Protecting the Digital Ecosystem

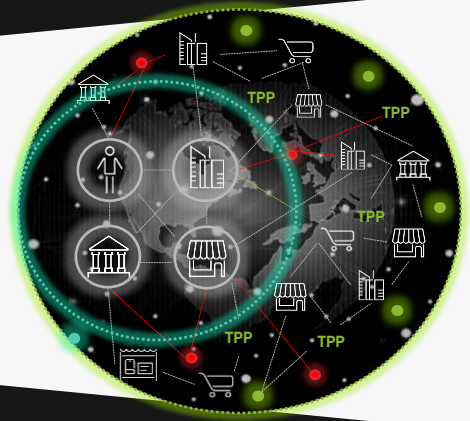
Expanding Security throughout an Evolving Ecosystem and frictionless Security

Carsten Mürl
carsten.muerl@mastercard.com

Safeguarding an evolving ecosystem goes beyond protecting transactions

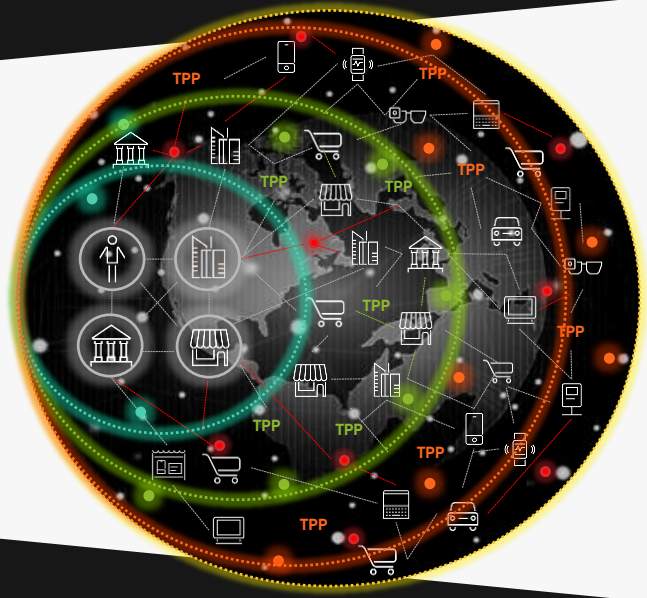
Early Ecosystem

- Well-defined stakeholders
- Protected connections
- Mostly physical acceptance
- Limited large-scale threat
- Growing digital acceptance



Expanding Ecosystem

- New cyber entities
- Increased digital acceptance
- Unprotected connections
- Increased large-scale threat
- More types of transactions



Evolving Ecosystem

- Infinite IoT digital growth
- Countless unprotected connections
- Infinite large-scale threat
- Proliferation of cyber entities
- Increased regulations
- More ways to pay

Consumers and businesses interact beyond cards and payments…demanding protection at every point

Consumers

Payments
(Retail, bill payment, digital wallet)

Personal Entertainment
(Vacation, transit, GPS, Kindle, TV, streaming, movies)

Household
(Appliances, security)

Social media
(Facebook, YouTube)

Businesses

B2B
(Open banking, account-based payments)

Corporate T&E
(Business travel/booking, transit, events, meetings)

Business Admin/ Management
(Security protocols)

Digital Marketing
(Facebook, LinkedIn, YouTube)

MANY interactions…ONE Experience

Increasing digital data and interactions via IoT points to the need for greater security beyond payments

BIGGER DATA

2.5 QUINTILLION

bites of data generated per day by humans and their devices[1]

MORE INTERACTIONS

4.7 BILLION

active internet users around the world in January 2021[1]

2021 ECOSYSTEM TRENDS

RISE IN ECOMMERCE

$9 TRILLION

in digital transaction value by 2024 – increasing 60% over 4 years[2]

INCREASED DIGITAL BANKING

50%

of the world will be using digital wallets by 2024[2]

GROWTH IN IOT

27 BILLION

Is the estimated number of IoT devices by 2025[3]

1. TECHJURY, HOW MUCH DATA IS CREATED EVERYDAY IN 2021? 2021.
2. JUNIPER, ONLINE PAYENT FRAUD 2021-2024.
3. GARTNER, IOT SECURITY PRIMER: CHALLENGES AND EMERGING PRACTICES, 2020.

