# Enabling a seamless experience

For increased profitability

# Mastercard is evolving with the ecosystem…
# from securing transactions to protecting trust in every interaction

Continuously monitoring and evaluating all points of interaction to identify and address threats and vulnerabilities

**Digital** — Enhance security in the consumer digital transaction journey

**Financial** — Extend security to other types of transactions beyond cards
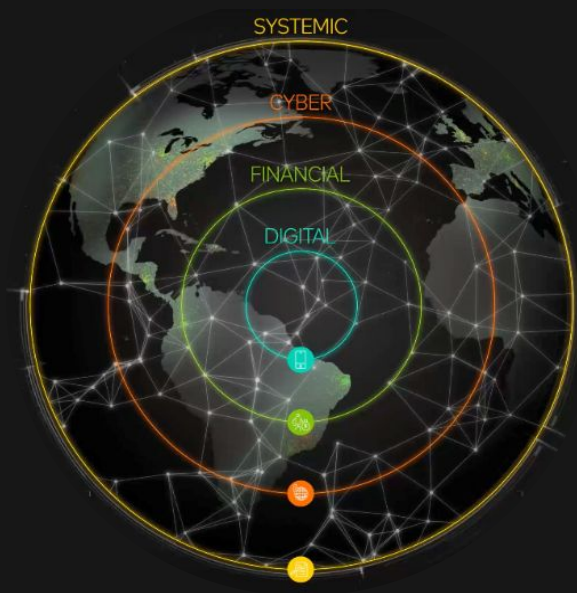
**Cyber** — Expand security beyond transactions to cyber environments

**Systemic** — Extend security to mitigate systemic operational risk

Protecting every transaction. Securing every interaction



SYSTEMIC
CYBER
FINANCIAL
DIGITAL

# Increased ecommerce spend opens opportunities for higher fraud and reputational risks

14% of attacks mimic human behavior that can **bypass bot-detection tools**[1]

Card-not-present fraud is forecast to rise **from $17.5B in 2020 to $31.3B in 2025**[3]

For every $1 in losses due to credit card fraud, merchants lose **$13 in false declines**[2]

**86% of customers are trusted** and deserve to be treated as such, with lower friction[1]
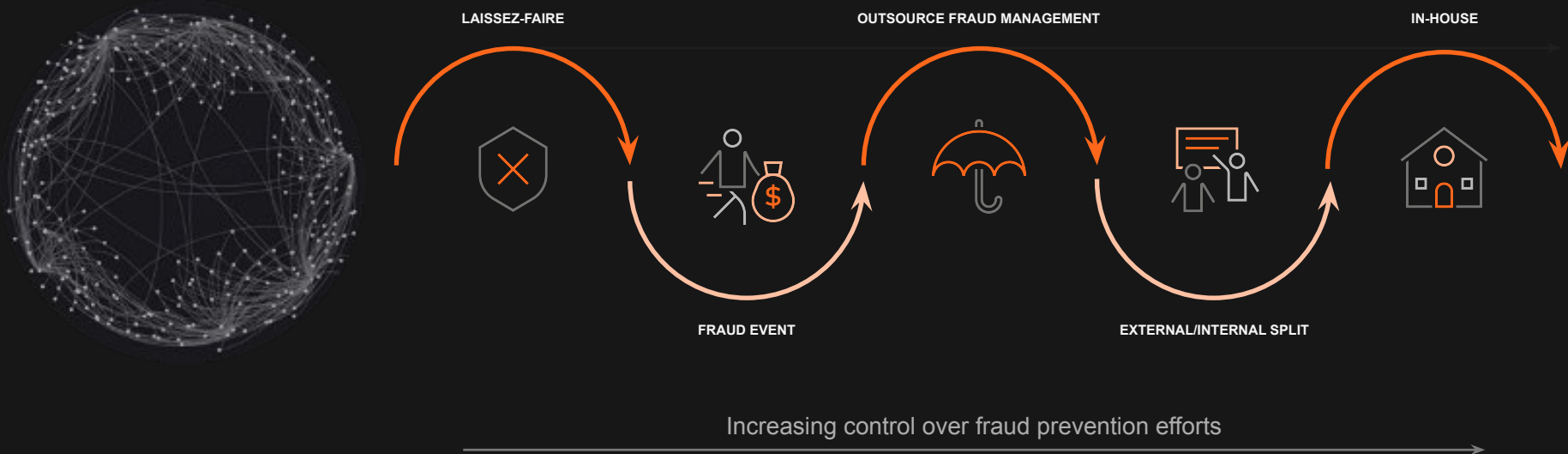
1. NuData, 2022
2. Sapio Research, 2020
3. Juniper Research, Online Payment Fraud:
   Deep Dive Data & Forecasting 2021–2025, 2021

# The ecosystem of fraud prevention is increasingly complex and allows retailers to manage with varying degrees of control

LAISSEZ-FAIRE

OUTSOURCE FRAUD MANAGEMENT

IN-HOUSE

FRAUD EVENT

EXTERNAL/INTERNAL SPLIT

Increasing control over fraud prevention efforts

# Mastercard offers a wide range of Cyber & Intelligence solutions to address pain points across the customer journey

**Account Creation** → **Login** → **Checkout** → **Customer Service** → **Ecosystem Protection**

## Key Challenges

- Increasing sophistication of fraud (e.g. CNP/device fraud, bot attacks, account takeover)
- Fraudulent accounts (e.g. bots, synthetic IDs)

- Evolving industry standards for authenticating cardholders
- Inability to detect identity data discrepancies and abnormal user behavior

- Low approval rates and false declines
- Cart abandonment
- Losing good customers due to high-friction processes

- Back-office costs and resources associated with processing chargebacks and disputes
- Lengthy dispute resolution process

- Enterprise-wide threats (e.g. ransomware attacks, data breaches)
- Lack of visibility into risk exposure from third-party partners
- Supply chain disruptions

## Mastercard C&I Capabilities

**Customer Retention**

Verify good users with minimal friction across account lifecycle

**Reduce Fraud Costs**

Increase approval rates while preventing fraudulent transactions

**Chargebacks/Disputes**

Prevent and manage chargebacks and minimize loss of revenue and reputation

**Operational Resilience**

Proactively monitor and assess enterprise-wide risk

# Mastercard can help to achieve business goals through tailored solution sets that address specific pain points

## Customer Retention

Synthetic Fraud

Account Takeover

Increase Approval Rates
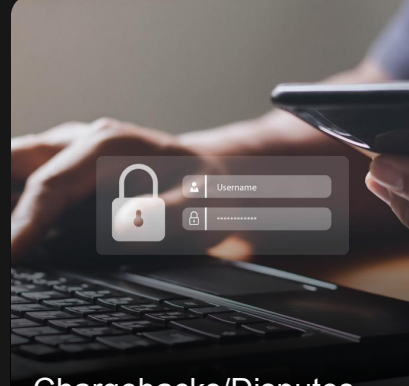
Reduce Friction

Identity Insights

Authentication

NuDetect
Ekata
Brighterion

## Reduce Fraud Costs

Third Party Fraud

Stolen Credit Card/Credentials

Loyalty Fraud

Card Testing Fraud

Payment Insights

NuDetect
Ekata
Brighterion

## Chargebacks/Disputes

First Party Fraud/Friendly Fraud

Refund Fraud

Post Transaction Enrichment

Dispute Resolution

Improve Consumer Experience

Ethoca Alerts
Ethoca Consumer Clarity

## Operational Resilience

Ransomware Attacks

Assess Cyber Risk

Third Party Vendor Assessment

Network Protection

Security and Infrastructure Assessment

Impact Analysis

RiskRecon
Systemic Risk Assessment

# How Mastercard can support you

99% fraud ring identification with precision via account opening solutions[1]

