Payments Webinar Education Series

Session #3: Compliance of All Kinds

October 15, 2021

Infinicept

GET PAYMENTS GOING YOUR WAY™

Presenting Today

Dan Spalinger, Infinicept Senior Consultant

Dan helps develop and revise Underwriting, AML, Compliance, Credit and Risk policies and procedures.

Prior to Infinicept, Dan spent three plus years as the Underwriting and Risk Manager for the Payment Facilitator program at two large acquirers, and over 15 years within the Credit departments of some of world's largest Banking and Automotive enterprises.

He now seeks to expand card acceptance across the globe, partnering with enterprises desiring to stand up programs necessary to mitigate risk in this burgeoning space.

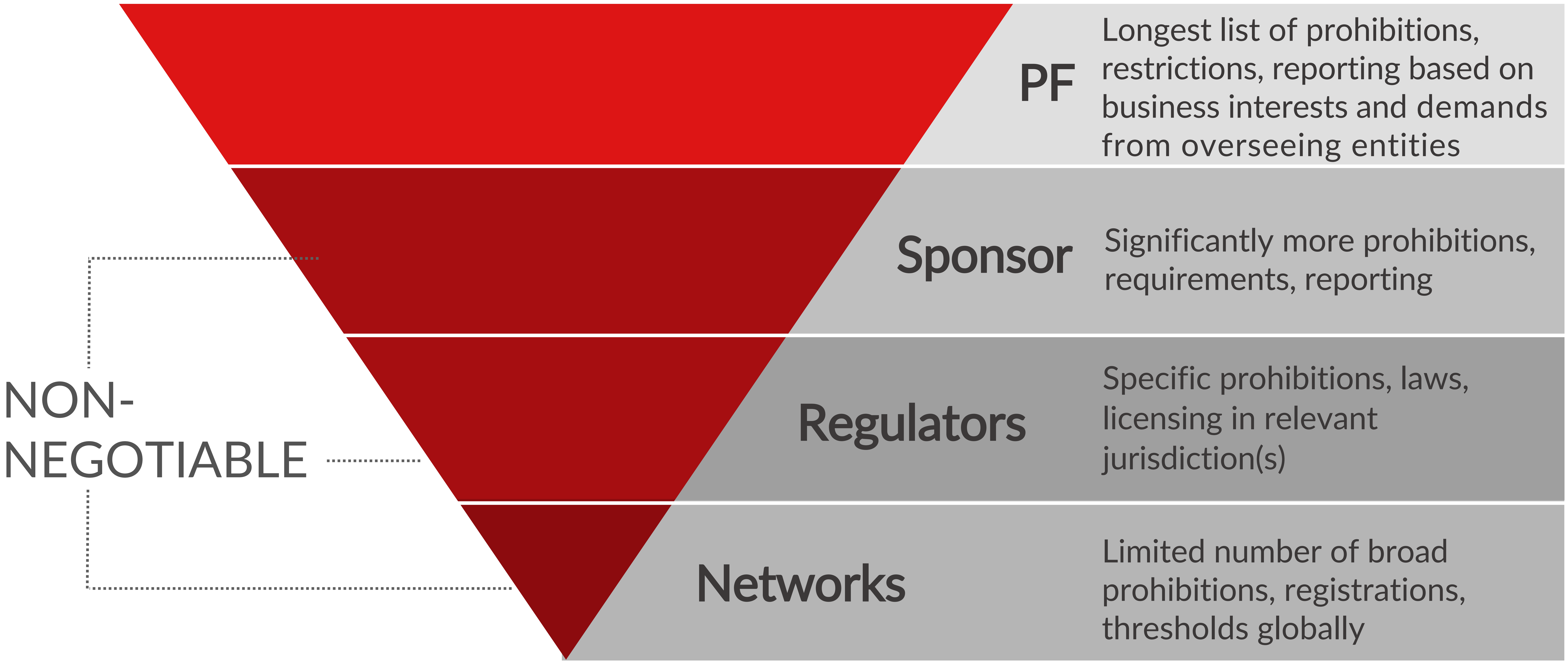
Background

- As a Payment Facilitator (PF) you are beholden to rules and regulations from many entities, let's cover who and what they are.
- Compliance is achieved by remaining aware of changing conditions and implementing appropriate processes.
- Ongoing education, communication, and industry participation are key supports.