Criminals are exploiting the increasing gaps in security to compromise trust across billions of interactions

Digital Risk

Card-not-present fraud, friendly fraud

- Digital commerce transaction values will total **$18T** by 2024[1]
- By 2024, digital transaction fraud will equate to **$50.5B**[2]

Financial Risk

Money laundering, ACH/real-time payments fraud

- **$2T+** laundered globally each year[3]
- **45%** of 2020 B2B payments projected to go through ACH rails[4]
- **$36B+** in global regulatory fines to organizations for AML, KYC and sanctions non-compliance violations[5]

Cyber Risk

Malware, ransomware, data breaches, identity theft

- **$3.86 million** is the average total cost of a data breach[6]
- **$5.2T** estimated annual global cyber crime damage costs by 2021[7]

Systemic Risk

Heightened risk exposure from environmental influence

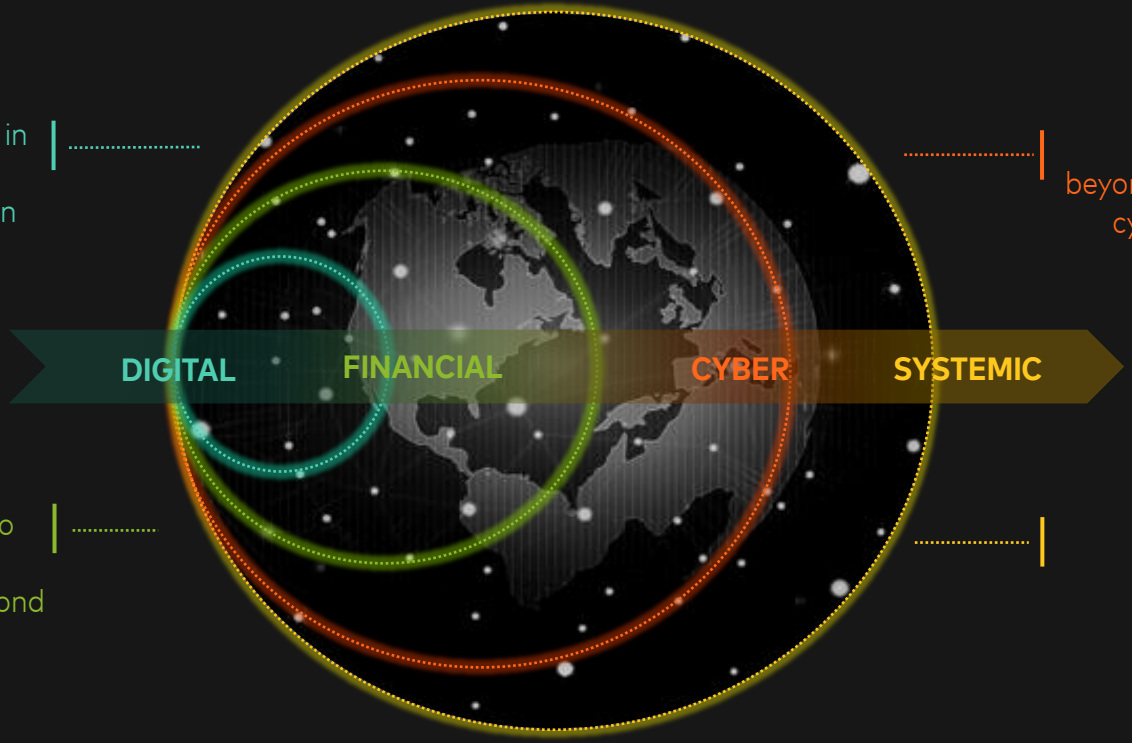
- Following SolarWinds damage, cyber insurance companies are expected to see losses up to **$90B**[8]
- COVID-19 drives large decline in trade – resulting in **$1.7T** in losses to US companies from tariffs on Chinese imports[9]

1. JUNIPER DIGITAL COMMERCE KEY TRENDS SECTORS AND FORECASTS 2020. 2. JUNIPER ONLINE PAYMENT FRAUD. 2020. 3. MONEY LAUNDERING AND GLOBALIZATION, UNITED NATIONS OFFICE ON DRUGS AND CRIME, 2018. 4. NACHA.ORG. 2019. 5.FENERGO ANNUAL REPORT GLOBAL BANKING FINES. 2019. 6. IBM. THE COST OF A DATA BREACH. 2020. 7. ACCENTURE. NINTH ANNUAL - COST OF CYBER CRIME STUDY. 2019. 8. ROLL CALL - CLEANING UP SOLAR WINDS HACK MAY COST AS MUCH AS 100B. JAN 2021. 9. FEDERAL RESERVE BANK OF NEW YORK – THE INVESTMENT COST OF US-CHINA TRADE WAR. MAY 2020.

We are evolving with the ecosystem…from securing transactions to protecting trust in every interaction

Enhance security in the consumer digital transaction journey

Expand security beyond transactions to cyber environments



Extend security to other types of transactions beyond cards

Extend security to mitigate systemic operational risk

One trusted source for protection

A CLOSER LOOK

AT OUR SECURITY STRATEGIES

Enhancing digital security requires ongoing monitoring to safeguard the ecosystem