A luxury retailer prevented $7.5M of fraud 12k+ disputes in one year of implementation[2]

32% of good customers identified with 97% precision by leveraging identity data[1]

Analysis of one customers' third-party service providers identified 10% as high-risk[3]

1. Ekata Case Study, 2022
2. Ethoca Case Study, 2022
3. RiskRecon Internal Analysis, 2019

# Want to know more?

Mastercard is committed to identifying how to maximize profitability

For more information contact:


Laura Iannelli
laura.Iannelli@mastercard.com

# Appendix

# Focus on the consumer behind the device

NuDetect helps trust good users, recognize them once they become consumers, and secure their accounts from harm.

Behavioral insights

Device intelligence

Trust network data

**RISK SCORE**

Account opening

Create Account
username
password

Account access and update

Login
username
password

Checkout

Checkout

# Drive results by making better decisions

### 1-to-1 behavioral insights
Assessment of users against their expected normal behavior.

### 1-to-many behavioral insights
Evaluation of user behavior against normal population.

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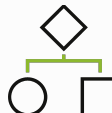Resilient to software updates, cookie wipes, and major device changes.

### Risk score
Used to validate good users or flag anomalies.

### Intelligence portal
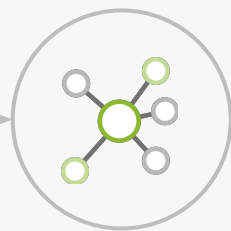Full access to traffic insights for real-time analysis.

### Customized security
Combination of built-in and tailored rules for optimal results.

# Real-time assessment for a tailored consumer experience

- Account sign-up
- Account access
- Profile update
- Purchase

NuDetect real-time score for each use case

## What we provide

LOW/NO RISK

MEDIUM RISK

HIGH RISK

## What clients can do

- Remove additional friction
- Bypass a manual review
- Build a tailored user experience

- Automate a custom authentication step-up for further verification

- Require a manual review
- Reject the request
- Flag the account for future interactions

# Help consumers enjoy a tailored experience in a safer environment

See the
proof points

→

**1** Improve the user experience
Offer a simple, secure digital experience across the consumer journey.

**2** Drive revenue
Reduce fraudulent purchases and preserve the consumers' lifetime value.

**3** Decrease fraud
Prevent unnecessary – and costly – manual reviews and customer service inquiries.

**4** Reduce operational costs
Detect fraudulent activity before any losses occur.

# How a merchant preserved a seamless user experience during an attack

## Context and challenge

Ensure the merchant's trusted consumers were undisturbed while the company mitigated constant attacks that bypassed bot-detection tools.

## Approach

Leverage NuDetect's behavioral and device insights to flag risk and identify trusted traffic.

1. Risky traffic incorrectly flagged as non-risky. The affected accounts were shared with the client for remediation.

## 0%
of trusted users impacted

### Result
The merchant successfully maintained a good experience for its trusted consumers.

## 99.9%
Mitigation rate

## 0.01%
False-negative rate[1]

# Ekata's verification builds trust by delivering increased conversion in digital onboarding

## Increase Passive Authentication

Predictive signals enable reduced step-up friction, streamline KYC checks and exceed expectations of good customers
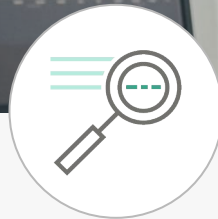
## Mitigate Synthetic Identity Fraud

Use real-time assessments to capture compromised identities that traditional KYC processes may miss — and prevent credit bust-outs before losses happen
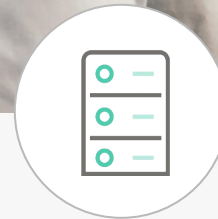
## Onboard Thin-File and Unbanked

Leverage predictive data to confidently convert customers with limited financial history from internal or traditional credit or other sources

EKATA
mastercard

# Ekata's data and risk indicators help you know your customer and how their information is being used online — not just in the financial services ecosystem

Name

Email

Phone

IP

Address

## Validity of identity elements

- Does this email belong to the person?
- Is this address valid? Is it residential?
- What type of phone number is this?

## How they are used online

- When was this email first/last used?
- How many times has this address been used?
- Why are there 50 IP addresses associated with a single phone number?

EKATA
mastercard

# Ekata relays real-time validity checks, risk scores and linkages to help you confidently make risk decisions

**Validity Checks**
Evaluates the authenticity of user input that is provided by the applicant.

**Identity Risk Score**
Built on the combination of dynamic data across five core identity elements and their usage patterns.

**Network Signals**
Catches most recent activity of an identity element to determine its riskiness.

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

**Reliability Assessments**
Returns a risk signal on the combination of identity elements to confirm usage consistency.

**Scalability**
Flexibility to support massive volume requirements while reliably retaining low latencies.

EKATA
mastercard

Ekata streamlines the digital onboarding process by providing
real-time data to confidently perform risk assessments and apply more or less friction dynamically

**Applicant**

**Ekata solution**

**Verified identities**

Low-friction experience
• Limited to no step-up authentication

**Potential risk**

Medium-friction experience
• Step-up authentication for further verifications

**Suspected fraud**

High-friction experience
• Document requests and manual reviews

EKATA
mastercard

# Provide good consumers with a frictionless account opening experience

Create loyalty, opportunity and inclusion while lowering acquisition costs.
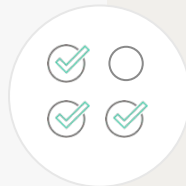
### Passive validation of applicants

Reduce the number of good customers that are challenged to provide additional documentation.
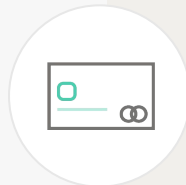
### Improve thin-file consumers' experiences

Go beyond traditional credit checks to identify good thin-file customers without costly friction — and with lower overall acquisition costs.

### Detect synthetic identities

Flag compromised identities and fraud often missed in traditional KYC processes before incurring revenue loss.

