PYMNTS | Payoneer

OCTOBER 2022

Cross-Border Commerce Futures:

How AI And Biometrics Are Transforming Global Risk Management

Cross-Border Commerce Futures: How AI And Biometrics Are Transforming Global Risk Management, a PYMNTS and Payoneer collaboration, examines how efficient, secure and compliant cross-border payments help small to mid-sized businesses (SMBs) and entrepreneurs achieve their global ambitions during crises that impact their business.

Cross-Border Commerce Futures:

How AI And Biometrics Are Transforming Global Risk Management

PYMNTS | Payoneer

Cross-Border Commerce Futures: How AI And Biometrics Are Transforming Global Risk Management was produced in collaboration with Payoneer, and PYMNTS is grateful for the company's support and insight. PYMNTS retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

Introduction

While the introduction of cross-border payments at scale has empowered many businesses globally, it has also amplified the risk of money laundering schemes or other financial crimes. Remote onboarding of customers and rapid, high-volume payments provide more opportunities for criminals. Bad actors leverage sophisticated technology to gain access to financial platforms or create technical vulnerabilities to launch attacks. Thankfully, more payments platforms are using technologies such as artificial intelligence (AI) and biometrics to develop robust defenses — allowing FinTechs to effectively manage compliance on behalf of their business customers.

Cross-Border Commerce Futures: How AI And Biometrics Are Transforming Global Risk Management, a PYMNTS and Payoneer collaboration, looks at how advanced technologies are transforming global risk management for businesses with cross-border operations.

The Risk Management Landscape:

Challenges in identifying and mitigating modern fraud and AML risks

For FinTechs and financial institutions (FIs), keeping up with the ever-increasing sophistication of criminal elements while supporting a long-term growth strategy can be challenging, if not impossible.

First, there is the matter of identifying suspicious transactions and vulnerabilities to fraud — a critical task for businesses and payment services providers supporting global companies and entrepreneurs.

This requires more than a basic understanding of how fraud works — it demands up-to-the-minute awareness of the latest tactics used by bad actors to infiltrate, compromise or dupe accounts, and the best ways to combat the tools they use.

As new technologies emerge in retail and financial services, bad actors leverage these same innovations to evolve their methods of committing fraud and other crimes. Cross-border operations add additional challenges, ranging from navigating compliance requirements to managing multiple currency payments.

Global risk management becomes even more difficult at scale — as business success and transaction volume increase, technical vulnerabilities to complex fraud attacks also grow exponentially.

For example, managing KYB requirements can be a global challenge. FinTechs and FIs may find themselves caught in the middle: Preserving user experience is a priority, but the complexity of cross-border regulations can make seamless payments difficult to consistently deliver as requirements vary from region to region.

Why “payments as usual” are fraught with new risks when businesses operate internationally

The risk of fraud and other financial crimes increases as a business grows. Authenticating, tracking and monitoring payments is a complex process, and this complexity increases when it comes to cross-border payments.

Onboarding each new business relationship to ensure compliance with global anti-money laundering (AML) and combating the financing of terrorism (CFT) standards can be daunting for FinTechs and FIs of all sizes — especially in light of new and complex global regulations. New know your customer (KYC) and CFT reporting standards require more stringent transaction monitoring, heightening the risk of noncompliance. Here are just some examples of the compliance tasks the industry must fulfill as they process payments across international borders:

Global KYC and CFT standards monitoring

These standards may vary by region, even when international mandates are the same. Businesses must comply with international regulations and the rules applicable to each party involved in a transaction. Financial Action Task Force, European Union and United States regulations may also change over time as new technologies and business models emerge, and organizations must be prepared to heighten their compliance efforts.

Proactive noncompliance risk screening

Sanctions list screening is a complex task for businesses attempting to manage compliance independently. Payee information must be verified against sanctioned actor lists such as OFAC SDN, PEP, HMT, RES 1988, AQ, CFSP and others on a regular basis. Organizations must update their screening processes as these lists change to ensure that payments are not sent or received from the flagged individuals, corporations or state actors.

Real-time, transaction-level monitoring

This layer of compliance management reveals persistent vulnerabilities to fraud and other financial crimes, making it the most efficient way to block fraud attacks and mitigate previous security failures. This level of sophisticated analysis is particularly challenging for growing businesses, especially at scale, without the use of advanced monitoring technologies like AI and biometrics.

Managing Risk:
Whose problem is it, anyway?