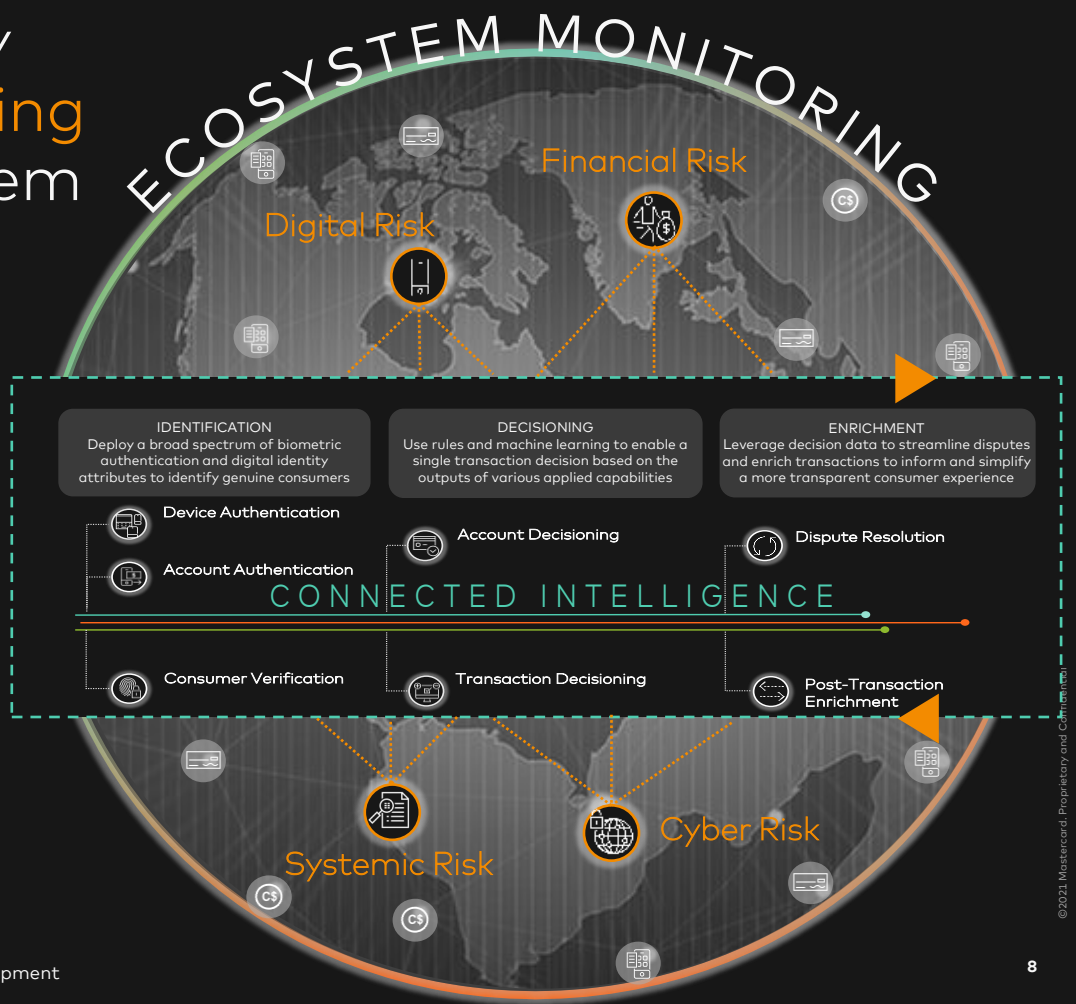
Continuously monitor and evaluate all points of interaction to identify and address threats and vulnerabilities

Digital Risk
SAFETY NET/PREPAID MONIITORING
THREAT SCAN

Financial Risk
AML ACCOUNT RISK
SANCTIONS SCREEN*
REAL-TIME PAYMENTS MONITORING*
TRACE FINANCIAL CRIME

Cyber Risk
SAFETY NET/PREPAID MONIITORING
THREAT SCAN
CYBER SECURE
ID THEFT PROTECTION
RISKRECON

Systemic Risk
SYSTEMIC RISK ASSESSMENT*
CRYPTO SECURE*



Card - Non-Card - Both *In development

Enhancing security across all transaction types in the consumer digital journey with Connected Intelligence

Digital Risk

Financial Risk

Cyber Risk

Systemic Risk

IDENTIFICATION
Deploy a broad spectrum of biometric authentication and digital identity attributes to identify genuine consumers

DECISIONING
Use rules and machine learning to enable a single transaction decision based on the outputs of various applied capabilities

ENRICHMENT
Leverage decision data to streamline disputes and enrich transactions to inform and simplify a more transparent consumer experience

- Device Authentication
- Account Authentication
- Consumer Verification
- Account Decisioning
- Transaction Decisioning
- Dispute Resolution
- Post-Transaction Enrichment

DIGITAL FINANCIAL CYBER SYSTEMIC

Enhancing security across all transaction types in the consumer digital journey with Connected Intelligence

Digital Risk
SAFETY NET/PPM
THREAT SCAN

Financial Risk
AML ACCOUNT RISK
SANCTIONS SCREEN*
RTP MONITORING*
TRACE FINANCIAL CRIME

Cyber Risk
SAFETY NET/PPM
THREAT SCAN
CYBER SECURE
ID THEFT PROTECTION
RISKRECON

Systemic Risk
SYSTEMIC RISK ASSESSMENT*
CRYPTO SECURE*

IDENTIFICATION
Deploy a broad spectrum of biometric authentication and digital identity attributes to identify genuine consumers