Today's Agenda

- Who are you overseen by?
- MATCH & OFAC scrubbings
- SAR and Submerchant reporting requirements
- PF program data requirements and high-risk registrations
- MC & V Chargeback program thresholds
- PCI Compliance

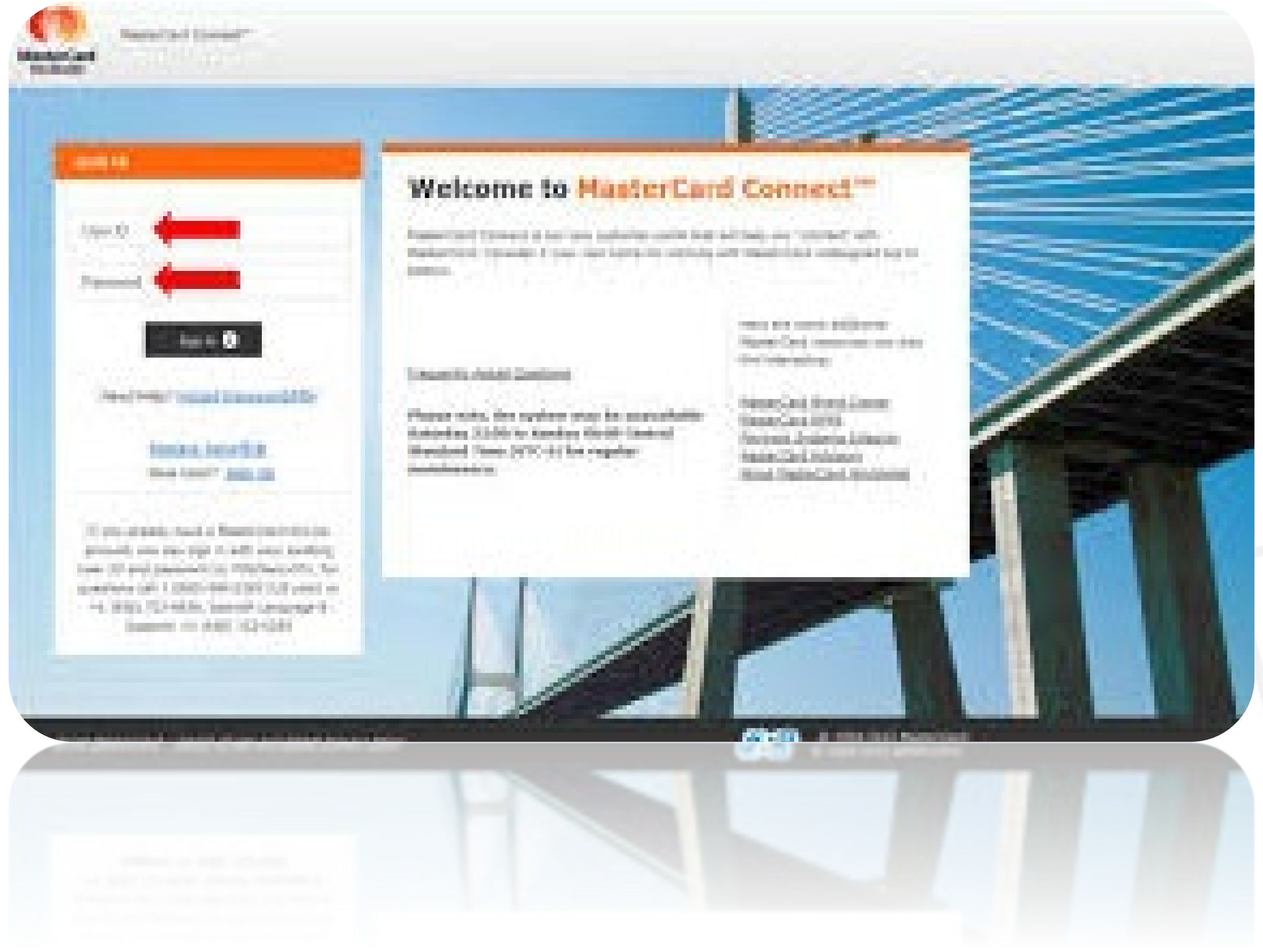
Regulatory and Compliance Demands

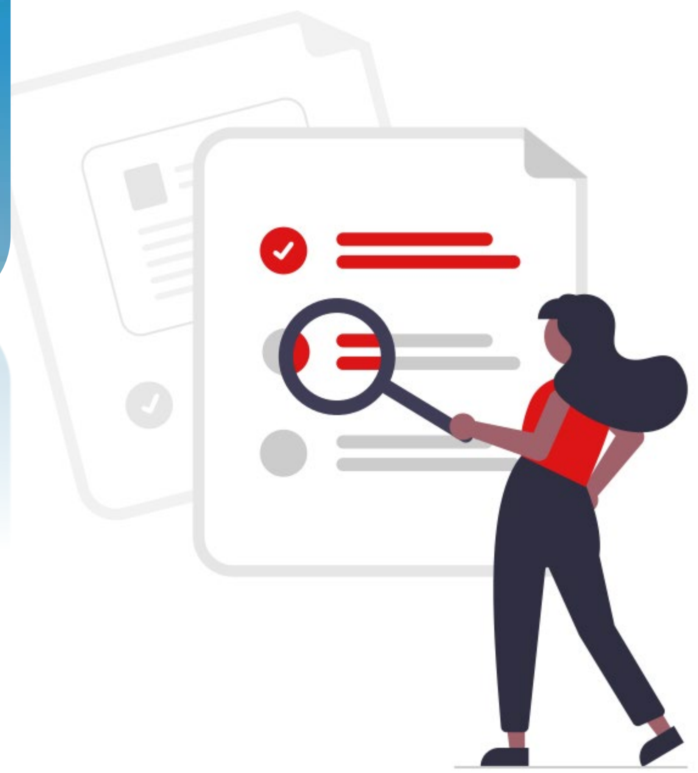


Required by Mastercard And Visa, Run by The Acquirer

MATCH Reports

- Cannot have as a submerchant (Visa)
- Required by Mastercard and Visa prior to processing
- Not a blocklist
- Use for investigation
    - Partial MATCH hits
    - Multiple inquiry hits can be an indication of fraud or other problems