**EKATA** mastercard

# Decrease friction and increase conversion

### Customer

- Global financial services company

### Customer problem

- Too many good customers going through high friction processes
- All customers sent through the same KYC process
- Concerns about level of application conversions due to poor customer experience

### Result
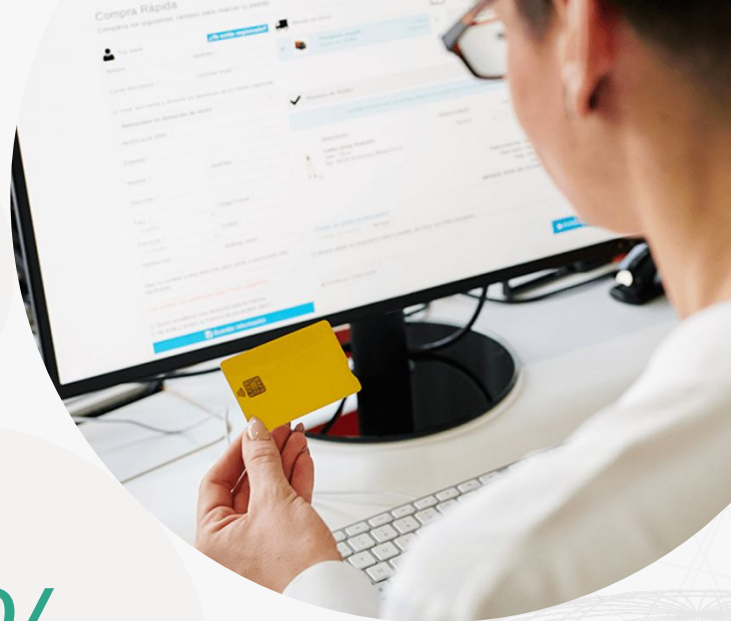
- Empowered the merchant to define KYC processes each customer would undergo according to risk profile

# 60%
increase in passive verifications

# 50%
reduction in abandonment

EKATA
mastercard

# Improve bad user detection

### Customer
- A payday loan company

### Industry
- Payments

### Customer problem
- Fraudulent users were able to open new accounts
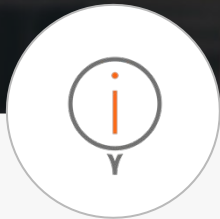- Desire to catch bad users earlier in the account opening flow

### Result
- Improved ability to catch bad users (fraudulent and defaulters) at account opening

# 15:1
# ROI

# Maximize approval rates and fight payment fraud in every transaction, providing consumers a better validation experience

## Flag fraudulent transactions in the shopping cart

Ekata data plays a key role in pre-authorization flows, where it can be used to mark a potential transaction on an account.
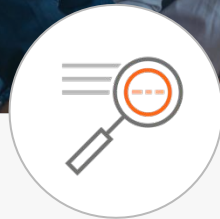
## Assess rejected transactions in real time

Ekata data may be used during transaction processing to identify true fraud or falsely declined good customers, literally adding revenue to the bottom line.

## Efficient and effective manual review

After authorization, questionable transactions may be flagged based on Ekata risk indicators and sent to manual review for investigation.

# The Five Key Identity Elements

Ekata's data and risk indicators help you know who your customer is and how their information is being used online — not just in the e-commerce ecosystem

**Name**

**Email**

**Phone**

EKATA: MERCHANT

**IP**

**Address**

## Validity of identity elements

- Does this email belong to the person?
- Is this address valid? Is it residential?
- What type of phone number is this?

## How they are used online

- When was this email first/last used?
- How many times has this address been used?
- Why are there 50 IP addresses associated with a single phone number?

# Ekata relays real-time validity checks, risk scores and linkages to help you confidently make risk-oriented decisions

**Validity Checks**
Evaluates the authenticity of user input that is provided by the applicant.

**Identity Risk Score**
Built on the combination of dynamic data across five key identity elements and their usage patterns.

**Network Signals**
Catches the most recent activity of an identity element to determine their riskiness.

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

**Reliability Assessments**
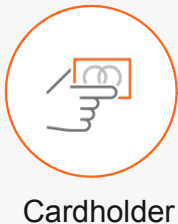Returns a risk signal on the combination of identity elements to confirm usage consistency.

**Scalability**
Flexibility to support massive volume requirements while reliably retaining low latencies.
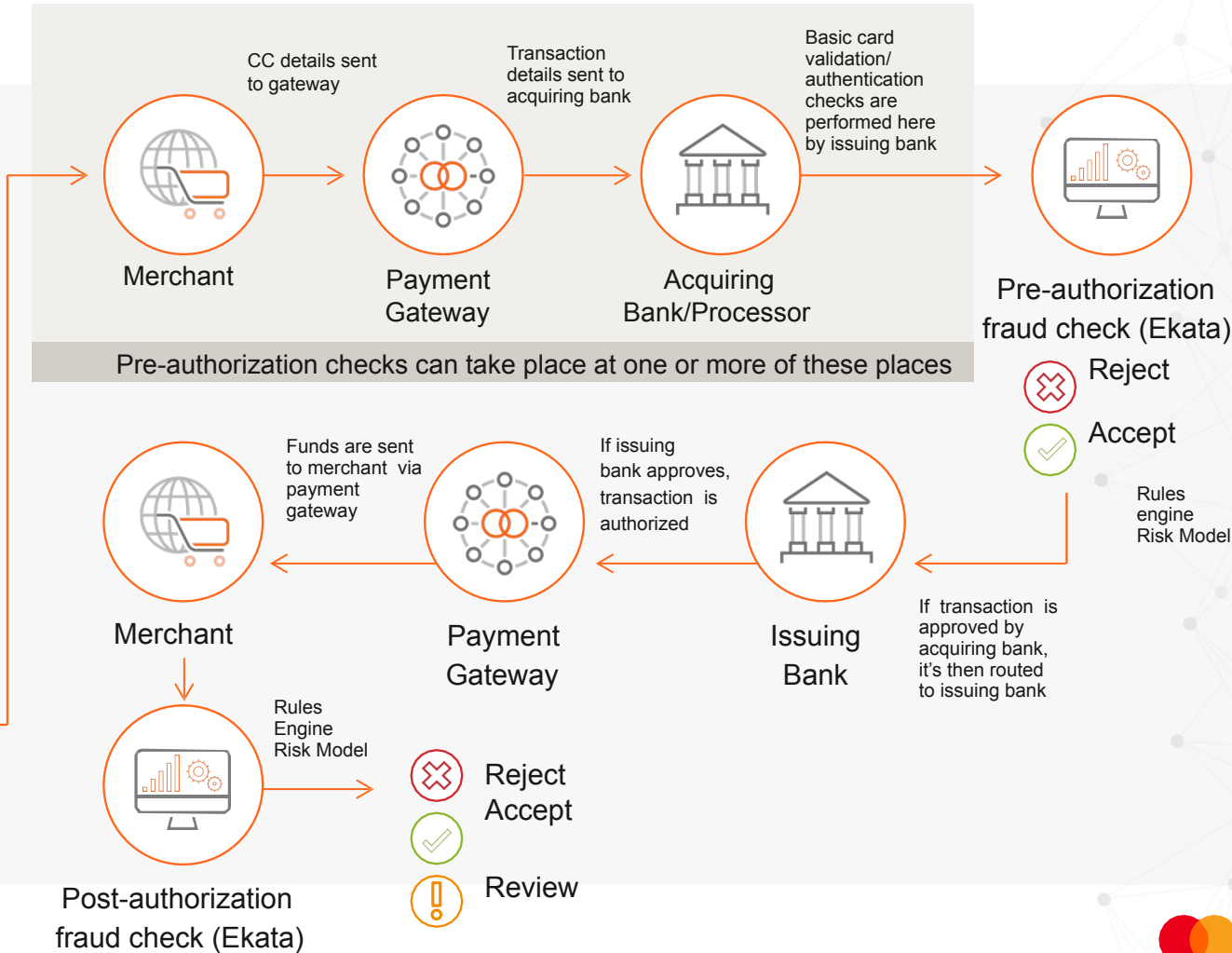
Ekata is versatile
in both pre- and post-
authorization and works  in
both manual and
automated transaction
approval workflows