Device Authentication
EKATA
SMART INTERFACE
TRUSTED DEVICE

Account Authentication
SMART AUTHENTICATION
VERIFY ACCOUNT NAME/RISK

Consumer Verification
IDENTITY CHECK
ID VERIFICATION
NUDETECT (NUDATA)

DECISIONING
Use rules and machine learning to enable a single transaction decision based on the outputs of various applied capabilities

Account Decisioning
EKATA
NUDETECT (NUDATA)

Transaction Decisioning
BRIGHTERION
DECISION INTELLIGENCE
DIGITAL TRANSACTION INSIGHTS
PREVENT BUSINESS/RETAIL FRAUD
PREVENT MONEY MULES

ENRICHMENT
Leverage decision data to streamline disputes and enrich transactions to inform and simplify a more transparent consumer experience

Dispute Resolution
ETHOCA ALERTS
MASTERCOM

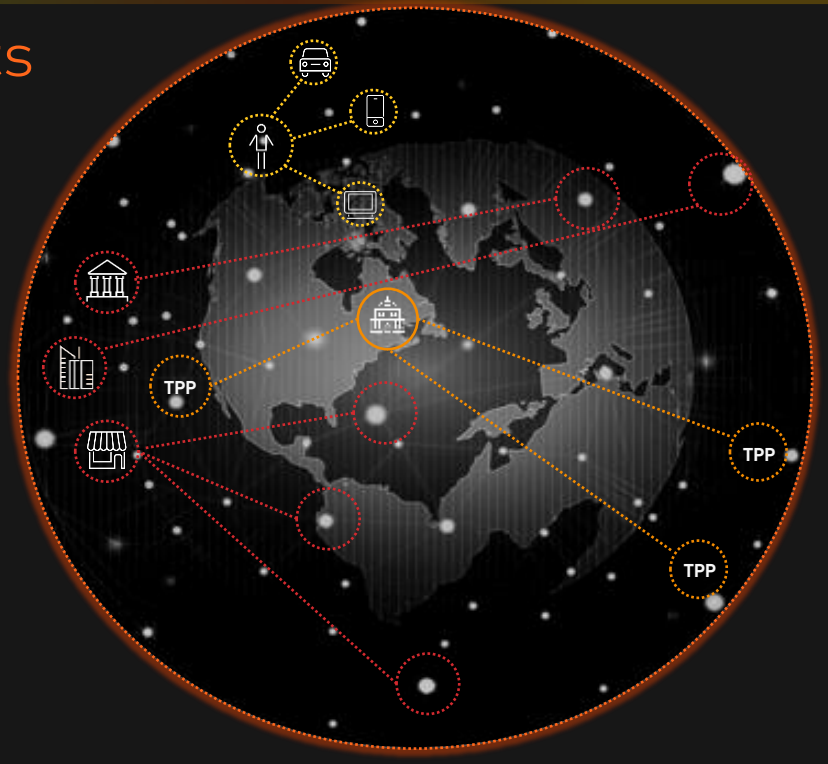
Post-Transaction Enrichment
ETHOCA CONSUMER CLARITY

Card - Non-Card - Both *In development

Protecting cyber environments

Enable cyber risk management at stakeholder touchpoints

- → Confirmed alerts for account data compromise
- → Predictive notifications to determine at-risk accounts
- → Cyber risk ratings and remediation
- → Protection of consumer payment credentials and PII on the dark and surface web