- Acquirers must ensure merchants terminated by their PFs are appropriately added to MATCH if listing criteria are met

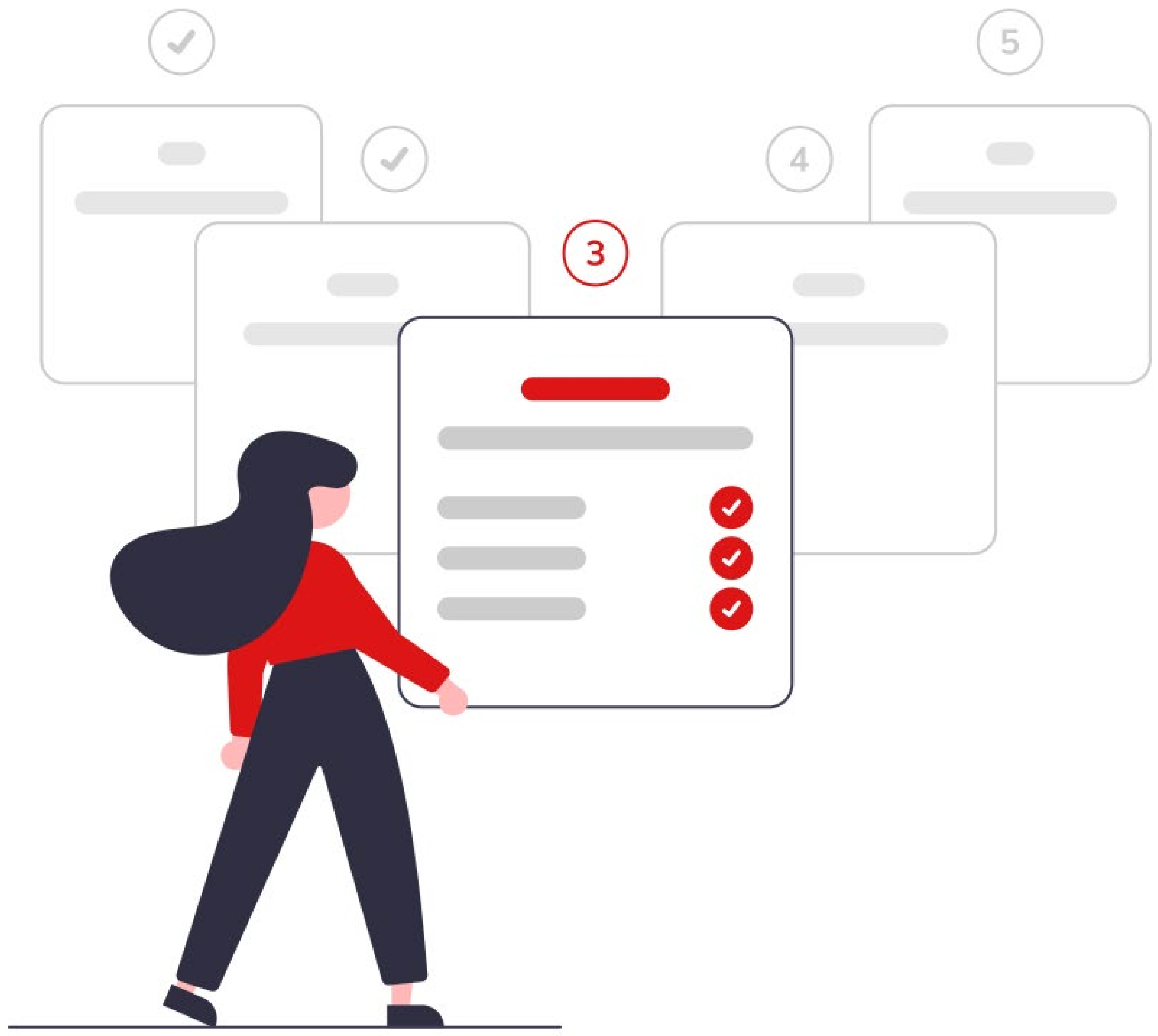




OFAC

Office of Foreign Asset Control (OFAC)

- Verify applicant, principals, and owners are not on the OFAC list of prohibited merchants
- Re-run this check periodically (monthly at minimum) on existing merchants
- Not just OFAC (includes numerous lists including those established by other Government Departments such as Commerce)
- Not just businesses and individuals but geographies as well
- Often run by the Acquirer as well within their own OFAC screening process ensuring backup



