Mastercard® Healthcare Solutions

Bridging the healthcare technology gap

mastercard

Mastercard® Healthcare Solutions

How Mastercard is partnering with the healthcare industry to secure its patients and data, while driving down costs

mastercard

Contents

The current environment

The healthcare industry faces a growing technology gap. While many healthcare organizations have deep expertise in technologies that preserve and enrich life, they often lack experience with advanced tools like predictive data analytics, artificial intelligence (AI), and cybersecurity that have been leveraged in financial services and other industries for years, which would help address critical operational issues, like:

- Driving down costs by eliminating fraud, waste, and abuse (FWA)
- Securing the highly sensitive patient or member information they've been entrusted to protect
- Enhancing the patient experience by making interactions more efficient and personalized

The industry is challenged by the siloed nature of healthcare delivery, the numerous stakeholders involved, and a complex claims and payment process. And the exponential growth in healthcare data—healthcare data already accounts for 30 percent of the world's data volume[1]—makes it difficult for payers to keep up. Usually, a problem—whether a simple error or deliberate fraud—isn't detected until after a claim is adjudicated. Plus, the digitization of data has led to an increase in the risk of data breaches. The pandemic has only heightened the industry's exposure to cybersecurity risks and data threats, while increasing the need for cost control and efficiency.

Fraud and waste are significant

$300B

Up to 10% of annual healthcare expenditures in the U.S., $300B, are lost due to fraud, waste, and abuse costs each year[2]

FWA losses hurt revenue

12%

Healthcare firms lost an average of 12% in annual revenue as a result of FWA in payments[3]

Surging data requires analysis

30%

Healthcare data makes up 30% of the world's data volume[1]

Data threats grow bigger

↑ 25%

more large healthcare data breaches were reported in 2020 than the year before[4]

HSA accounts under attack

12%

of HSA account balances are at risk, as fraudsters increasingly steal consumer data through digital channels[5]

Ransomware targets healthcare

18%

of ransomware attacks in Q4 2020 targeted healthcare—more than any other industry[6]

Innovative technologies promise to help transform healthcare for payers, providers, and patients

Mastercard is helping the healthcare industry bridge a growing technology gap. Armed with advanced tools like predictive data analytics, artificial intelligence, cybersecurity products that help threat detection, digital identity tools, and flexible billing solutions, we're helping payers and providers improve business results by tackling critical challenges.