CYBER SECURE

ADC insights and cyber risk assessment

RISKRECON

Cyber risk ratings of third-party relationships

ID THEFT PROTECTION

Protection of consumer personal information

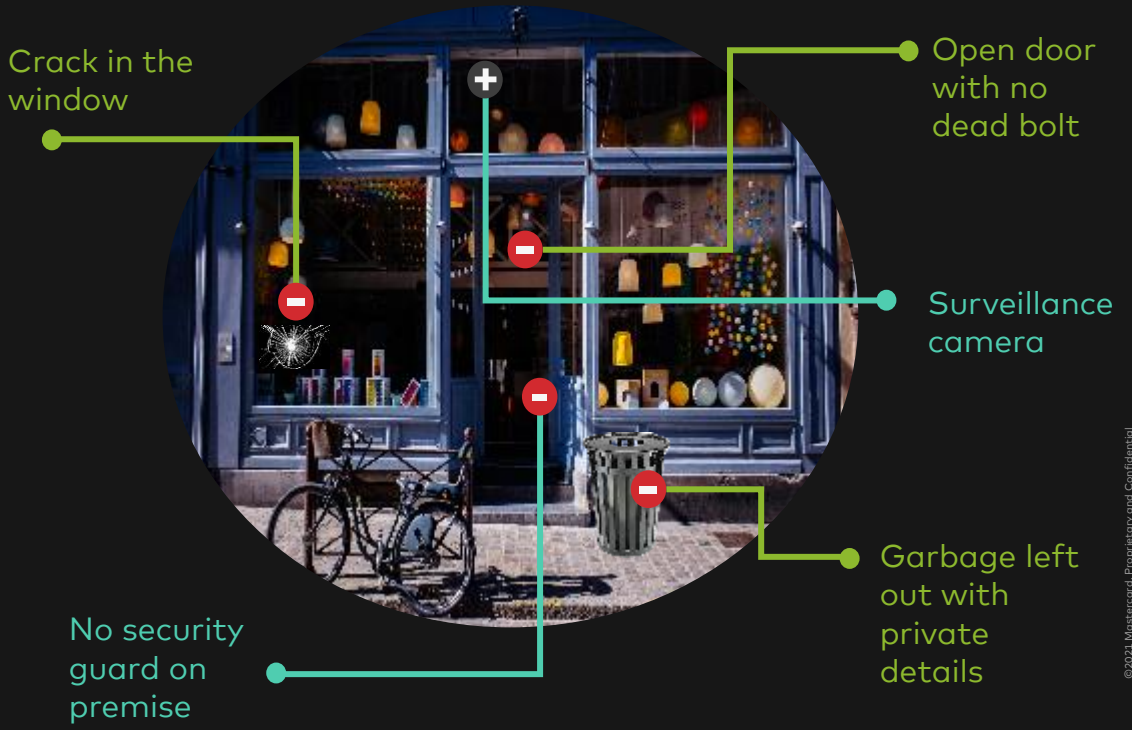
What is cyber risk scoring?

IN CONTEXT

Imagine a thief standing across the street casing a business and assessing both the security safeguards as well as potential gaps for exploitation.

Cyber risk scoring does this same thing in a cyber environment, passively evaluating the security safeguards and gaps in an organization—without interfering in their business—to score cyber risk.

Security safeguards and gaps are assessed by categories for **Security** and **Infrastructure**.



How is the cyber risk score determined?

The cyber risk score is determined by evaluating over 43 criteria across 11 security domains. The impact of all vulnerabilities is analyzed to produce a cyber risk score.

Input

An organization's online web link is used as an input

Security Assessments

1

Evaluate security measures in place to combat risks like malware and ransomware

1. Email security
2. Data loss history
3. Network filtering
4. Governance
5. DNS security
6. Threat intelligence
7. Defensibility

Infrastructure Assessments

2

Assess software and hardware system risks

8. Web encryption
9. Web applications
10. Software patching
11. System hosting

Impact Analysis

3

Analyze the impact each issue uncovered based on its criticality as well as sensitivity of the system where it's identified

RiskRecon for risk premium calculation

will help you in identifying potential cyber security risks. Therefore, associated portfolio risks can be minimized, and better insurance offers can be placed on the market.

HSB **Use Case**

Low-risk customer

Medium-risk customer

High-risk customer

Customer's inquire for a cyber security insurance

Provision of information by a customer

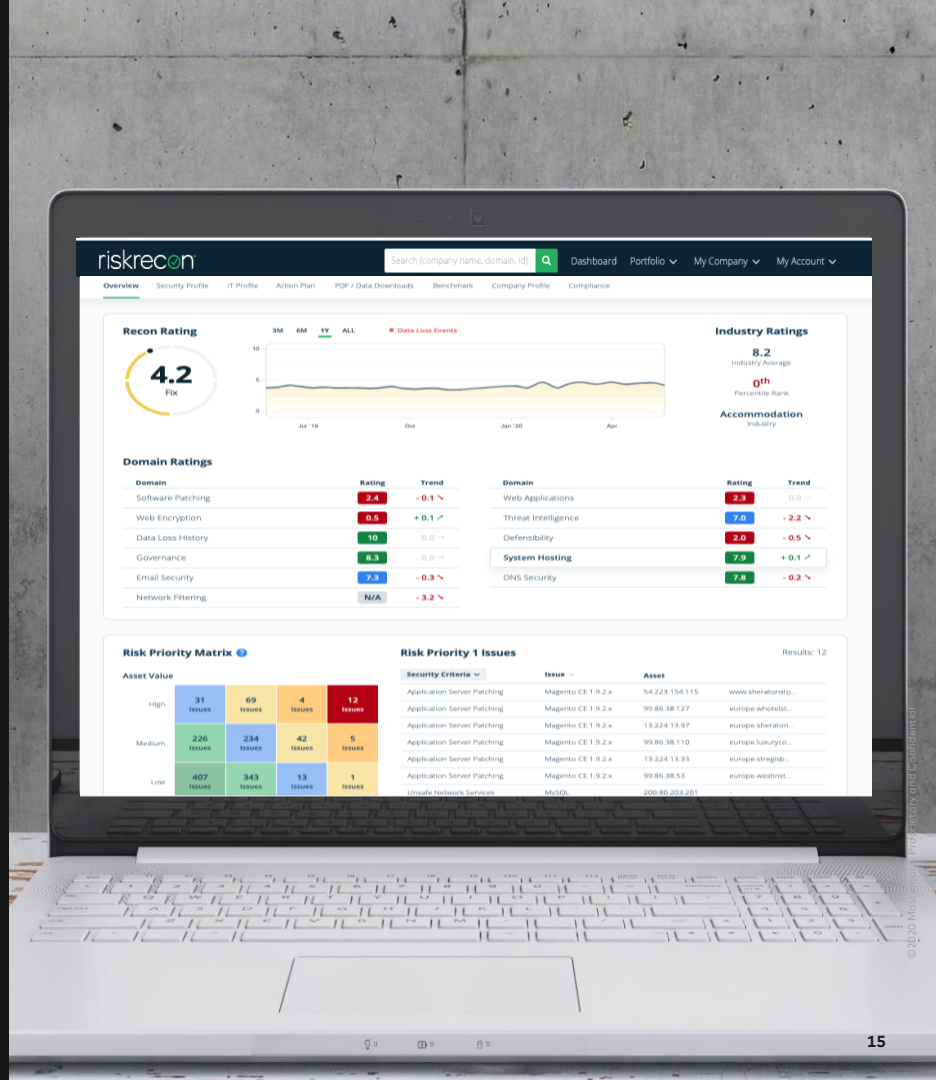
Underwriting & cyber risk premium calculation