**The chart is a simplified, theoretical representation of where Ekata's transaction solution might be used. As each customer's workflow will be unique, their workflows will differ greatly.**

Cardholder

CC details sent
to gateway

Merchant

Transaction
details sent to
acquiring bank

Payment
Gateway

Basic card
validation/
authentication
checks are
performed here
by issuing bank

Acquiring
Bank/Processor

Pre-authorization
fraud check (Ekata)

Reject

Accept

Rules
engine
Risk Model

**Pre-authorization checks can take place at one or more of these places**

Funds are sent
to merchant  via
payment
gateway

Merchant

If issuing
bank approves,
transaction  is
authorized

Payment
Gateway

Issuing
Bank

If transaction  is
approved by
acquiring bank,
it's then routed
to issuing bank

Rules
Engine
Risk Model

Post-authorization
fraud check (Ekata)

Reject

Accept

Review

# Provide good consumers with a frictionless shopping experience and reduce payment fraud

## Customer friction

Stop losing good customers due to high friction or delayed fulfillment times. Make higher-fidelity identity decisions while requiring limited customer data.
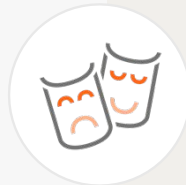
## Identity fraud/abuse

Make real-time risk assessments to capture compromised identities to reduce chargeback rates and prevent other types of abuse.

## False declines

Leverage authoritative and behavioral identity signals to unlock revenue from false declines.

# Prevent fraud attacks and reduce manual review rate

## Customer

- Crowdfunding platform

## Customer problem

- Fraudulent campaigns cause fraud loss and reputational damage
- Extremely reticent to reject any good customers
- Manual review rate too high to keep up with

## Result

- Reduced fraud capture rate at sign up by 8x and reduced review rate by 50%

# 8x
Fraud capture rate at sign up

# 50%
reduction in review rate

# Ethoca Consumer Clarity™

Ethoca Consumer Clarity allows merchants to provide rich purchase information to cardholders within their banking application and to financial institutions for call centre and back-office agent use.

Merchants can eliminate transaction confusion, significantly reduce unnecessary disputes and chargebacks and mitigate fraud losses by sharing information into both digital and call centre channels.

For consumers, this includes easy-to-recognise information such as logos, itemised digital receipts, carbon footprint estimates and more. Plus, information is delivered on-demand through secure and trusted issuer channels.

*Includes all major card brands.

ethoca
by

# Ethoca Consumer Clarity™ shares purchase information with multiple issuer channels
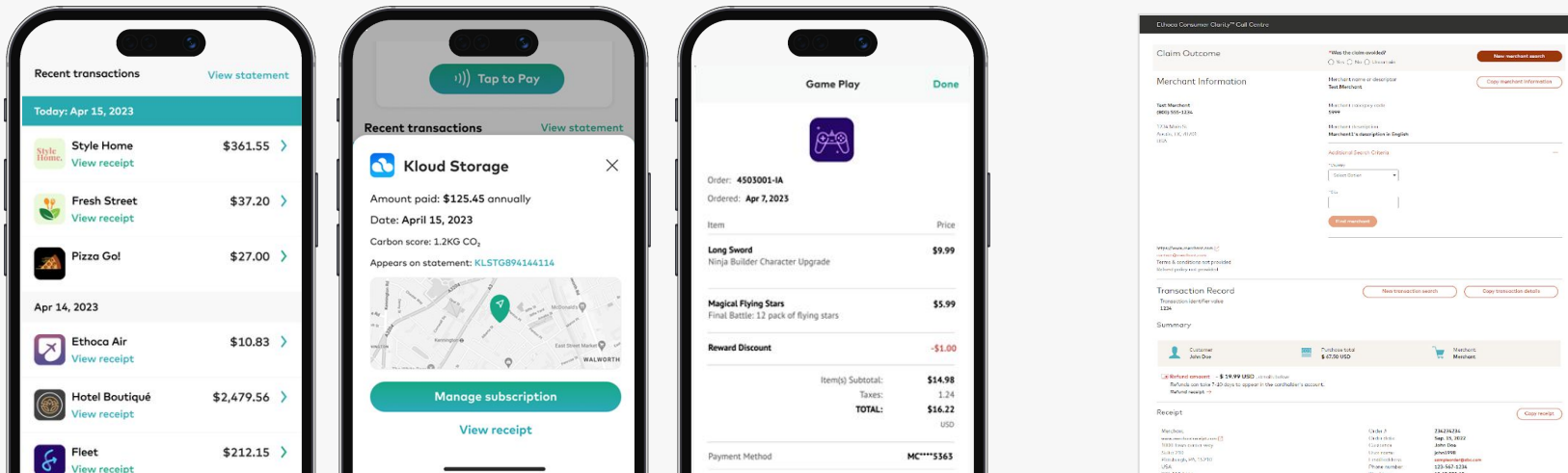


## Digital banking channels

Merchants can provide details like clear logos and digital receipts for use in digital bank channels to help improve clarity. Issuers also have access to additional details like cleansed merchant names, carbon footprint estimates and subscription controls to enhance their digital bank channels and reduce disputes.