SAR

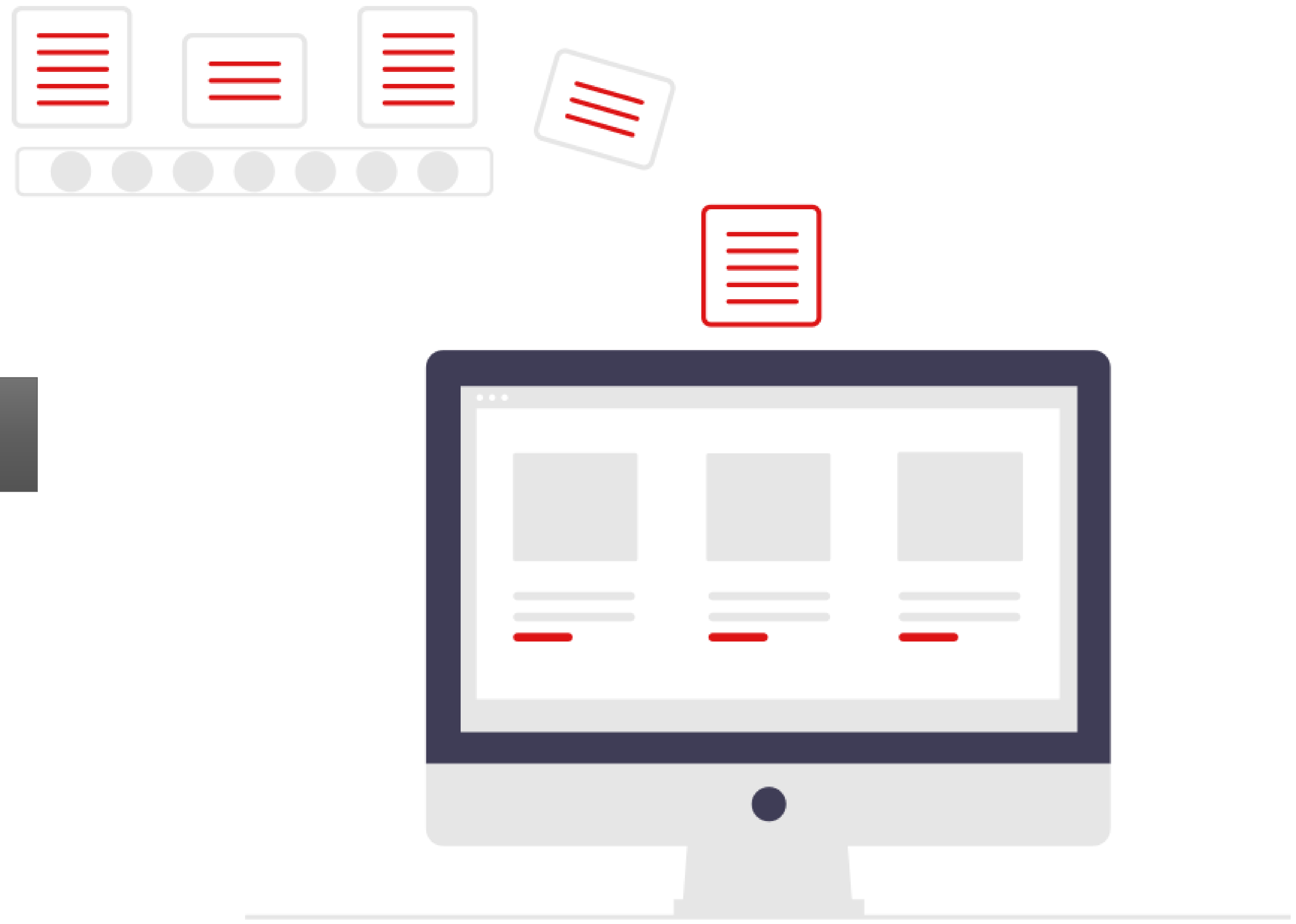
Suspicious Activity Report (SAR) Filing

- Your Acquirer (or sponsor Bank via your Acquirer if it is not a registered financial institution itself) is required to report on certain activity under the BSA (Bank Secrecy Act)
- Some Acquirers may ask that you also support the filing of CAR (Continuous Activity Report) for when the suspicious activity is ongoing
- Certain Acquirers push this requirement directly down to their Payment Facilitators. Others file SARs themselves, requiring their PFs to provide them information necessart to assist them in determining if a SAR should be filed
- Safe Harbor rules protect financial institutions from certain liabilities arising due to the filing of SARs
- No information regarding the filing or potential filing of a SAR may be disclosed to the individual or merchant
- Criminal activity by insiders, when the amounts exceed certain thresholds, and certain activity association (child exploitation, cybercrime, terrorist funding, etc.) are all drivers of reportable events