Insurance contract offer with an adjusted premium

Signed insurance contact

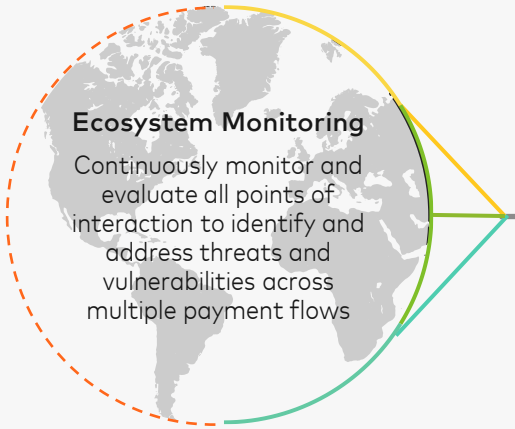
Pinpoint and prioritize cyber risk from third parties

- ✓ Aggregated **cyber risk score** for every third-party service provider and vendor based on the assessment of their cyber environment
- ✓ **Alerts** on issues exceeding risk thresholds, not just a general listing of all issues uncovered
- ✓ Downloadable **detailed reports** on all uncovered vulnerabilities
- ✓ **Benchmarking** of third-party service providers and vendors against standardized compliance frameworks and amongst one another
- ✓ **Actionable risk plans** are easily shared with third-party service providers and vendors using the collaboration portal



riskrecon
mastercard

Optimizing Connected intelligence across all payments



Ecosystem Monitoring

Continuously monitor and evaluate all points of interaction to identify and address threats and vulnerabilities across multiple payment flows

Identification

Broad spectrum of authentication and digital identity attributes to identify consumers

- **Consumer Authentication**
- **Device Authentication**
- **Account Verification**

Decisioning

Rules and machine learning to enable a decision based on the outputs of various applied capabilities