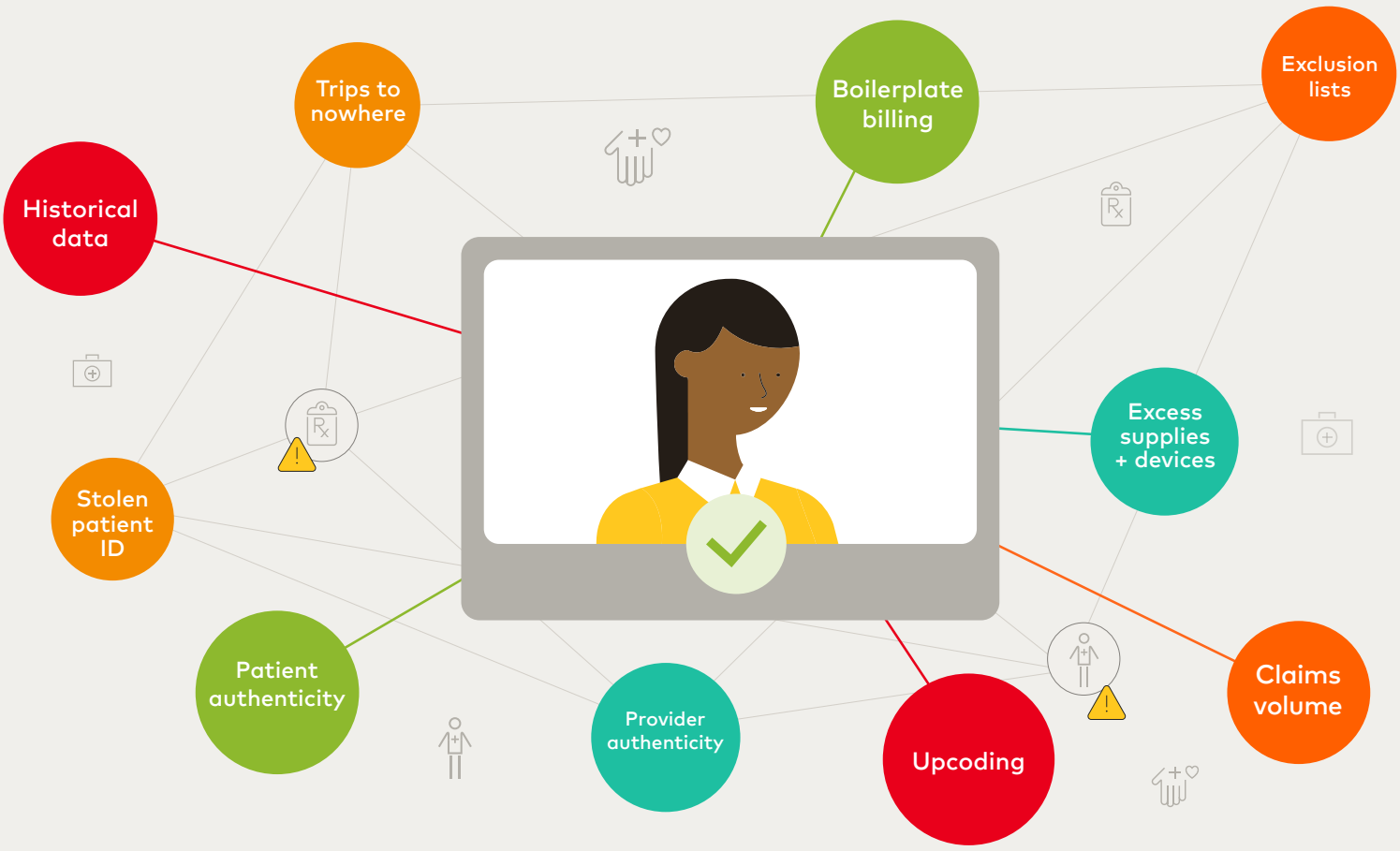
We're improving the patient and member experience by helping payers and providers improve outcomes, improve the digital experience, and simplify and enhance the billing and payment process. And we're keeping valuable healthcare data safe and secure by using the same cybersecurity and digital identity solutions we use to protect billions of credit card transactions. With our proven technology and deep industry experience, we're helping make the healthcare system more convenient, more secure, and more cost-effective.

Reducing healthcare costs

A major challenge facing the healthcare industry is the high proportion of erroneous or fraudulent claims, which cuts into payers' revenues and drives up the cost of healthcare. Compounding the problem is a cumbersome claims process and "pay and chase" tactics—investigating claims after they have already been paid—resulting in a small percentage of these lost dollars ever being recovered.

At Mastercard, fraud detection is always on, every microsecond of every day. Processing more than 1 billion payments transactions daily, we use artificial intelligence, machine learning, and other tools to analyze thousands of data points and hundreds of decision points to flag suspicious activity. We apply these same tools to healthcare claims data, identifying anomalies that require investigation. Our approach: prevent an overpayment before it occurs. Our AI models have now been trained to identify fraud, waste and abuse (FWA) within healthcare claims, at the pharmacy as well as other challenges.

AI detection of FWA



The power of AI

Mastercard AI's patented Smart Agent technology creates an end-to-end suite of profiling and modeling capabilities that continuously adapt and improve results—staying current with trends, patients, providers, and practices—and can be tailored to each customer's business needs and goals. This seamless combination of advanced AI tools delivers personalized decisions in milliseconds to payers, insurance companies, business leaders, or other entities. Models evolve at scale with an organization's data, increase detection rates, and decrease operational costs and false positives.

Our predictive analytics are also helping our partners reduce readmissions and drive down costs through greater use of value-based care models, including cutting the length of hospital stays and helping improve outcomes by driving greater adherence to treatment protocols.