## Call centre and back office

Empower issuer call centre and back-office teams with relevant purchase details to address cardholder enquiries.

ethoca
by

# Merchant details

Give consumers convenient access to your merchant details such as a clear logo and geolocation within their banking app for simple purchase recognition

Eliminate confusion caused by unclear descriptors and provide clear **merchant names**

Provide ease-of-purchase recognition with visual cues such as **merchant logos**

Share **merchant geolocation\***: latitude and longitude details enable issuers to display maps
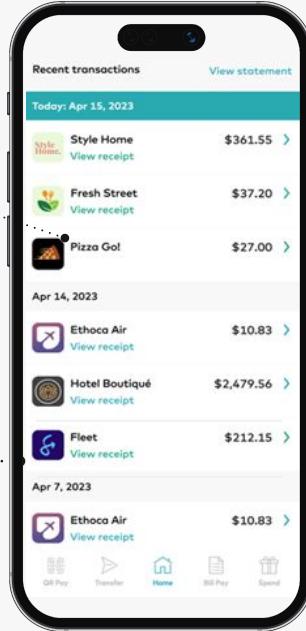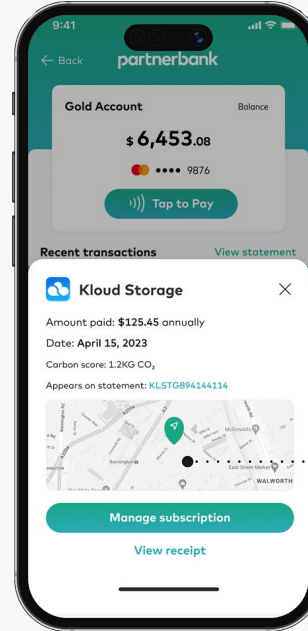
**Transaction list**
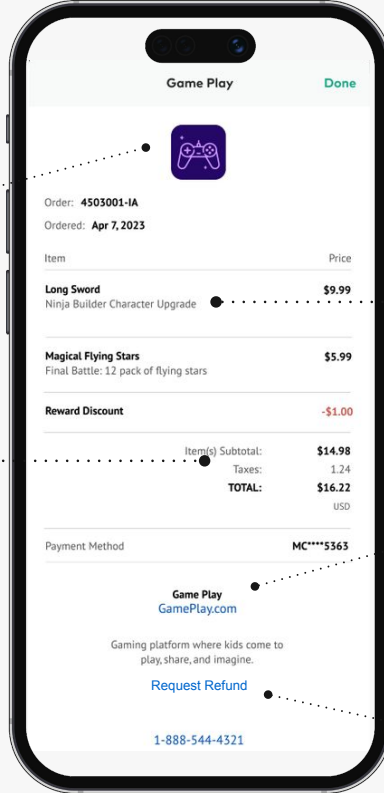
**Individual transaction view**

*Most precise information based on availability.

ethoca
by

# Digital receipts

Provide your customers with convenient access to digital receipts within their digital banking app

**Issuer-branded** interface; **no third-party** messaging

Remove confusion caused by unclear costs with **itemised details** (e.g., taxes and shipping charges)

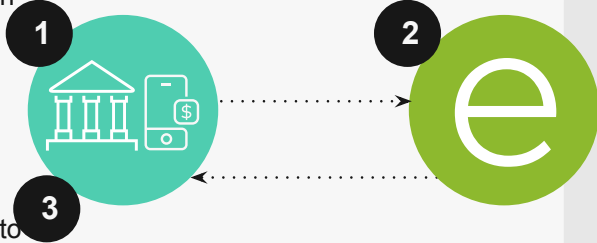Provide description of **purchased items** for easy recall

Facilitate direct merchant contact by providing **address, phone number, email or web URL information**

Enable direct merchant interaction with specific cardholder options such as **view order details, request a refund, buy again or write a review** using embedded links

Game Play — Done

Order: 4503001-IA
Ordered: Apr 7, 2023

| Item | Price |
|---|---|
| Long Sword<br>Ninja Builder Character Upgrade | $9.99 |
| Magical Flying Stars<br>Final Battle: 12 pack of flying stars | $5.99 |
| Reward Discount | -$1.00 |

Item(s) Subtotal: $14.98
Taxes: 1.24
TOTAL: $16.22
USD

Payment Method     MC****5363

**Game Play**
GamePlay.com

Gaming platform where kids come to
play, share, and imagine.

Request Refund

1-888-544-4321

Based on information provided by merchant.

ethoca
by [Mastercard]

# Ethoca Consumer Clarity: How purchase data is shared with cardholders

**Ensuring data privacy:** Purchase information is never stored with card issuers or networks. This ensures the highest level of privacy and security.

Cardholder views their purchases online or in their banking app.

**1**

**2**

Ethoca retrieves the required purchase information based on the issuer's implementation and cardholder's transactions.

**3**

Details are sent back to cardholders in real time, helping them recognise their purchases. Confusion is eliminated and a dispute or chargeback is avoided.

Merchants can provide their logo to be used with **merchant details**, to enable the provision of cleansed descriptors and geolocation details.

Ethoca retrieves in-depth transaction details directly from merchants. **Digital receipts** are shared directly with cardholders and not stored on issuer's systems.

Direct merchant interaction is enabled allowing the cardholder to **view order details, requesting a refund, buy again or write a review** using embedded links.

Merchants can participate by providing information like their logo or digital receipt details for use in digital banking channels. Issuers can display this information provided by the merchant alongside additional insights like carbon footprint estimates or subscription controls that are supplied through third-party providers.

ethoca
by
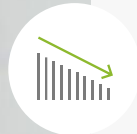
# Ethoca Consumer Clarity: Merchant benefits

## Reduce friendly fraud
Provide purchase clarity to remove upfront confusion and eliminate invalid disputes

## Eliminate revenue loss
Consumer purchase recognition eliminates unnecessary refunds and revenue loss

## Reduce chargeback costs
Avoid unnecessary chargebacks from friendly fraud and customer disputes

## Increase acceptance
Prevent spending disruption and increase acceptance as issuer fraud models improve
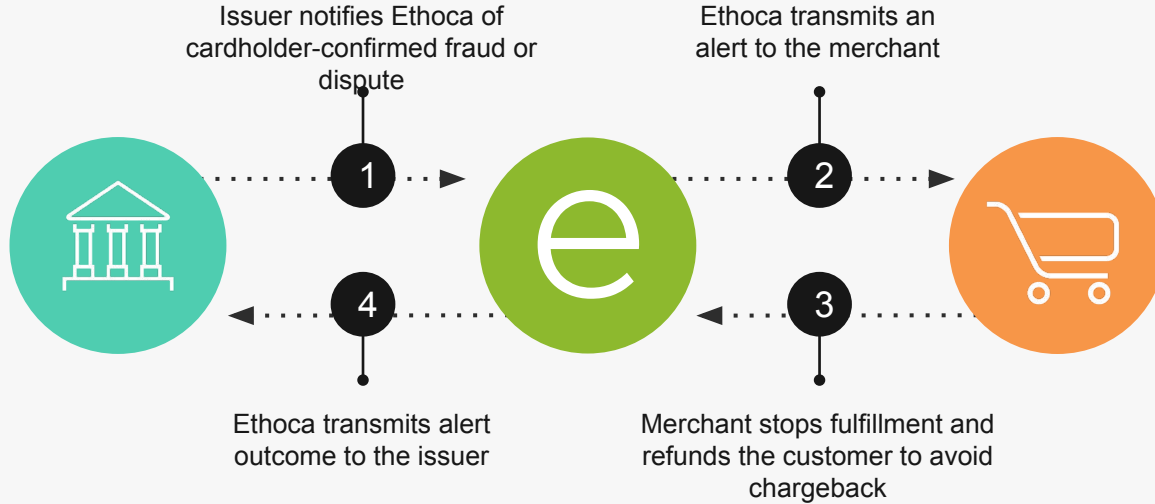
## Engage consumers
Redirect disputes from issuer to merchant by providing clear contact information

ethoca
by

# Ethoca Alerts

Ethoca Alerts reduces the time it takes for merchants of all types and sizes to be alerted of confirmed fraud and disputes. This gives them a unique window of opportunity to halt the fulfillment of goods and services, refund customers and stop chargebacks before they happen.

