Mastercard Guidance for BRAM Compliance

Business Risk Assessment and Mitigation (BRAM)

May 19, 2017
Mastercard Position on Illegal Activity

• Mastercard does not tolerate use of its brand, programs, or services to further any illegal activities

• Mastercard requires its customers (and their merchants/cardholders) to comply with all applicable laws and Mastercard Rules and Standards

• Mastercard has aggressive programs to detect illegal activity

• Mastercard is committed to working closely and cooperating with law enforcement
The BRAM Program is an initiative launched in 2005 which is designed to protect Mastercard and its customers from illegal and brand-damaging transactions, which may pose significant fraud, regulatory, or legal risk, or may cause reputational damage.
BRAM Program Violations

*Examples of BRAM Violating Transactions

- Illegal sale of prescription drugs and/or tobacco products
- Illegal Internet gambling / miscoded gambling
- Child exploitation
- Offensive adult pornography
- Sale of counterfeit merchandise
- Sale of goods or services in violation of intellectual property rights
- Sale of certain types of drugs or chemicals (synthetic drugs, salvia divinorum, etc.)
- Coerced Transactions

*Examples are not exclusive. Any product or service that is illegal or brand-damaging is included in BRAM.
Entities

European Commission

Medicines & Healthcare products Regulatory Agency

National Center for Missing & Exploited Children

International Centre for Missing & Exploited Children

International Anti-Counterfeiting Coalition

CSIP

Drug Enforcement Administration

Motion Picture Association of America

The Software Alliance

BSA

Mastercard
BRAM Investigative Process

Referrals
- Law Enforcement
- Rights Holders
- Web Crawler
- Internal Investigation

Mastercard Process
- Conduct Investigation
- Perform Trace
- Confirm Non-Compliance
- Notify Acquirer

Acquirer Process
- Conduct Investigation
- Cease Activity
- Provide Response
- MATCH Listing
Child Exploitation / Human Trafficking

- Mastercard is an active partner on several coalitions to protect children from commercial sexual exploitation and human trafficking.
- Mastercard serves on the Board of Directors for the Financial Coalition Against Child Pornography (FCACP).
- Includes private sector partnership with law enforcement agencies to combat the commercial distribution of child pornography.
- Structure a systematic process that can be leveraged by all stakeholders to share information and take appropriate action to prevent child pornography merchants from entering the payments system and establishing merchant processing accounts.

Participation with coalitions to protect children from commercial sexual exploitation include:

- European Financial Coalition Against Commercial Sexual Exploitation of Children Online – EFC
- Financial Coalition Against Child Pornography – FCACP
- Associated Groups –
  - International Centre for Missing & Exploited Children – ICMEC
  - National Center for Missing & Exploited Children – NCMEC
Once alerted to suspected child exploitation, we submit the URL to NCMEC via the CyberTipline.

NCMEC will confirm and send to law enforcement who will conduct a test transaction.

If law enforcement proceeds with the investigation, they will advise us to action or not so that we do not interfere with their investigation.

If we action, we follow the law enforcement investigative process and notify the acquirer of the noncompliance and provide 2 days to cease the illegal activity and respond.
Synthetic Drugs

• Mastercard continues to see an increase in synthetic drug violations
• These are products with psychoactive and/or stimulant characteristics
• Create health and safety concerns
• Increasing number being created and sold
• Marketed as incense/potpourri/bath salts
• Marketing is targeted to youths
• Change molecular structure to continuously evade regulation and law enforcement
• Current deaths from PINK
• Violations of intellectual property rights (trademark and copyright infringements) continue to increase

• Mastercard has a clear IP Piracy Policy where we investigate all complaints of suspected IP infringement located online at: https://www.mastercard.com/us/wce/PDF/mastercard_Anti-Piracy_Policy.pdf

• Dedicated email address of ipinquiries@mastercard.com and form for reporting of any suspected IP infringement

• Work with a variety of law enforcement agencies worldwide, IP rights owners and associations that represent IP rights owners
  • IP infringement covers pirated movies, TV shows, music and software
  • IP infringement also covers counterfeiting of brands such as luxury fashion brands ranging from Louis Vuitton to Ugg’s to Ray Ban’s
New BRAM Items Added