AI's continuous updates and reduced false positives enable real-time detection, resulting in denial of fraudulent transactions before they are processed. Real-time detection is made possible by architecture that allows personalization of models to address our clients' unique challenges. Advanced AI works with your historical data, enriches it, and adapts the information for analysis. And with Mastercard's proprietary distributed file system, which has no single point of failure, users can expect 99.9999 percent uptime.

Lightning response times

<10ms

Mastercard's distributed architecture delivers lightning speed response times, below 10 milliseconds, and end-to-end encryption and traceability

Unlimited scalability and resilience

99.9999%

Our distributed file system has no single point of failure, so customers benefit from 99.9999% uptime

AI's algorithms identify and compare every data point within a transaction, looking for behaviors and patterns. They compare frequency, transaction size, location, health diagnoses, sudden changes in billing behavior, and more. The data is then compared to other service provider results to identify anomalous behavior. AI reduces hours of investigation to milliseconds.

Mastercard AI can help payers

Assess new providers to reduce onboarding risk

Continuously monitor provider behavior and risk levels

Manage daily transaction fraud risk in real time

Address omnichannel fraud across vectors, channels, transactions

"Rules-based systems require constant care and manual revisions because they quickly become dated. Maintaining these rules is difficult and costly to do when a system has thousands of lines of code supporting tens of thousands of rules. In our experience, 40 percent of FWA investigations prompted by such rules turned out to be false positives—good claims that rules mistakenly identified as fraud."

- Tim McBride, AHFI, Director of Product Development and Innovation for Mastercard Healthcare Solutions

Case study

SITUATION

Milliman Inc.'s Payment Integrity group audits health claims for payers, saving its customers millions of dollars each year. To take advantage of the sophisticated capabilities artificial intelligence could bring to its practice, Milliman engaged Mastercard Healthcare Solutions to build an AI model using its proprietary technology.

SOLUTION

Mastercard's team of data scientists conducted a six-step AI Express model development process to deliver a strong return on investment in detection of fraudulent providers for Milliman's clients.

RESULTS

The new model uncovered more than $239 million in potential savings from 2,700 high-risk providers for fraudulent claims for just one mid-sized Milliman payer client.

$239M

in potential savings for fraudulent claims identified

PART 2

Keeping valuable healthcare data safe and secure

Healthcare data is an attractive target for hackers because they can get $250 on the dark web for each stolen patient record—compared to $5.40 for a payment card and only 53 cents for a social security number.[7] Breaches are not only costly—on average, $429 per stolen record[8]—they also damage the reputations of providers and payers. Yet the healthcare industry remains a laggard in cybersecurity preparedness, ranking 8th among 18 major U.S. industries.[9]

Mastercard, at its core, is a cybersecurity trailblazer. We protect our data enterprise and network from 200 network attacks every minute of every day. Our mission is to provide industry-leading tools to protect business enterprises and improve security at every touchpoint, while making end-user experiences frictionless.

Mastercard has advanced cybersecurity solutions to the next level, enabling solutions to share data and learn from one another as part of Mastercard's Connected Intelligence vision. By bundling native and several acquired capabilities, we offer holistic, integrated solutions matched by no other payments network.

Mastercard delivers strong security with low friction throughout the healthcare experience. And because our systems continuously learn from every transaction and grow more intelligent, accuracy rises over time.

- Mastercard's multi-layered, connected intelligence begins as the patient or member interacts with their device or account and increases along each step of their journey
- Leveraging thousands of unique data points and hundreds of decision points throughout the customer journey, as well as our coordinated set of AI-based solutions and machine learning tools, we help payers and providers deliver a more secure digital ecosystem and a seamless user experience
- We also use digital identity tools to verify user identities in order to ensure rightful access to data
- Our cybersecurity tools help identify third-party vendor and enterprise risk to help an organization pinpoint its vulnerability to attack.

