules and linked decision records.



² Swift, IBAN resource. swift.com/swift-resource/9606/download

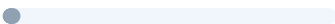
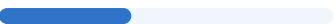
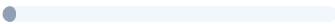
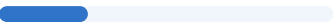
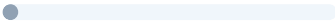
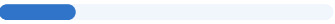
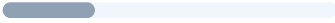
³ Shufti, AML screening. shuftipro.com/aml-screening/

SECTION 03

How often does the network location disagree with the document origin?



In Shufti's analysed sample, VPN or proxy sessions had higher rates of disagreement between network country and document-issuing country than the traffic where no VPN or proxy was being used, across all four sectors shown below.

SECTOR	STANDARD TRAFFIC MISMATCH	VPN OR PROXY MISMATCH	MISMATCH-RATE RATIO
Forex	5.40% 	39.57% 	7.33×
Payments	4.06% 	26.61% 	6.55×
Gaming	4.71% 	22.98% 	4.88×
Crypto	27.65% 	77.00% 	2.78×

Methodology: Shufti analysis of a sample of over 4 million onsite identity-verification sessions between 1 January to 31 August 2026. "VPN or proxy" refers to connections classified in those categories; datacentre and hosting traffic is counted as standard traffic. The mismatch calculation includes sessions with both network country and document-issuing country available. Server-side API integrations were excluded from this analysis. Ratios divide the displayed VPN/proxy mismatch rate by the standard-traffic rate and are rounded.

7.33x

FOREX · VPN OR PROXY MISMATCH RATE RATIO

Forex sector showed the largest relative difference between standard and masked traffic. VPN or proxy traffic accounted for 0.63% of all forex sessions in the sample, but when a forex session arrived over VPN it was 7.33x more likely to mismatch network and document country than standard traffic. Whereas the crypto had an overall high mismatch rate, more than a quarter of standard sessions differed from document- issuing countries. Higher use of VPN/proxy in the crypto sector aligns with overall use of anonymity techniques in crypto due to ambiguity around its legal status in many jurisdictions and privacy concerns.

Note: A country mismatch can reflect legitimate travel or residence abroad. Use it to trigger a location check where relevant to the service by establishing where a customer is accessing the platform and applying the policy for that location.

SECTION 04

How often does the same identity appear in two locations at once?

Shufti conducted an analysis of linked authentication attempts from two different locations between a certain timeframe. 1.563% of all pairs linked through this analysis found authentication attempts from two different locations that would require a travel faster than 900 km/h. A 2021 OFAC guidance for crypto ⁴ industry refers to such behavior as improbable logins.

1.563%

of linked pairs showed attempts from two locations requiring travel faster than 900 km/h.

4.33×

Flagged pairs were 4.33 times as likely to involve a VPN or proxy as unflagged pairs.

Those flagged pairs were 4.33 times as likely to involve a VPN or proxy as unflagged pairs. A change in network exit point can produce apparent movement without physical travel. So this is a signal to investigate further, not a conclusion.

⁴ OFAC, Sanctions compliance guidance for the virtual currency industry (2021). ofac.treasury.gov/media/913571/download

The analysis links sessions using a derived device profile. Unrelated users, though extremely rare, can share that profile, known as fingerprint collision, so check the linkage against authenticated account information when investigating an alert.

Investigate the apparent movement using account information, fresh location evidence and session history before deciding whether to restrict access.

Methodology: Shufti analysis of a sample of over 4 million onsite identity-verification sessions between 1 January to 31 August 2026. The reported travel metric is calculated on linked authentication pairs using a minimum 30-minute time interval across attempts to reduce concurrent retries. Device-profile collisions and network geolocation errors can affect results.



SECTION 05

What do regulators actually expect?



5.1 · OFAC

OFAC Compliance: a risk-based sanctions programme

OFAC's 2021 virtual-currency guidance⁴ recommends geolocation and IP-blocking controls to prevent persons located in comprehensively sanctioned jurisdictions from accessing their platform, with authorisations and exemptions taken into account. Its geolocation discussion specifically names screening against known VPN IP addresses and identifying improbable logins.

It also recommends using relevant information already held, including customer and counterparty addresses, invoices and transaction details, and collecting customer information throughout the relationship. Compliance with this specific guidance requires payment/transaction screening controls.