# Ethoca Alerts: How actionable issuer information is shared with merchants quickly

Issuer notifies Ethoca of cardholder-confirmed fraud or dispute

**1**

Ethoca transmits an alert to the merchant

**2**

**4**

**3**

Ethoca transmits alert outcome to the issuer

Merchant stops fulfillment and refunds the customer to avoid chargeback

### With Ethoca Alerts, merchants can…

- stop the order/suspend the service

- process a refund or credit back to customer (eliminating the need for a chargeback)

- attempt to identify more fraudulent transactions through link analysis

- update fraud rules to prevent future fraud

ethoca
by

# Ethoca Alerts: Merchant benefits

## Fight fraud
Take action to stop the fulfillment of fraudulent orders before it's too late

## Prevent chargebacks
Eliminate chargebacks and reduce related costs

## Increase acceptance
Issuing refunds promotes higher acceptance and improves the customer experience

## Reduce future fraud
Bolster fraud screening to identify future fraud and prevent spikes

## Find related fraud
Use link analysis to eliminate related fraudulent orders

## Improve satisfaction
Customers no longer need to go through the long and frustrating chargeback process

ethoca
by

# RiskRecon helps you to effectively assess cyber risk from third-party business relationships

RiskRecon proactively monitors the cyber environment of any entity with an online presence to identify cyber risks and vulnerabilities before they can be exploited.

By effectively assessing cyber risk from third parties, organizations can ensure they do not fall victim to cyber attacks from the risks incurred through their business relationships.

riskrecon
by

# Pinpoint and prioritize cyber risk from third parties

✔ Aggregated cyber risk rating for every third-party service provider and vendor based on the assessment of their cyber environment

✔ Alerts on issues exceeding risk thresholds along with in-portal viewing and alert management through the Alert Management Center

✔ Downloadable detailed, summary and executive summary reports on overall organization cyber risk profile on demand

✔ Benchmarking of third-party service providers and vendors against standardized compliance frameworks and amongst comparable competitors

✔ Actionable risk plans are easily shared with third-party service providers and vendors using the collaboration portal

✔ View of organization's cyber risk visibility to their extended supply chain of fourth-party providers

✔ Aggregated systemic risk* scores evaluated across all business relationships for financial, ESG, and operational risk dimensions via Mastercard Systemic Risk Assessment (additional systemic risk dimension scores available through Systemic Risk Assessment)
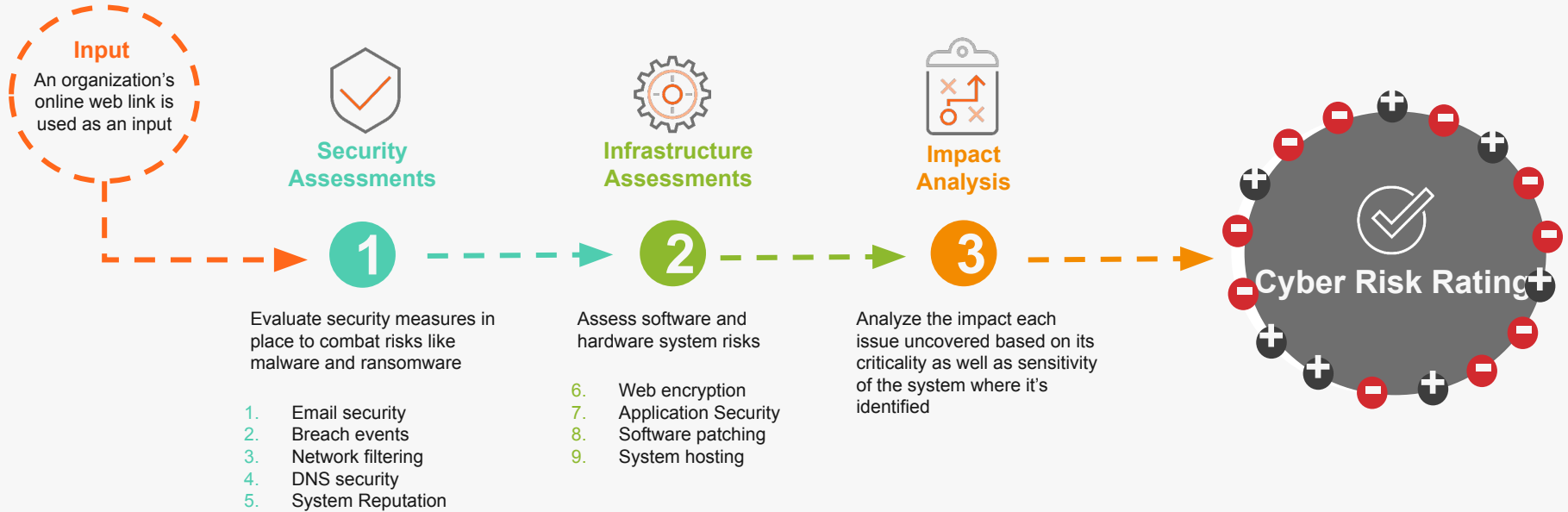
*Systemic risk refers to the risk of a cascading failure, caused by linkages within the financial system, resulting in significant business impact.

riskrecon by (Mastercard)



**DID YOU KNOW?**

Companies with cyber risk rating of 'F' are 4x more likely to experience a data loss event according to RiskRecon analysis.