A simple, seamless, secure way to verify identity

The arrival of the COVID-19 pandemic in 2020 accelerated consumers' shift toward digital-first lifestyles, including virtual "visits" to their doctors. Securing and confirming identities of those purporting to be patients is already a major challenge for healthcare payers and is bound to grow as the industry continues its path into a digital future. This is a challenge that must be met, as medical identity theft is not only costly to payers and providers, but can impact consumers in many ways:

- Getting billed for treatments not received
- Delays in receiving care when false data is entered in their records
- Lost medical benefits
- Misdiagnosis or mistreatment due to incorrect information in patients' records

Give patients real-time access to their health data with Mastercard ID Verification

As a data security leader, Mastercard has the expertise and solutions to protect your patients and members, and your business. Mastercard ID Verification is a real-time identity verification service leveraging a variety of capabilities and external data sources that provides fast, secure, and reliable consumer verification. ID Verification was designed to help organizations with:

- New member enrollment in a health insurance plan, app or portal account
- Patient ID proofing
- Patient identity data sharing
- Meeting regulatory requirements such as 800-63-3 and Identity Assurance Level 2, allowing secure access to patient identity data
- Preventing potential errors such as applying a patient's most recent visit to the wrong medical record, or creating a duplicate record

ID Verification is comprised of a suite of API services, embedded into a user's web or mobile application, to provide an easy, seamless user experience. Operating behind the scenes within the user's application, identity is verified without requiring any downloads or being redirected to a different website. API calls can be configured to require just a single input from users, and personal data can be auto-filled to expedite enrollment.

Case study

SITUATION

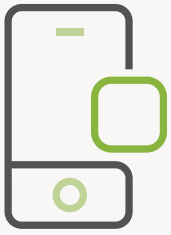
ThedaCare®, a preventative and holistic healthcare provider serving over 600,000 community members at over 180 points of care in Northeast and Central Wisconsin, wanted to offer its members a new healthcare app so that patients can easily connect with care providers, manage their care information, receive alerts, and more.

SOLUTION

Mastercard ID Verification service, integrated within b.well Connected Health, enables ThedaCare's app users to securely verify their identity in real time using their mobile phones in a fast, frictionless process.

RESULTS

During the four-month pilot period, the implemented solution achieved an 87% success rate in instantly verifying a user's identity and pre-filling their personal information, delivering more accurate user data.



87%

success rate in instantly verifying an app user's identity and pre-filling their personal information

PART 3

Verifying users and protecting patient information with biometrics

As healthcare participants quickly expand their interactions to online channels, the need to accurately identify patients, and protect their privacy and information, has become critical. Our user verification tools look at the user's behavior and can detect anomalous activity in a patient or admin account before a bad actor accesses any information or submits a fraudulent claim.

NuData technology evaluates inherent patterns, such as typing cadence or device insights, to make an assessment in real time at login or other points of interaction. This prevents bad actors from accessing sensitive data, submitting a healthcare claim, or other types of fraud that take place within online user accounts. We support the healthcare industry in two primary ways:

Account takeover

The surge in exposed personal data is allowing account takeover (ATO) fraud to thrive. To thwart bad actors, NuData looks at user behavior and other data points to validate legitimate logins. Then the account is analyzed in real time across the entire session to make sure there are no sudden changes in behavior after the login.

Even if users present the correct credentials, NuData can detect risky users with over 99 percent accuracy. This helps healthcare organizations:

- Stop scripted attacks at login
- Increase customer confidence that their data is safe
- Lower friction on trusted users

New account fraud

How can you tell if new users are legitimate when it's the first time you see them? NuData evaluates if the user is behaving as a good user or as a machine. Through passive biometrics, machine learning, and billions of anonymous data points, we flag high-risk accounts in real time so organizations can close them now and prevent fraud tomorrow, helping healthcare organizations:

- Prevent future fraud
- Avoid fraudulent transactions
- Lower operational costs

Case study

SITUATION

A global bank was experiencing a large scale account takeover attack, which was emulating user behavior and bypassing the bank's existing fraud solution, resulting in unauthorized access to user accounts.