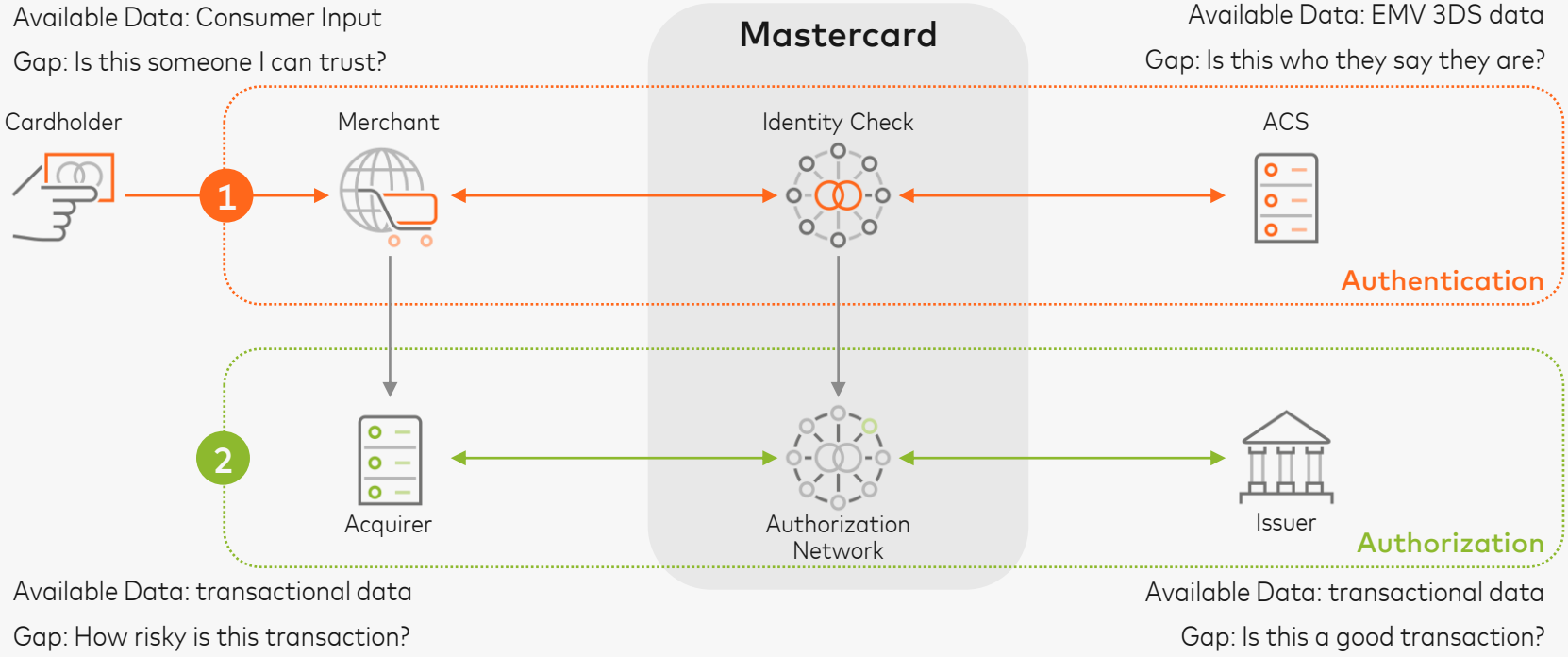
- **Transaction Decisioning (Fraud & AML)**
- **Account Decisioning**

Enhancement

Streamlined disputes and enhance transactions for a simple transparent consumer experience

- **Dispute Resolution**
- **Post-Transaction Enhancement**

The risk of the unknown – information gaps between issuers, merchants & acquirers lead to sub-optimal risk assessment and approval rates



Mastercard has a differentiated set of assets including Device-, Person- and Transaction-Intelligence, empowering our partners to make smarter decisions

Device Identity

Bot Detection, Good User Validation

Device Intelligence

Have we seen this device before?

Is this a known device or a device historically associated with fraud?

Person Identity

Synthetic ID & Thin File

PII Data & Risk Signals

Are these data elements linked to a genuine person?

Do we see fraudulent patterns in the usage of this data?

Transaction Identity

Authentication Insights

Transaction Data

Was this card used at many merchants at rapid succession?

Is this a suspicious merchant category?

Improve the user experience at checkout by accurately identifying the consumer device passively and leveraging rich network data

CNP Transaction Processing

Threats

Fraud Losses	False Declines	Adding unnecessary Fricition

Device Identity

Bot Detection, Good User Validation

Person Identity

Synthetic ID & Thin File

Transaction Identity

Authentication Insights

KEY FEATURES

Trust Network Data
Full access to traffic insights for real-time analysis

Risk Score
Used to validate good users or flag anomalies

Globally unique device ID
Resilient to software updates, cookie wipes, and major device changes

BENEFITS

1. **Reduce friction at checkout**
   Offer a simple, secure digital experience across the consumer journey
2. **Identify Fraud**
   Detect fraudulent activity before any losses occur
3. **Reduce operational cost**
   Prevent unnecessary – and costly – manual reviews and customer service inquiries

A bank removed friction on 91% of its trusted users

Bank mitigated +99% of the 250M threats in two weeks.

High-performing identity verification capabilities lower friction through real-time validity checks, risk scores and linkages to help you confidently make risk decisions

CNP Transaction Processing

Threats

- Fraud Losses
- False Declines
- Adding unnecessary Fricition

Device Identity

Bot Detection, Good User Validation

Person Identity

Synthetic ID & Thin File

Transaction Identity

Authentication Insights

Name — Email — Phone — IP — Address

KEY FEATURES

Validity Checks
Evaluates the authenticity of user input

Identity Risk Score
Built on combination of dynamic data across 5 core identity elements and their usage patterns

Reliability Assessments
Returns a risk signal on the combination of identity elements

Identity Network Score
Built on usage patterns of identity elements across real-world queries from our network