• Circumvention Devices - Illicit Streaming Devices (ISD aka Black Boxes)
  • Applications installed on the streaming device/black box allows for circumvention of technology designed to prevent access to copyrighted material
  • Devices sold with pre-installed applications to specifically circumvent technologies will be considered a BRAM violation

• Securities Trades In Canada
  • Securities trades including binary options trades are regulated in Canada
  • Must be registered with each provincial and territorial securities commission
  • Global Security Bulletin 15, November 2016
Product/Service to Watch - Binary Options Trades

- Receiving attention from various governments worldwide
- Receiving referrals from Canada, US, and others
- Watch for further Regulations – Israel, etc.
- Concerns include deceptive practices, increased fraud and chargebacks, illegal operators and charging undisclosed fees to name a few
- Reminder that investment earnings must be processed as a Payment Transactions (see Transaction Processing Rules)
- Transactions must be processed under MCC 6211 (Securities – Brokers / Dealers)
- Countries may regulate as gambling, therefore merchants operating in these countries must code the transactions with MCC 7995 (Gambling)
- Revised Cardholder Dispute Standards for Investments and Similar Disputes (Global Operations Bulletin No. 10, 3 October 2016)
Product/Service to Watch – Possible Circumvention Routes

• e-Voucher Merchant Models
  • May be used to circumvent Mastercard Rules for illegal activity such as gambling
  • Model is considered a Digital Wallet Operator (DWO) and must be compliant with those rules
  • Funding from a wallet to a prepaid card to circumvent rules

• Unregistered Staged Digital Wallet Operators (DWO)
  • Observed many unregistered DWOs
  • Not compliant with Mastercard Rules, registration requirements and operational activities
  • Accepting deposits that may circumvent rules such as deposits for gambling but are not coded as such
  • Funding from a wallet to a prepaid card to circumvent rules

• Prepaid Card Programs
  • Issuers should monitor for compliance with AML, jurisdictional regulations and Mastercard Rules, etc.
  • Acquirers should monitor the loading of funds to identify any patterns (i.e., same BIN, same country, etc.)
Products/Services to Watch - Gambling

• Miscoded Gambling Transactions in Asia Pacific Region
  • Identified merchants involved in illegal gambling schemes to circumvent gambling laws and Mastercard Rules
  • Patterns include a high concentration of cardholders from countries with gambling restrictions and large transaction volumes in a short period of time

• Gambling Regulations & Referrals
  • France – Online Gaming Regulatory Authority (“OGRA” or “ARJEL” in French)
  • Poland – Ministry of Finance / Polish Parliament / Internet Gambling Act of 15 December 2016
  • Hungary - National Tax and Customs Administration of Hungary, Central Management/Gambling Supervision Dept. sending referrals
Claims of Coercion – Card Present

• Mastercard will consider a claim of coercion valid if the cardholder (or the cardholder’s immediate family member) is coerced to complete a transaction because of threat of physical harm or the unlawful taking of property if the cardholder refuses to complete the transaction (Global Security Bulletin No. 5, 16 May 2016)

• Claims of coercion will be reported via email to BRAM@mastercard.com

• Investigate alleged coerced transactions if Mastercard receives complaints by two or more issuers against the same merchant

• Issuers must submit alleged coerced transactions to the System to Avoid Fraud Effectively (SAFE) using fraud type code - Lost Fraud (00) or Stolen Fraud (01)

• If valid, it will be deemed a violation of Rule 3.7, “Integrity of Brand and Network”, with a potential assessment

• First chargeback rights under reason code 4849 – Questionable Merchant Activity if Mastercard deems a valid claim of coercion
Merchant Transaction Laundering (TL)

• Merchant transaction laundering (TL) is the action whereby a merchant processes payment card transactions on behalf of another merchant (also known as “transaction aggregation” or “factoring”)

• Mastercard deems merchant transaction laundering to be a violation of Mastercard Rule 5.1

• Mastercard continues to observe that the majority of BRAM violations include TL

• In most cases, it appears that the acquirer was not aware of such activity and did not implement a sufficiently robust monitoring or detection service to address this activity

• Mastercard continues to encourage acquirers to monitor for and detect merchant transaction laundering