Brand Required Transaction Monitoring

Traditional Transaction Monitoring

- Internal negative data base
- Large transactions
- Large batches
- Large or unmatched credits
- Descending declines – no longer a technical chargeback
- Multiple authorizations on the same card
- Same transaction amounts
- Low transaction amounts
- Unsettled authorizations
- Excessive keyed transactions
- Outside of approval parameters
- Forced sales
- Prepaid card
- Same BIN
- Same card across portfolio



More Than Traditional Monitoring

- Changes in Average Ticket
- Delayed Delivery
- International Credit Card Sales Percentages
- Transactions occurring at odd hours
- Transaction anomalies based on Business Type
- Liability with a single cardholder

Reporting Requirements: Portfolio, MCC, Agent, Submerchant

Trending Report – Submerchant Name						
	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
Sales (NT$)						
Sales #						
Refund (NT$)						
Refund #						
Chargebacks (NT$)						
Chargebacks #						
Refund % # refunds / # sales						
Chargebacks % # chargebacks / # sales						
Reject EFT amount						
Reserve amount						

The Mastercard and Visa PF Programs

Volume Threshold

- At $1,000,000 USD in Mastercard or Visa Volume, the submerchant must:
  - Have contract that includes the acquiring bank
  - Receive funding direct from the acquiring bank

Prohibited Submerchants

- Aggregating PFs are not allowed
- Internet Gambling in jurisdictions where illegal
- Marketplaces
- Merchants on MATCH
- Sale of any goods or services that purports to test, cure, treat, or prevent COVID-19
- Staged Digital Wallets

Registration is required with EACH Acquirer

- The PF must receive a written confirmation of registration prior to running transactions.
- Mastercard registration is $3,000 USD
- There is a Mastercard discovery fee of $9,000 USD to be assessed to a given acquirer if a PF is found to be operating but not properly registered
- Visa registration is $5,000 USD

Data Requirements

Identification

- Both PF and submerchant must be identified in the transaction, authorization & settlement records, descriptors, receipts and billing statements
- Transactions must be labeled with MCC code appropriate for the submerchant (not PF)

Unique Identifier

- Additional transaction message data fields must be populated
  - PF ID
  - Submerchant ID

Reporting and Audits

- Quarterly reporting on submerchant activity – when requested or when the identifier is not passed
- Card Brands may conduct financial or operational audits at any time

Other Requirements

- Payment facilitator must comply with PCI requirements
- Payment facilitator will be reviewed by sponsoring acquirer annually
- Payment facilitator must have its own risk-based periodic review process for its own portfolio

Visa PF High Risk Merchant Registration Programs

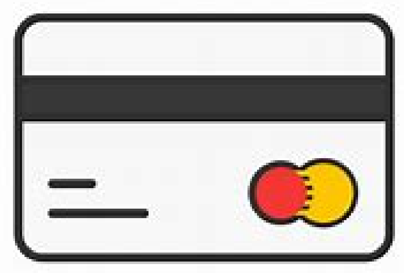
Card-Not-Present Merchant Types Requiring Visa High-Risk Registration

All CNP Merchants in the following MCCs:

- MCCs 5122 and 5912, Drugs, Drug Stores, Pharmacies (but only if conducting non-intra country transactions)
- MCCs 5962, 5966, and 5967, Direct Marketing (Inbound or Outbound or Travel Related)
- MCC 5993, Cigar Stores And Stands (but only if conducting non-intra country transactions)
- MCC 7273, Dating And Escort Services
- MCC 7995, Betting, Lottery Tickets, Casino Gaming Chips, Off-Track Betting And Wagers At Racetracks
- Certain CNP Merchants in the following MCCs:
- MCC 4816, Computer Network/Information Services (Only For The Sale Of Access to Cyberlockers Or Remote Data File-Sharing Services)
- MCC 5816, Digital Goods-Games (Only For Transactions Related To Skilled Game Wagering—Daily Fantasy Sports As Example)
- MCC 6051, Non-Financial Institutions (Only For The Sale Of Cryptocurrencies)

Mastercard PF High Risk Merchant Registration Programs

Card-Not-Present Merchant Types Requiring Mastercard High-Risk Registration



All CNP Merchants in the following MCCs:

- MCC 4816, High-Risk Cyberlocker Merchants
- MCC 6051, Cryptocurrency Merchants
- MCC 6211, High-Risk Securities Merchants
- MCCs 5967 and 7841, Non-Face-To-Face Adult Content and Services
- MCC 7995 Non-Face-To-Face Gambling Merchants
- MCC 5122 and 5912, Non-Face-To-Face Pharmaceutical Merchants
- MCC 5993, Non-Face-To-Face Tobacco Product and ENDS (Electronic Nicotine Delivery Systems) Which Include E-cigarettes, Vape Pens, And Cartridge Merchants

Limitations of Payment Facilitators

A Few Extra Steps & Reporting…

Increased Reporting Required (when indicator not passed)