BENEFITS

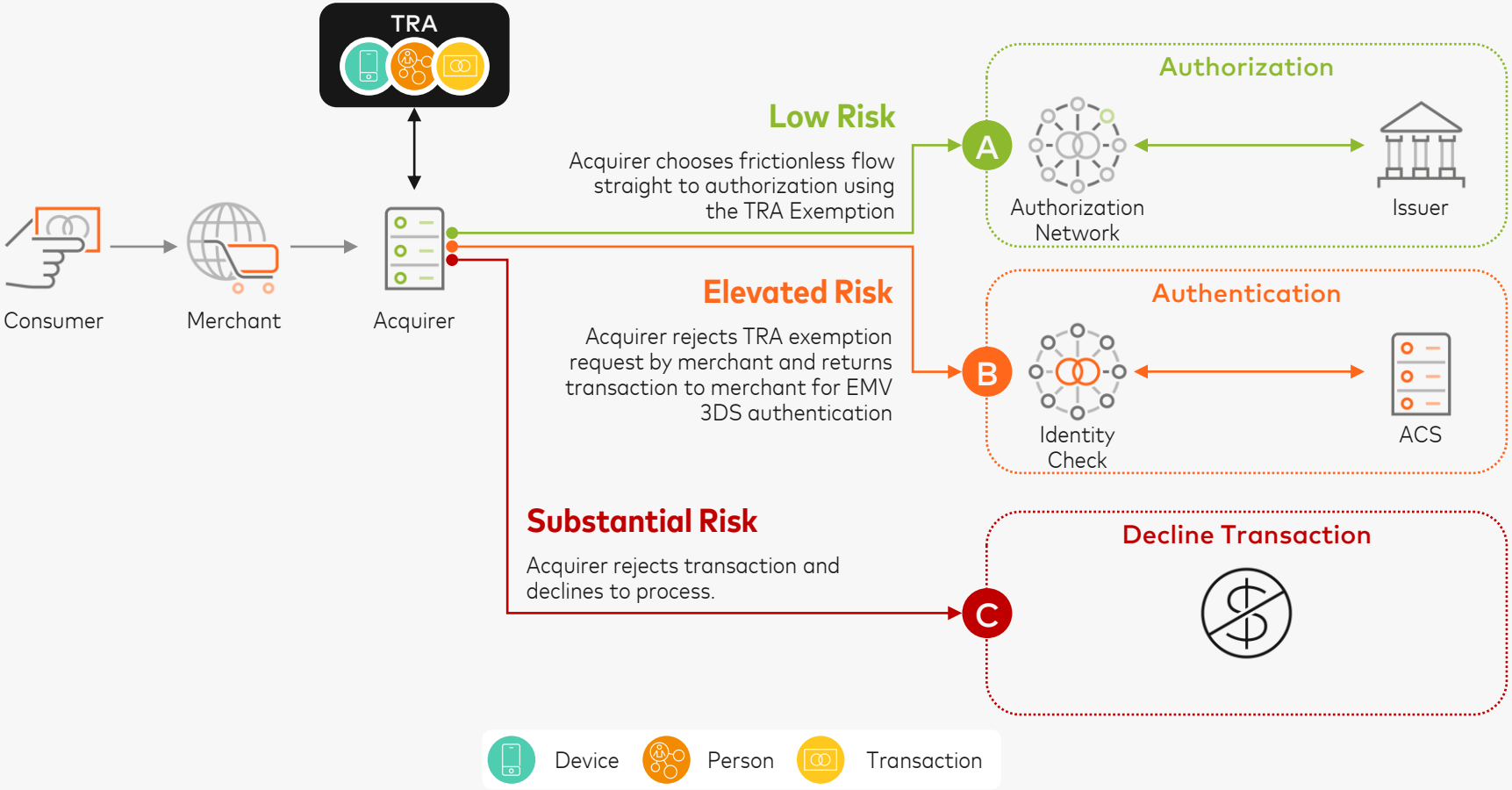
1. **Reduce friction at checkout**
   Stop losing good customers due to high friction or delayed fulfillment times
2. **Identify Fraud**
   Reduce chargeback rates and prevent other types of abuse
3. **Reduce false declines**
   Leverage authoritative and behavioral identity signals to unlock revenue from false declines

False positives can cost up to **10 x** the loss to fraud[1&2]

50% reduction in abandonment

1. Nilson Report 2019
2. Ekata internal research

Offer frictionless checkout to good users, while maintaining high security through actively validating the user's identity where elevated fraud risk is identified



Leveraging Device-, People- & Transaction Insights to drive more security and better user experience in digital payments

Reduce Fraud

Make real-time risk assessments to capture compromised identities and reduce abuse.

Reduce Friction

Stop losing good customers due to high friction. Make higher-fidelity identity decisions while requiring limited customer data

Drive Revenue

Improve revenue by growing successful transactions and reduced cost due to fraud losses

RiskRecon

POC

- Free-of-charge Proof of Concept (POC) – short scoping doc with company name, infos & some vendors you want to screen and we prepare the dashboard for you – our sales support helps you

Free Access

- Self testing the system with 30-days free testing access – you login and define up to 50 vendors - Get free access to the RiskRecon portal and see the security ratings of up to 50 vendors of your choice – our sales support helps you

LINK to get free access: Request a Demo | RiskRecon

EKATA

POC

- Free-of-charge Proof of Concept (POC) – you pass through your TRX-data and we tell you how much fraud we would have catched

Talk to us & test us

Contact Cyber & Intelligence Solutions:

Carsten Mürl
carsten.muerl@mastercard.com,
01723867787