Businesses should design and test customer-access controls around the ways users can conceal their location, including VPNs, proxies, location spoofing, rooted or emulated devices and remote access. Reassess those controls as your service, technology and circumvention risks change.

For compliance with OFAC sanctions use OFAC's current programme information⁵ to update jurisdiction rules when applicable sanctions change. For example, OFAC's comprehensive Syria sanctions programme ended on 1 July 2025, while some targeted sanctions still remain. Earlier violations can still be investigated. OFAC explains the distinction in FAQ 1220.⁶

⁴ OFAC, Sanctions compliance guidance for the virtual currency industry (2021). ofac.treasury.gov/media/913571/download

⁵ OFAC, Sanctions programs and country information. ofac.treasury.gov/sanctions-programs-and-country-information

⁶ OFAC, FAQ 1220. ofac.treasury.gov/faqs/1220

5.2 • MiCA

MiCA: distinguish market access from reverse solicitation

For third-country firms providing crypto-asset services, MiCA's reverse-solicitation exemption concerns services initiated exclusively by the client. ESMA interprets that exemption narrowly and says contractual disclaimers cannot override contrary facts.

ESMA also identifies geo-blocking as one possible precaution for a third-country firm refraining from providing crypto-asset services to EU clients. Firms relying on reverse solicitation should retain records showing how the client initiated the relationship and whether the firm or anyone acting on its behalf solicited them. See ESMA's guidelines, paragraphs 16 and 23–28.⁷

Set a clear policy for EU access and document any reliance on the reverse-solicitation exemption.



⁷ ESMA, Guidelines on reverse solicitation under MiCA (ESMA35-1872330276-2030). esma.europa.eu/sites/default/files/2025-02/ESMA35-1872330276-2030_Guidelines_on_reverse_solicitation_under_MiCA.pdf

5.3 · EU TERRITORIAL SANCTIONS

EU territorial sanctions: restrictions below country level

EU territorial sanctions can apply below country level. For example, Ukraine as a country is not under EU territorial sanctions but its specific regions under Russian control are. Council Regulation (EU) No 692/2014⁸, as amended, concerns Crimea and Sevastopol. Council Regulation (EU) 2022/263⁹, as amended, covers the non-government controlled areas of Ukraine in the oblasts of Donetsk, Kherson, Luhansk and Zaporizhzhia.

The first thing is identifying the restrictions that apply to your business, its services and potential customers or recipients of that service. The territorial connection may get established through a company's registered office, its operations or the destination of a service.

Use regional rules where sanctions cover part of a country like in the case of Ukraine. For compliance with EU territorial sanctions ensure the geo-blocking and payment screening both work at relevant moments of your business activity. Match evidence from both controls with applicable restrictions. For example session-location signals for customer access, and recipient, bank or service-destination details for the relevant transaction. Keep your geographic rules current and review any unresolved territorial connections before permitting the affected activity.

⁸ Council Regulation (EU) No 692/2014, consolidated text. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014R0692-20250225

⁹ Council Regulation (EU) 2022/263, consolidated text. eur-lex.europa.eu/eli/reg/2022/263/2025-02-25/eng

SECTION 06

How do geo-blocking controls fail?



Regulatory guidance and existing enforcement examples points clearly towards the following failure modes in geo-blocking controls:

01 Control working but measuring the wrong location

In the TradeStation¹ example, the mobile control read a US server's IP instead of the customer's. Requests could therefore appear domestic even when customers were elsewhere.

02 Control stops running

A separate TradeStation control remained disabled after an update. The application continued operating while that restriction was inactive.

03 Incomplete geographic coverage

The Interactive Brokers¹⁰ enforcement example describes omissions involving Crimea and Sevastopol. A control can operate correctly against its configured rules while those rules leave relevant territories uncovered.

04 The failure goes unnoticed

Ineffective testing and an unaddressed loss of notifications allowed the TradeStation problems to persist. The weakness here is the failure to detect that protection has stopped working.

¹ OFAC, settlement with TradeStation Securities. ofac.treasury.gov/media/935351/download

¹⁰ OFAC, Interactive Brokers enforcement release. ofac.treasury.gov/media/934501/download

“

Regulators do not hold systems accountable.
They hold people and firms accountable for
how they use those systems.”