- All PFs must report quarterly (PF and each submerchant) to licensed bank – if requested
- High risk PFs must report monthly
- In AP Region the Acquirer must submit monthly Merchant data in the merchant master file format (Visa)

Increased Transaction Requirements

- Must have dynamic descriptors capabilities that indicate both the PF AND the submerchant (for Mastercard) or the PF or submerchant or combination of the two (for Visa)
- Must have dynamic MCC capabilities that indicate the MCC of the sub-merchant NOT the PF
- Must pass an PF indicator and a Submerchant Indicator

Descriptors

- Mastercard:
  - PF must be in the descriptor prior to the *
  - Submerchant must be after the *
  - Example: ABC*Small Submerchant
- Visa:
  - The PF name, or submerchant name, or a combination of the PF and submerchant names, separated by *
  - Example: PF*Submerchant

Name Format Samples

Mastercard

- PF name must be to the left of the *
- Using a PF named "PAYMENOW" and a Sponsored Merchant named "Shoes Online", the "*" must be in the following positions of the Merchant Name field:
  - 4 (PAY*SHOES ONLINE),
  - 8 (PAYMENO*SHOES ONLINE), or
  - 13 (PAYMENOW_INC*SHOES ONL)

Visa

- The unique name convention of having PF and submerchant names will no longer be required
- Because the unique identifier is included in the transaction records, the descriptor can be one of the following:
  - The PF name (alone)
  - The Submerchant name (alone)
  - A combination of the PF and submerchant names, separated by "*" (e.g., PF*SUBMERCHANT)
- The name chosen should be the name that is most recognizable to the cardholder

Mastercard Unique Identifier Requirements

Payment Facilitator ID Field

- The PF ID must match the Company ID provided during Payment Facilitator registration or will be provided directly by the Corporation.
  - DE 48 (Additional Data—Private Use), sub-element 37 (Additional Merchant Data), subfield 1 (Payment Facilitator ID) of Authorization Request/0100 and Financial Transaction Request/0200 messages; and
  - PDS 0208 (Additional Merchant Data), subfield 1 (Payment Facilitator ID) of First Presentation/1240 messages.

Submerchant ID Field

- The PF ID must match Submerchant ID supplied by the Acquirer or Payment Facilitator.
  - DE 48 (Additional Data—Private Use), sub-element 37 (Additional Merchant Data), subfield 3 (Submerchant ID) of Authorization Request/0100 and Financial Transaction Request/0200 messages; and
  - PDS 0208 (Additional Merchant Data), subfield 2 (Payment Facilitator ID) of First Presentation/1240 messages.