FOR ILLUSTRATIVE PURPOSES ONLY
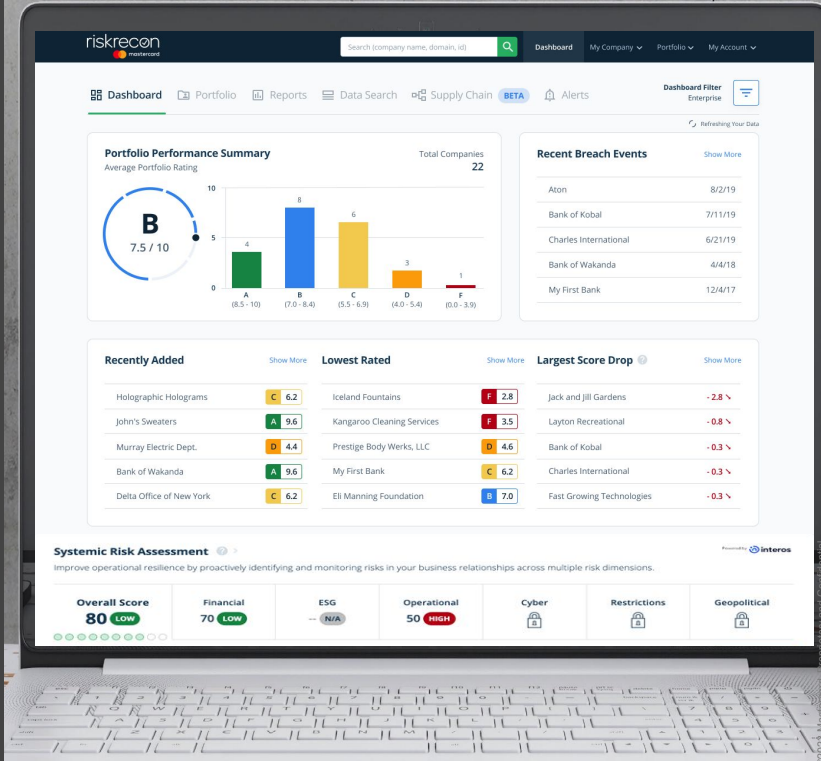
# How is the cyber risk rating determined?

The cyber risk rating is determined by evaluating over 40 criteria across 9 security domains. The impact of all vulnerabilities is analyzed to produce the cyber risk rating.

**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. Breach events
3. Network filtering
4. DNS security
5. System Reputation

**Infrastructure Assessments**

**2**

Assess software and hardware system risks

6. Web encryption
7. Application Security
8. Software patching
9. 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

**Cyber Risk Rating**

riskrecon
by

# Accurate and reliable cyber risk assessments help you reduce losses while saving time and resources

**Reduce financial losses from third-party cyber risk**
Advanced third-party assessments at an affordable price ensure your cyber environment is not in danger of compromise

**Gain greater control and flexibility managing third-party cyber risk**
Cyber risk assessments can be performed as often as needed on as many third and fourth-party service providers as needed

**Save time and resources managing third-party cyber risk**
Automated third-party risk assessments reduce the time taken and the number of manual resources needed to monitor third-party cyber risk

**Obtain more reliable, accurate assessments of third-party cyber risk**
Accurate and verifiable data of third parties collected from public domains ensures cyber risk assessments are completely reliable

**Realize a new line of revenue**
Additional revenues from offering My Cyber Risk to your small and medium business customers, competitively priced to encourage awareness of cyber risk in their environments, which ultimately reduces the cyber risk to your business

riskrecon
by

# RiskRecon assists Fortune 500 financial institution in identifying critical threats from high-risk vendors

## Context & Challenge

A Fortune 500 financial institution was challenged with identifying and prioritizing high-risk cyber threats from vendors. As a result, they spent time investigating non-critical issues, leaving significant critical cyber risk issues unnoticed and unresolved.

## Approach

Effortlessly integrated into the financial institution's workflow, RiskRecon accurately alerted the institution to critical threats for high-risk vendors based on set risk severity thresholds.

riskrecon by

# Results

## 50%
risk reduction in over 3 years

## $630K+
annual savings across people, process and technology

*RiskRecon's continuous monitoring and prioritization of third-party vendor risk helped the financial institution to identify critical issues on a regular basis—enabling quick remediation of severe threats in a timely and consistent manner.*

# Account Protection

Mitigates fraud in real time and verifies good users across an account lifecycle, ensuring an end-to-end seamless digital experience for your customers

## Identification

**Deploy behavioral analytics to evaluate customer's identity and ensure a frictionless experience**

**Leverage identity analytics and verify consumer attributes and documentation**

## Decisioning

**Check consumer financial credit risk**
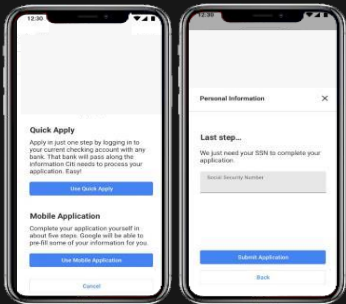


| **Monitor** | **Identify** | **Authenticate** | **Assess** | **Detect** | **Verify** | **Capture** | **Evaluate** | **Reduce** |
|---|---|---|---|---|---|---|---|---|
| Users and Devices | Abnormal User Behavior | Users with Behavioral Biometrics | Consumer Identity Data | Identity Data Discrepancies | Consumer Attributes | Consumer Income/Asset Employment | Consumer Credit Risk | Credit Delinquency |

**Solution Benefits**
Enable Ecosystem Trust • Fraud Prevention • Optimized Customer Experience
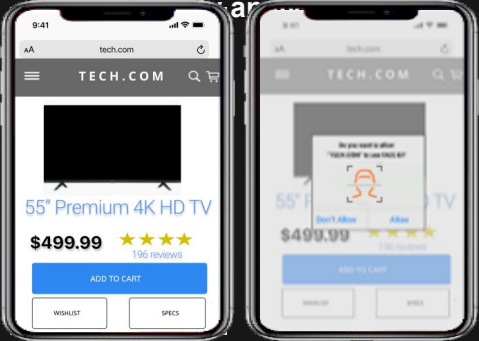
# Transaction Optimizer

Provides an end-to-end view of each transaction, helping you better authenticate users and evaluate transaction risk to enhance decisioning

## Identification

**Proactively manage account continuity and customer identity using behavioral and identity analytics**



| Identify | Maximize | Verify |
|---|---|---|
| Abnormal User and Device Behavior | Account Continuity | Consumer Attributes |

## Decisioning

**Prevent fraudulent approvals and make informed decisions by incorporating account and transaction intelligence into your decisioning flow**
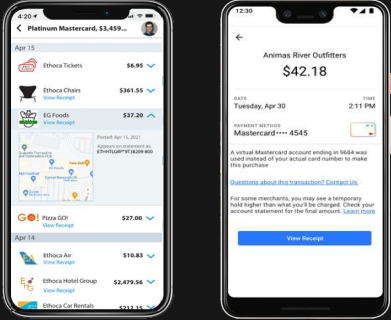


| Assess | Integrate | Optimize |
|---|---|---|
| Payment Transaction Data | Transaction Fraud Rules | Approvals and Declines |

## Enrichment

**Prevent/manage chargebacks and minimize the loss of revenue and reputation**



| Reduce | Optimize | Leverage |
|---|---|---|
| Friendly Fraud and Chargebacks | Consumer Digital Experience | Transaction Insights |