Ray Blake, as quoted in Shufti's If Your Verification System is 99% Accurate, Are You Really Safe? webinar summary.¹¹

¹¹ Shufti, If Your Verification System is 99% Accurate, Are You Really Safe? Webinar summary. shuftipro.com/wp-content/uploads/PDF-Verification-system-Webinar-Summary.pdf

SECTION 07

What should a defensible location-control programme contain?

Build customer-location controls around six capabilities, with defined handoffs to payment screening:

01 Maintain a written policy

Map restrictions to the entity, product and activity. Record rule versions, effective dates, sources, exceptions and the person accountable for updates.

02 Determine location evidence

Use available IP, GPS, Wi-Fi, cellular and other device or network signals to assess the customer's access location. Confirm availability and accuracy of these signals for each browser, operating system and integration type.

03 Determine checks at relevant points

Decide when to check access location at different instances like onboarding, login, relevant transaction initiation or after a change in circumstances. Separately define the information and screening needed for incoming and outgoing payments. Jurisdiction-rule changes should trigger reassessment.

04 Test specific circumvention techniques

Evaluate VPN/proxy detection, location spoofing, device-integrity risks, remote access and session anomalies against your own system or application. Establish what each check detects, on which platforms, and its known false-positive and detection limits.

05 Monitor the process

On set intervals check signal availability, error rates and decision distributions. Investigate an unexplained fall in blocks alongside traffic volumes, signal availability and control errors. Test expected restrictions after new releases and configuration changes; verify that test traffic actually reaches the control.

06 Record reviewable decisions

Preserve enough evidence to reconstruct the rule, input, action and any override. Assign retention by record category and applicable obligations.

These requirements apply whether you've white-label partners or embedded integrations. Obtain evidence of what each partner collects and enforces. For payment providers, also establish which party, bank and routing fields are available, how missing details are obtained, and who investigates alerts or prevents execution or release while review is pending.

SECTION 08

What evidence should you be able to retrieve?

Keep linked records for customer-access and payment decisions. Each should identify the evidence used, the applicable rule and the outcome. Verify that records can be inspected and exported, with retention configurable by record category. The following fields provide a starting point:



RECORD FIELD

WHAT TO CAPTURE

Decision reference

Unique decision ID, customer/account reference, timestamp and requested action; session reference for access checks and payment reference for transaction screening.

Applicable policy

Entity, product, rule ID/version, jurisdiction restriction and legal or policy basis.

Evidence considered

For access: location signals, collection time, confidence, integrity checks and conflicts.

For payments: party, address, account, bank, route and purpose data considered, screening results and any information obtained during review.

Outcome

Access: allowed, restricted or pending review.

Payment: cleared, under review, rejected or blocked as applicable; reason, legal basis and any required report reference.

RECORD FIELD	WHAT TO CAPTURE
Review or override	Reviewer, rationale, supporting evidence, approved exception if applicable, scope and expiry.
Control assurance	Relevant release/configuration version, test reference, monitoring incident and subsequent remediation.
Retention and access	Record category, retention basis, deletion schedule, access controls and any applicable legal hold.

OFAC extended relevant recordkeeping requirements from five to ten years. Under 31 CFR 501.601, transaction records generally run from the transaction date; blocked-property records are kept while blocked and for the required period after unblocking. Confirm the applicable scope and dates against OFAC's final rule.¹² Set retention for raw location signals according to the evidence required for each record category and applicable privacy and security obligations.

¹² OFAC, final rule on recordkeeping requirements. ofac.treasury.gov/media/934131/download

SECTION 09

How Shufti supports geo-blocking compliance

Shufti Geolocation Compliance¹³ links customer-location checks to verified identity, helping teams apply jurisdiction rules and keep a record of each access decision. It supports five parts of the control programme:



Establishing geolocation

GPS, Wi-Fi and cellular signals are cross-checked to assess the device's position. A confidence radius helps evaluate customers close to a jurisdictional boundary.



Detecting circumvention

Checks cover VPNs, proxies, Tor, GPS spoofing and device tampering. IP/device mismatches and rooted, jailbroken or emulated devices can be routed to review.



Applying restrictions

Configurable maps define permitted regions and exclusion zones. A confirmed restricted location takes precedence over a passing trust score, keeping the geographic rule decisive.