SOLUTION

The client was able to stop 99% of attacks with NuData's account takeover solution. The sophisticated attacks involved thousands of logins per hour. Within two weeks, NuData stopped millions of fraudulent attempts that were missed by the previous solution.

RESULTS

NuData mitigated 250 million automated attacks with 99% accuracy and a false positive rate of only 0.1%—successfully safeguarding consumer information without impacting the user experience.

99%

With 99% accuracy, NuData mitigated 250M automated ATO attacks

Detecting and prioritizing cybersecurity risks

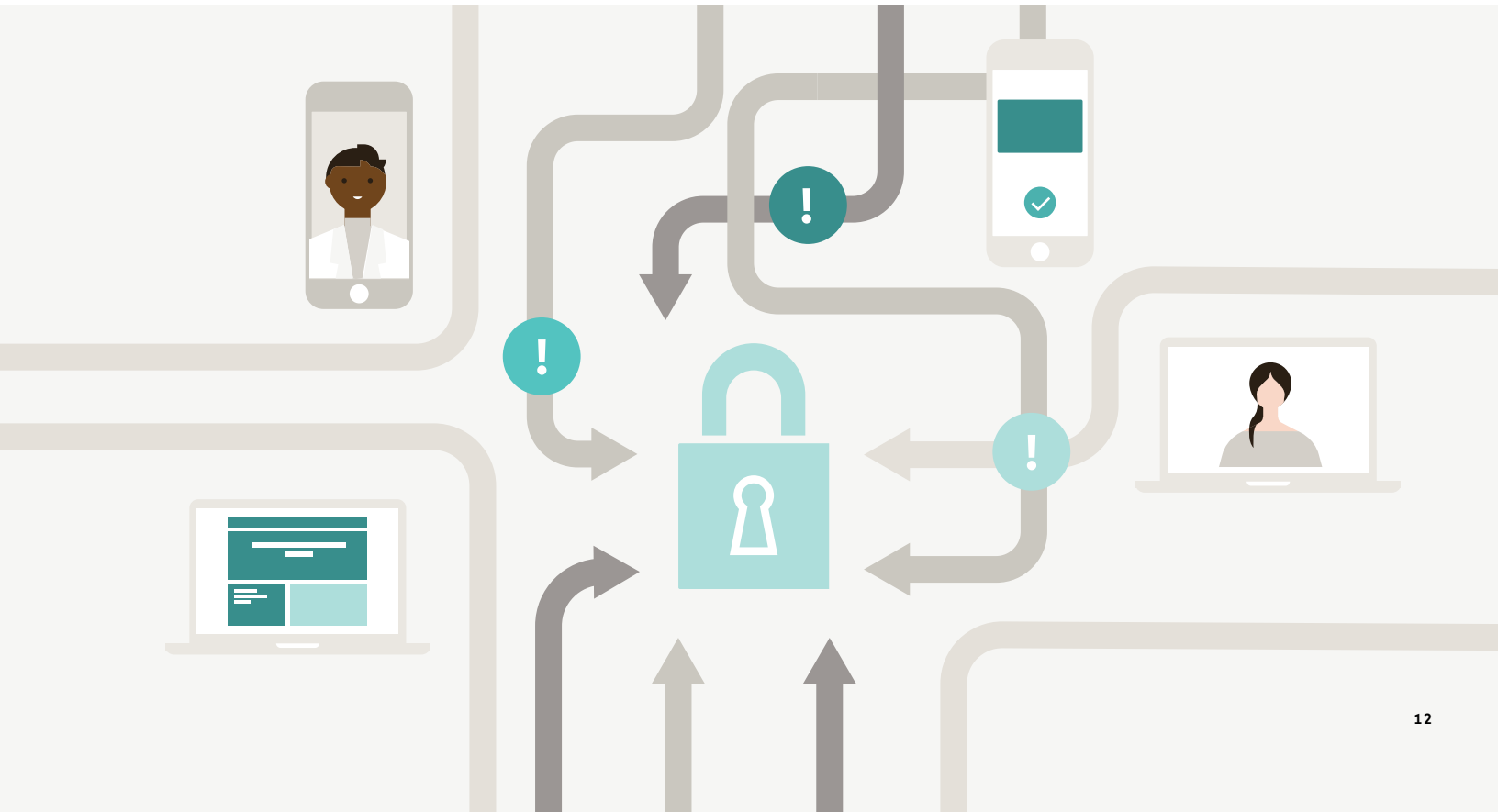
Understand how your health organization and ecosystem is protected by assessing your cybersecurity posture internally and externally with Cyber Quant and RiskRecon