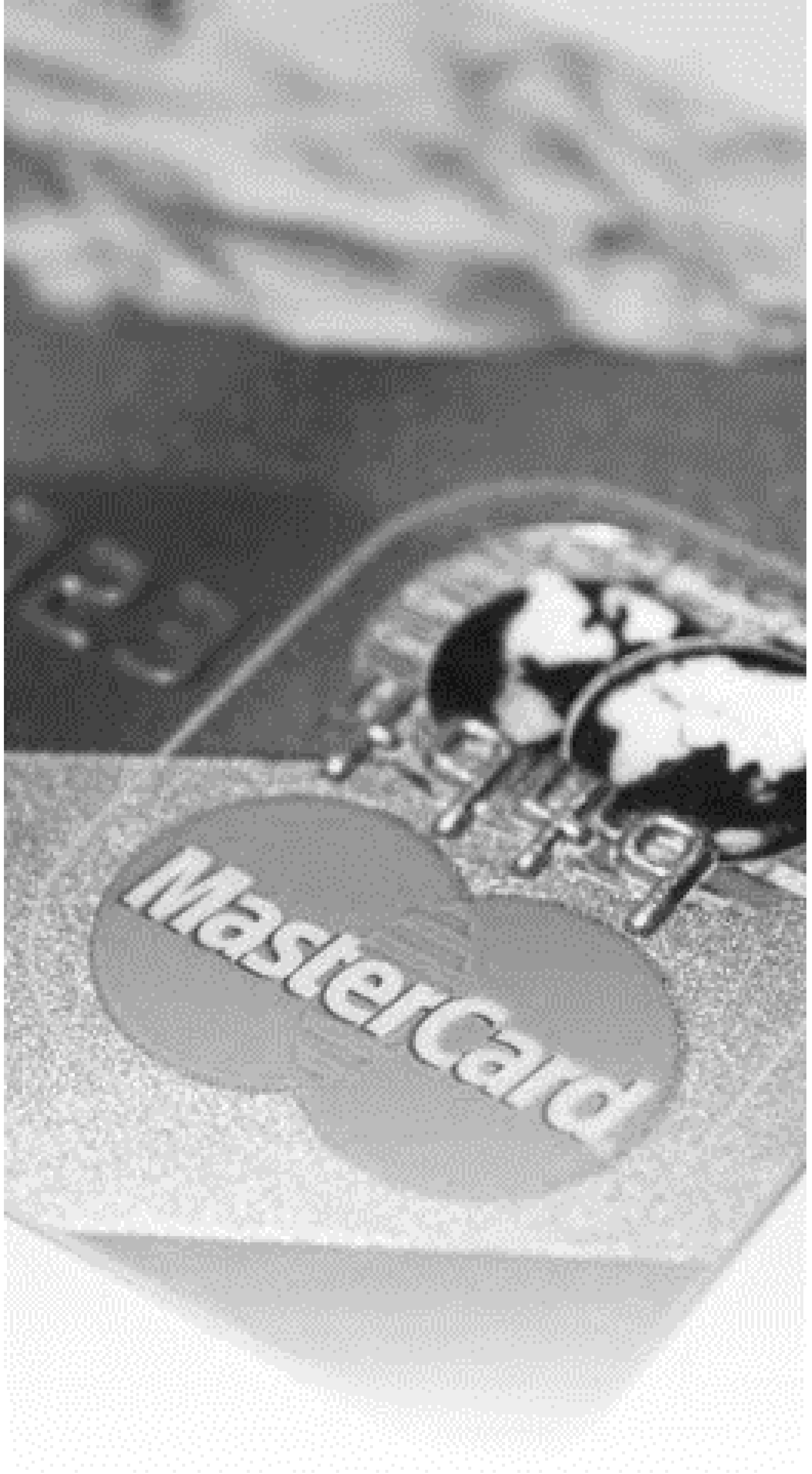
Visa Unique Identifier Requirements

Payment Facilitator ID Field

- The PF ID is the business identifier assigned by Visa to the acquirer when the acquirer registers the entity as a third-party agent with Visa.
  - Position in VisaNet Integrated Payment (V.I.P.) System and Length: Field 104 Usage 2; 8 characters
  - Length and Position in BASE II: TCR1 (Member message text); 8 characters

Submerchant ID Field

- The Submerchant ID is assigned by the PF and must be a unique value for each submerchant. The identifier should remain assigned to the submerchant regardless of the acquirer. The indicator may be numeric or alpha-numeric.
  - Position in VisaNet integrated Payment (V.I.P.) System and Length: Field 104 Usage 2; 15 characters
  - Length and Position in BASE II: TCR1 (Member message text); 15 characters



Mastercard Excessive Chargeback Program

The purposes of ECP (Excessive Chargeback Program) is to:

- Monitor chargeback activity for all merchants, including submerchants of PFs
- Identify and address possible fraud and/or weak business practices which introduce unwanted behavior to the ecosystem
- Incentivize mitigating action plans once c/b trends have been identified
- Protect cardholder experience

New ECP Thresholds	
ECM (Excessive Chargeback Merchant) >150 basis points + at least 100 chargebacks in each month	**HECM** (Excessive Chargeback Merchant) >300 basis points + at least 300 chargebacks in each month

As of 2020 (except for Canada which is Oct 2020):

- Merchants that act quickly to resolve their chargeback issue will be assessed significantly less while those that remain for an extended period will face increasing fines
- Beginning with April violations Acquirers no longer need to report merchant sales and c/b levels when they exceed ECP thresholds, or submit monthly c/b reports, and action plans
- Mastercard will notify Acquirers via the Data Integrity Tool when a merchant exceeds ECP thresholds
- **CMM (Chargeback Monitored Merchant)** threshold is eliminated while the threshold is modified, and a new HECM threshold will be established
- Assessment amounts will increase the longer a merchant is within the program

Visa Dispute Programs

VDMP
(Visa Dispute Monitoring Program)

- **Early Warning**
  - 75 or more Visa c/bs
  - 0.65% or higher ratio of overall Visa c/b-to-interchange ratio (by count)
- **Standard Threshold**
  - 100 or more Visa c/bs
  - 0.9% or higher ratio of overall Visa c/b-to-interchange ratio (by count)
- **Excessive Threshold**
  - 200 or more Visa c/bs
  - 1.8% or higher ratio of overall Visa c/b-to-interchange ratio (by count)

VFMP
(Visa Fraud Monitoring Program)

- **Early Warning**
  - $50,000 or more Visa c/bs
  - 0.65% or higher ratio of overall Visa c/b-to-interchange ratio (by count)
- **Standard Threshold**
  - $75,000 or more Visa c/bs
  - 0.9% or higher ratio of overall Visa c/b-to-interchange ratio (by count)
- **Excessive Threshold**
  - $250,000 or more Visa c/bs
  - 1.8% or higher ratio of overall Visa c/b-to-interchange ratio (by count)

What is PCI DSS Compliance?

- Payment Card Industry Data Security Standard (PCI DSS)
- PCI DSS was developed by a coalition of five card brands (American Express, Discover, JCB, Mastercard and Visa) to protect the integrity of the payments system
- Any entity that stores, processes or transmits cardholder data – including payment facilitators – must comply with the standard
- Payment Facilitators must provide their sponsor bank with an SAQ-D certification and Level 1 or Level 2 attestation on an annual basis.