Maintain coverage

Checks can run at registration, login and withdrawal, with periodic re-verification and more frequent checks near boundaries. Teams adjust triggers and rules through the console.

¹³ Shufti, Geolocation Compliance. shuftipro.com/geolocation-compliance/



Explain decisions

Each check returns Allow, Review or Decline with a trust score, reason code and timestamp. The platform enforces the verdict and retains the decision record.

For payments, Shufti Transaction Trust Monitoring¹⁴ assesses transaction information alongside verified customer context, including beneficiary or payer and payment-corridor risk. Missing required information is marked as not assessable, and alerts carry supporting evidence into review and escalation.

Bring your jurisdiction policy and a difficult access or payment scenario to a Shufti walkthrough¹⁵ to examine the checks, decisions and evidence.

Related reading: iGaming geolocation requirements, market by market.¹⁶

¹⁴ Shufti, Transaction Trust Monitoring. shuftipro.com/transaction-monitoring/

¹⁵ Shufti, request a demo. shuftipro.com/request-demo/

¹⁶ Shufti, iGaming geolocation requirements. shuftipro.com/igaming-geolocation-requirements/

FREQUENTLY ASKED

FAQ

01 Is IP blocking enough to satisfy OFAC?

An IP lookup is not a complete sanctions programme. OFAC's virtual-currency guidance also discusses VPN detection, improbable logins and other available information. Test those controls against the risks and restrictions applicable to the service.

02 How common is VPN use during identity verification?

In Shufti's analysed onsite sessions from January to August 2026, 1.71% were classified as VPN or proxy traffic.

03 Does MiCA require geo-blocking?

ESMA identifies geo-blocking as a possible precaution for third-country firms refraining from serving EU clients. Firms using the reverse-solicitation exemption need records supporting the client's exclusive initiative.

REFERENCES

- 1 OFAC, settlement with TradeStation Securities.
ofac.treasury.gov/media/935351/download
- 2 Swift, IBAN resource. swift.com/swift-resource/9606/download
- 3 Shufti, AML screening. shuftipro.com/aml-screening/
- 4 OFAC, Sanctions compliance guidance for the virtual currency industry (2021).
ofac.treasury.gov/media/913571/download
- 5 OFAC, Sanctions programs and country information. ofac.treasury.gov/sanctions-programs-and-country-information
- 6 OFAC, FAQ 1220. ofac.treasury.gov/faqs/1220
- 7 ESMA, Guidelines on reverse solicitation under MiCA. esma.europa.eu
- 8 Council Regulation (EU) No 692/2014, consolidated text. eur-lex.europa.eu
- 9 Council Regulation (EU) 2022/263, consolidated text. eur-lex.europa.eu
- 10 OFAC, Interactive Brokers enforcement release.
ofac.treasury.gov/media/934501/download
- 11 Shufti, If Your Verification System is 99% Accurate, Are You Really Safe? Webinar summary.
shuftipro.com
- 12 OFAC, final rule on recordkeeping requirements.
ofac.treasury.gov/media/934131/download
- 13 Shufti, Geolocation Compliance. shuftipro.com/geolocation-compliance/
- 14 Shufti, Transaction Trust Monitoring. shuftipro.com/transaction-monitoring/
- 15 Shufti, request a demo. shuftipro.com/request-demo/
- 16 Shufti, iGaming geolocation requirements, market by market. shuftipro.com/igaming-geolocation-requirements/



How Shufti supports geo-blocking compliance

Bring your jurisdiction policy and a difficult access or payment scenario to a Shufti walkthrough to examine the checks, decisions and evidence.

[Book a Shufti walkthrough](#)

Shufti is based in the United Kingdom and operates offices worldwide.



United States

16200 SW Pacific Hwy,
Suite H PMB 1053,
Tigard, OR



Cyprus

Arch. Makarios III
Avenue 229, Limassol



Dubai

Unit 507, Level 5, Gate
District Precinct
Building 03, DIFC,
Dubai



Hong Kong

8 Queen's Road East,
Wan Chai, Hong Kong



Pakistan

322-G3 Main Blvd,
Johar Town, Lahore,
Pakistan



Singapore

68 Circular Road
#02-01, Singapore



United Kingdom

Office 408,
Coppergate House, 10
Whites Row, London
E1 7NF

shuftipro.com
sales@shuftipro.com