Effective healthcare is measured by healthier patient outcomes. At the core of better outcomes sits the doctor-patient relationship and the ecosystem that supports and facilitates this relationship—including all the patient data that informs it. This data travels from lab to doctor to patient to payer, and a growing number of technologies—electronic medical records, smart health devices and monitors, telehealth, and other innovations—potentially expose this data to criminals. Cybercriminals are actively targeting this data and technology layer, which is why cybersecurity has a critical role to play in ensuring the confidentiality and integrity of the technology connecting doctors, patients, and healthcare systems.

Uncover your internal security gaps with Cyber Quant

Like a doctor checking a patient's vitals, Cyber Quant takes the pulse of a healthcare organization's technology and processes. Our diagnosis helps healthcare security officers and risk management teams focus improvements to their cyber posture within the organization where they will have the greatest impact. With Cyber Quant, healthcare organizations can:

- Validate internal-facing cyber capabilities and technology
- Map and analyze external cyber intelligence to assess the organization's capabilities in light of the dynamic cyber threat landscape
- Map the organization's maturity across multiple standards and frameworks, such as HIPAA, NIST, and PCI
- Quantify the cyber risks in financial terms so the organization can evaluate their return on cybersecurity investments
- Run simulations and prioritize the initiatives which will be most impactful in reducing cyber and organizational risks in light of the organization's cyber needs, the threat landscape, and their detection and protection capabilities
- Navigate the dynamic and ever-changing compliance risk landscape by providing assessment outputs and analysis to help organizations meet current and future regulations.



Case study

SITUATION

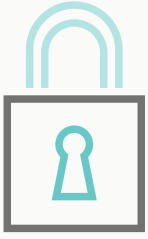
During a period of targeted ransomware attacks in 2020—and with security budgets severely constrained due to COVID-19—the CIO of a hospital system wanted to quickly evaluate where to make the next set of IT investments to protect the organization.

SOLUTION

The Mastercard Cyber Quant team helped conduct a rapid assessment across the hospital's various segments and lines of business. Mastercard evaluated responses from its questionnaire, conducted technical diagnostics, and assessed the threat landscape to determine the organization's security posture for each department.

RESULTS

The CIO was able to compare the security gaps between the clinical and research segments of the business and shift part of the funds to the clinical side to address its larger set of external threats and attacks. By addressing top-priority gaps, the hospital system was able to reduce financial risk by $25 million.



$25M

By addressing top-priority gaps, the hospital system was able to reduce financial risk by $25 million

"over half of organizations have experienced a data breach caused by third parties"

Secure your data from third-party vendor gaps with RiskRecon

When every business relies on dozens or even hundreds of third-party suppliers, vendors, and partners, it may not be surprising that over half of organizations have experienced a data breach caused by third parties.[10]

Data is at the heart of healthcare management—empowering providers, payers, and partners to successfully treat and support patient health. At the same time, it is vital for all players to protect this sensitive information.

RiskRecon helps mitigate third-party risk by proactively monitoring and evaluating the cyber environment of entities with an online presence—rendering a cyber risk rating and prioritized vulnerability findings so organizations can act quickly before they can be exploited.

With RiskRecon, healthcare organizations can:

Assess and benchmark their cybersecurity risk performance – Gain deep visibility into the current cyber state, with risk-based guidance to identify and prioritize remediation of the most impactful risks.

Assess and monitor third-party cybersecurity risk – Leverage RiskRecon cybersecurity assessments and automation to ensure third parties perform to your organization's standards.

Collaborate with vendors to address issues and improve security – Utilize RiskRecon's customizable alerting and action plans to provide vendors with the necessary support to ensure their success.