Security Standards Council®

Level 1 Requirements	Level 2 Requirements
> 6 million annual card transactions	1-6 million annual card transactions
Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA)	Annual Self-Assessment Questionnaire (SAQ)
Quarterly network scan by an Approved Scanning Vendor (ASV)	
Complete Attestation of Compliance Form	

How to Ensure PCI Compliance

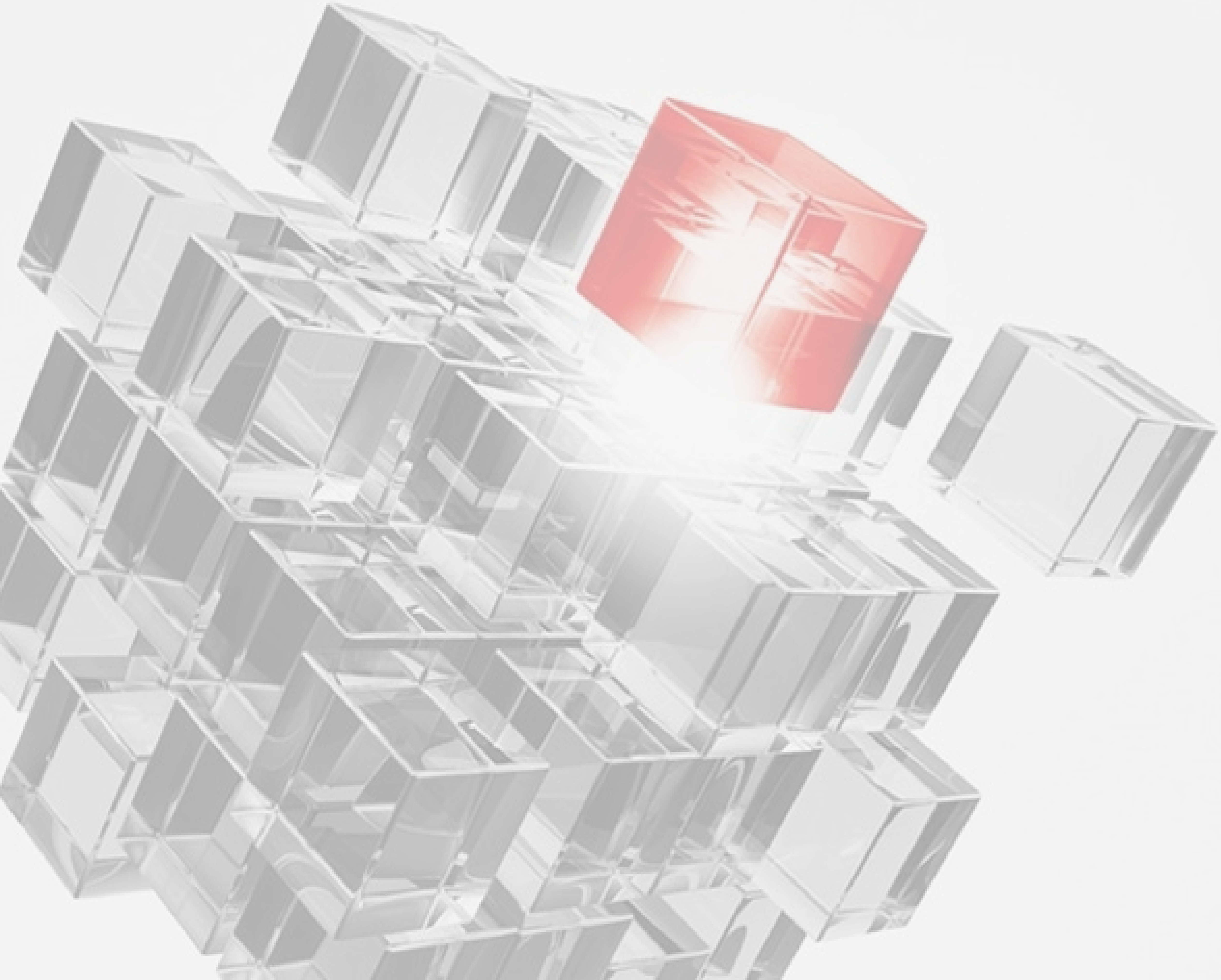
- Learn and understand what you need to achieve and maintain compliance
  - PCI website has great info and training
  - Firms like ControlScan can advise
- Consider the amount of customization and control over the customer experience
  - More individualized user experience may result in larger compliance scope
  - Less control brings less revenue but also smaller scope and lower risk
- Utilize a gateway and token vault so you never store sensitive data
  - Firms like Very Good Security (VGS) provide solutions that give you control and flexibility

ControlScan

VERY GOOD SECURITY

Upcoming: Last Session of the Series…

Oct. 29, 2021 – Session 4: Deconstructing the Cost of Becoming a Payment Facilitator



Infinicept

GET PAYMENTS GOING YOUR WAY™

Thank you

Dan Spalinger

+1 (603) 475-7860

dan@infinicept.com

www.infinicept.com