**Solution Benefits**
Consumer Identity Verification • Approval Rate Optimization • Fraud Mitigation • Operational Efficiency
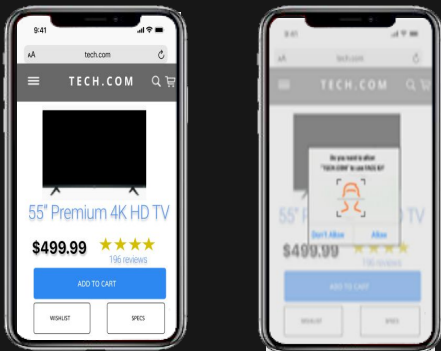
# CX and Loss Mitigation

Make every touchpoint seamless and secure by reducing your organization's operational costs from fraud/chargebacks without compromising the customer journey

## Identification

**Proactively manage account continuity and effectively authenticate payment data**
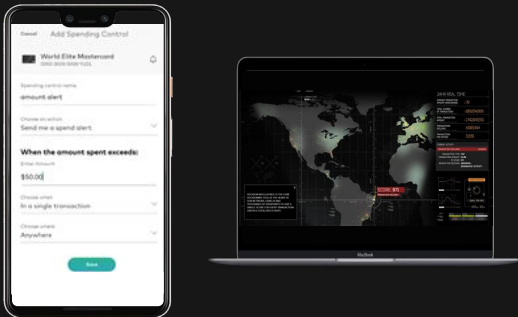


| **Maximize** | **Assess** | **Enable** |
|---|---|---|
| Account Continuity | Payment Transaction Data | Spending Alerts and Controls |

## Decisioning

**Empower consumers with account controls and make informed transaction decisions**



| **Prevent** | **Maximize** | **Mitigate** |
|---|---|---|
| Fraudulent Transactions | Genuine Transaction Approvals | Fraud-Related Operational Expenses |

## Enrichment

**Prevent/manage chargebacks and minimize the loss of revenue and reputation**
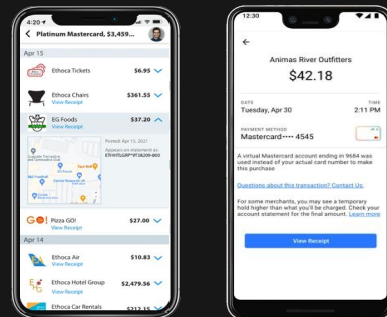


| **Reduce** | **Optimize** | **Leverage** |
|---|---|---|
| Friendly Fraud and Chargebacks | Consumer Digital Experience | Transaction Insights |

**Solution Benefits**

Consumer Identity Verification • Customer Experience • Fraud Mitigation • Operational Efficiency

# Cyber Risk Management

Mitigates cyber threats within your organization and across your business relationships, ensuring persistent security for your customers and uninterrupted operations for your business

## Identity Theft Protection
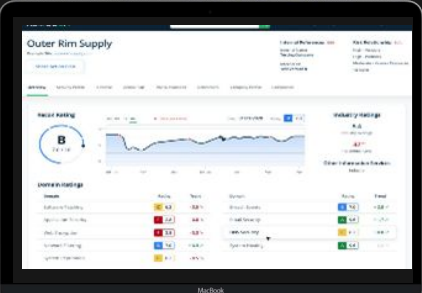
**Alert and remediate identity theft exposure**



| Detect | Alert | Resolve |
|---|---|---|
| Identity/Credit Fraud | Suspicious Activity | Identity Threats |

## Cyber Threat Protection

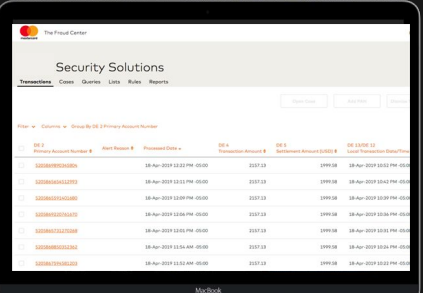**Gain visibility into your cyber vulnerabilities as well as risk exposure from third-party partners**



| Scan | Evaluate | Mitigate |
|---|---|---|
| Enterprise Cyber Risk | Third-Party Cyber Risk | Cyber Vulnerabilities |

## Authorization Network Security

**Limit fraud exposure from vulnerabilities in authorization networks**



| Monitor | Alert/Block | Reduce |
|---|---|---|
| Large-Scale Fraud Vulnerabilities | Fraud Attacks | Fraud Losses |

**Solution Benefits**
Supplier Vulnerability • Vendor Vulnerability • Stop Ransomware • Identify Data Breaches

# Systemic Risk Management

Optimize your operational resilience across relationships against evolving business risks, by proactively monitoring and assessing threats

## Compliance Risk Management

**Allows you to reduce regulatory compliance risk and remain compliant whilst continuing to be competitive**
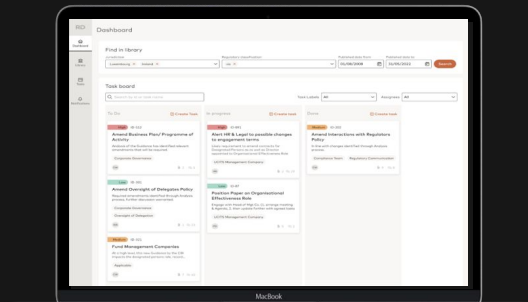


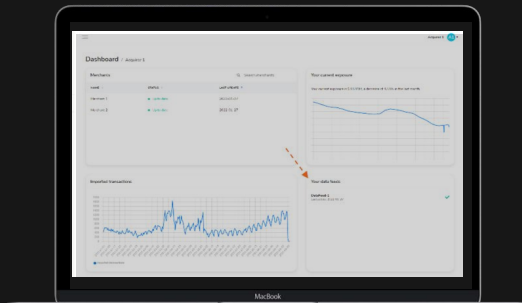| **Assess** | **Automate** | **Address** |
|---|---|---|
| Regulatory Environment | Regulatory Scanning | Compliance Requirements |

## Cyber Threat Protection

**Gain visibility into your cyber risk exposure from third-party partners**



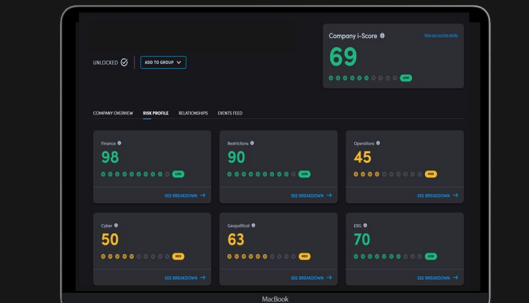| **Scan** | **Evaluate** | **Mitigate** |
|---|---|---|
| Enterprise Cyber Risk | Third-Party Cyber Risk | Cyber Vulnerabilities |

## Third-Party Risk Management

**Gain visibility into critical enterprise risks across your business relationships to reduce financial losses**



| **Identify** | **Assess** | **Optimize** |
|---|---|---|
| Business Relationships | Business Network Risks | Operational Resilience |

**Solution Benefits**
Sanctions/Restrictions • ESG • Reduce Cyber, Operational, Geopolitical and Financial Risks