Case study

SITUATION

A large network of healthcare providers and hospitals serving a regional community across a major metropolitan area in the U.S. experienced a third-party data breach, exposing tens of thousands of patient records. In the face of COVID-19, it needed to quickly upgrade its third-party risk management program.

SOLUTION

Continuous monitoring by RiskRecon enabled the provider to reduce its risk, make ongoing improvements in risk management, handle the new business challenges posed by the pandemic, and keep tabs on vendors without imposing time-consuming self-assessment requirements or wasting anybody's time with false positives.

RESULTS

The provider improved remediation of security risks within vendor environments by 40% and reduced third-party risk by 10% in the first six months.

40%

improvement in a healthcare provider's ability to manage third-party risk and a 10% reduction in that risk in the first six months

How industry participants benefit from Mastercard's healthcare expertise and solutions

We stand behind you with the full power of the Mastercard brand—leveraging the same technology, expertise, and scale we use to protect our own business and address critical challenges for partners and customers.

Payers

- **Gain greater confidence** in your payment processes, data, and system security
- **Improve engagement with, and outcomes for, your members** by employing our powerful analytics
- **Save millions lost to fraud, waste, and abuse** by detecting incremental suspicious claims before payments are made, using our superior AI capabilities
- **Accurately assess and quantify security risks** and apply the latest cybersecurity tools to protect your valuable data

Providers

- **Accurately assess and quantify security risks** and apply the latest cybersecurity tools to protect your valuable data
- **"Cure" critical operational issues** so you can focus on curing patients
- **Simplify and enhance** billing and payment processes

Partners

Mastercard aims to enhance your business rather than compete with it. We collaborate to augment and accelerate innovation in healthcare to help you:

- **Speed idea generation** by bringing concepts to life and fast-tracking promising solutions through prototype, pilot, and market launch
- **Enrich and expand your current offerings** and fill capability gaps by leveraging our technology assets and jointly devising solutions
- **Accelerate business growth** by choosing a strategic partner with proven capabilities and scale, committed to working together with you to address critical healthcare industry needs

Conclusion

If anyone needed proof that every business is a digital business, the pandemic brought it home. The time for incremental change is past, and leaders in healthcare are adopting a digital-first, people-centric ecosystem that reimagines the healthcare experience at every step. In this new era—in which 73 percent of healthcare executives say that their technology architecture is becoming critical to the overall success of their organization[11]—making the right technology choices matters more than ever.

Healthcare organizations can seize this opportunity to employ innovative technologies that transform the patient experience, improve health outcomes, ensure confidence in the security of patient and other data, while lowering costs and increasing revenue.

Mastercard, a widely recognized technology innovator, has the proven technology, deep industry experience, and commitment to help make the healthcare system safer, more secure, and more cost-effective. We bring value to payers, providers, and patients. And unlike other new entrants to the healthcare industry, Mastercard is working to enhance and grow payers' and providers' business—not compete with them.

Endnotes

1 Health IT Today, 2021.

2 National Health Care Anti-Fraud Association, *The Challenge of Health Care Fraud*.

3 PYMNTS and Brighterion, AI In Focus: Targeting Fraud, Waste And Abuse In Healthcare, 2021.

4 U.S. healthcare data breaches of 500+ healthcare records, HIPAA Journal, 2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020, 2021.

5 Devenir, 2018 Midyear HSA Market Statistics & Trends, 2018.

6 Coveware Quarterly Ransomware Report, Q4 2020.

7 2018 Trustwave Global Security Report.

8 IBM Security, Ponemon Institute, Cost of a Data Breach Report, 2019.

9 SecurityScorecard, 2019 Healthcare Report.

10 Ponemon Institute, A Crisis in Third-Party Remove Access Security, sponsored by SecureLink, 2021.

11 Accenture Digital Health Technology Vision, 2021.

mastercard

To learn more contact healthcaresolutions@mastercard.com to discuss how Mastercard can help your organization identify performance improvements.

Visit mastercard.us/healthcare-solutions