• Solutions are available
Merchant Monitoring Program (MMP) Update

• MMP launched in July 2015 for voluntary acquirer participation

• Over 130 institutions participating

• 10 registered MMSP’s providing services of BRAM content monitoring and Transaction Laundering (TL) detection

• Continue to encourage acquirers to proactively monitor and prevent BRAM violations and merchant transaction laundering events

• Mastercard has provided assessment mitigation on investigations where acquirers have implemented monitoring solutions for BRAM and transaction laundering detection

• Mastercard has witnessed many potential violations that have been identified by the MMSP and resolved by the acquirer prior to Mastercard identification thereby proving that the solutions are working in that acquirers are actioning these alerts to cease the activity thereby never resulting in a BRAM investigation
• Use risk and fraud control strategies designed to detect unusually sharp increases in merchant authorization requests and merchant deposits through daily or real-time monitoring. These suspicious spikes in transaction activity may indicate that a merchant is engaged in transaction laundering.

• Engage a third-party service provider (MMSP) that’s provides BRAM content monitoring and transaction laundering detection services

• Constantly monitor and review the entire merchant portfolio to ensure that merchants are not involved in BRAM and/or Transaction laundering that may constitute BRAM violations.

• Develop and maintain internal procedures for the identification, investigation, and termination (if necessary) of any BRAM violators. Such procedures should be in writing and should identify key contacts, internal escalation procedures, and minimum response expectations.

• Perform a test transaction to confirm any suspected Mastercard rule violation by using an actual Mastercard credit card to confirm the merchant processing, but also the merchant name and location disclosure and how it actually appears to a Mastercard cardholder on a credit card statement. This name should be prominently disclosed on the merchant website and should be the name that most readily identifies the merchant to the cardholder.

• Carefully and regularly review all merchants processing transactions that fall under the heightened risk MCCs, as well as payment facilitator and staged digital wallet type merchants processing transactions on behalf of their associated content suppliers. Report any BRAM violations to Mastercard.
Investigation Process - Acquirer

• Review initial underwriting/due diligence

• Review historical processing volumes and transaction sizes (along with credits, reported fraud and chargebacks)

• Review past risk management actions related to the merchant

• Review approved and violating URL’s

• Perform test transactions (if applicable)

• Contact merchant and perform an investigation with the merchant

• MMSP usage for BRAM content monitoring and/or merchant Transaction Laundering detection (rescan URL, provide rescan and historical monitoring reports in response)

• Cease the merchants illegal activity
Investigation Best Practices

• Proactively investigate all incidents of suspected non compliance

• Conduct a full investigation and gather all the known facts available at the time and ensure that ongoing developments are also recorded

• Maintain a comprehensive investigation report

• Work ahead of deadlines to ensure investigation reports and updates are delivered in a timely manner

• Develop clear and obtainable action plans and timelines to resolve issues and deliver requirements on time

• Develop a set of procedures and supporting process flows for noncompliance investigations

• In cases of noncompliance, submit a comprehensive investigation response to Mastercard providing answers to all questions and all required documentation
Develop Response to Mastercard

- Provide a formal response to Mastercard and include:
  - All documentation requested in the investigation letter
  - All data requested in the investigation letter
  - BRAM Response Form - April Bulletin (MCConnect Library)
  - MMSP report (rescan and historical monitoring reports)
  - Legal opinion (if applicable)
  - Final formal response on acquirer letterhead
  - Provide by response due date
  - Failure to respond by the due date may result in an additional assessment for non-response
Best Practices for a Good Response to Mastercard

• Provide a strong and detailed remediation plan that details the incident, all investigative information and steps and all corrective action
• Provide copies of all applications, agreements, MATCH inquiries and due diligence documents from onboarding and risk related actions
• Provide sales volumes and transaction counts in USD by month and then grand total of all months
• Provide screen prints of volumes that can be verified (merchant supplied figures will not be accepted) for the approved and violating sites
• Provide a review of the approved and violating URL’s, URL registrants and relationships to other merchant accounts and URL’s
• Provide a list of all Service Providers used and their functions
• Provide screen prints and reports from your registered MMSP reflecting the monitoring of the merchant and all URL’s
Questions