For many businesses, the burden of fighting fraud and managing compliance falls on their payments processing platforms. Yet the unique challenges of cross-border business growth in an evolving payments ecosystem — ranging from multi-region compliance strategies to transaction-level security measures — often leave even highly innovative payment services processors without adequate defenses against sophisticated attacks.

New tools for fighting financial crime and money laundering

Enter AI and biometrics — technologies that allow FIs to level up their data security, fraud detection and risk mitigation strategies. AI enhances risk analysis by leveraging lightning-fast processing power to identify fraud or financial crime vulnerabilities, monitoring transactions for signs of suspicious activity and helping businesses prevent financial loss. The use of unique identification through biometrics provides greater security around customer onboarding and is increasingly important because many regulated FIs now meet prospective customers digitally and not in person. Both technologies offer FinTechs and FIs opportunities to take risk and cost out of the compliance process and provide improved service to customers.

Why AI-based transaction-level monitoring is essential for managing risk

AI works at the transaction level to help block threats and detect sophisticated networks that are exploiting financial platforms. It also enables risk models to evolve continuously and ensure that compliance resources are used most effectively.

Q&A 1

Shay Dovev of ThetaRay on the global compliance challenge

Shay Dovev is senior vice president of strategic accounts for ThetaRay, a large data analytics and software as a service firm headquartered in Israel. We connected with Dovev to learn more about the technology behind his company's successful AML and anti-crime strategies.

Q: What are some modern security and noncompliance risks facing organizations?

A: Most are related to terror financing, AML, fraud and other financial crimes, which have become increasingly hard to stop, as old-fashioned controls can't stop new threats. A rules-based transaction monitoring system must constantly adapt to new typologies. Criminals will always exploit loopholes or gaps or come up with complicated schemes. Besides being expensive to operate and requiring significant manpower, rules-based architecture is not a smart implementation of technology. It relies on known rules that can be easily outsmarted by bad actors, including in cyber-engineered attacks.

Q: What is the value of a payments processing platform that uses model transaction tools?

A: Simply put, it's safer to transfer these payments. Having said that, each part of the transaction chain can better trust the entity it works with, enabling businesses [to open] in additional territories and enjoy more comprehensive risk coverage, even with third-party clients. In sum, FinTechs that implement modern systems can more easily win new business partners and grow their revenues.

Q&A 1

Shay Dovev of ThetaRay on the global compliance challenge (continued)

Q: So, innovation is key to better compliance results. How does compliance relate to business growth?

A: Compliance enforces the standard of security and information safety, as well as with whom we can and can't do business. Hence, there is a significant impact on business growth, according to where we are "allowed" to work, market and sell our services and where we can't. The level of risk drives the business forward or backward. Rather than de-risking, forward-looking FinTechs are increasing their reach in global markets as a source of new revenues. They are doing so by enhancing their risk controls and switching to smarter technology that effectively recognizes threats to make the corridor safe.

Q: So, how does the use of machine learning and AI accelerate risk/vulnerability identification and mitigation?

A: It overcomes a principal inherited problem — it may detect unknown risk patterns. Hence, basically the system is "insured," at least at a reasonable level, versus risk that never could have been spotted and acted upon. Patterns of illegal activity using digital platforms are new and evolving, coming within the context of unknown unknowns. Unsupervised machine learning and AI are much more effective tools for transaction monitoring because they can identify truly abnormal transactional activity without human bias for better decision-making. AI and machine learning solutions can respond and adapt to risks a lot faster.

Q&A 2

Micheal Sheehy of Payoneer on the role of technology in identity management and compliance

Micheal Sheehy is the chief compliance officer for Payoneer. We sat down with Sheehy to discuss the role of technology in improving how FinTechs and FIs manage compliance, particularly biometrics and AI.

Q: What does the future look like for organizations or entrepreneurs facing compliance challenges?

A: We look at the future from three perspectives when it comes to compliance. First, our customers expect seamless experiences when using our services. Whether it's via online forms or real-time interactions, they want us to collect compliance and regulatory requirements and focus on growing their businesses. Second, we anticipate that bad actors will always be innovating to find new ways to game the system, which means we can never be complacent. We all need to constantly invest in new tools, methods and expertise. Third, we take seriously our responsibility as stewards of the global financial system, working hand in hand with our regulators around the world whenever possible to collaborate on our common goal.

Q: How does AI and machine learning fit into the future of payments management?

A: Artificial intelligence is the future, but the future is already here in terms of the expectations of regulators around the world: They expect regulated entities like Payoneer, as well as the banks, to ensure that their compliance monitoring technology and framework are up to date and can evolve with the customer and the environment in which it operates. AI is important because it allows us to move from the rules-based "detect and report" paradigm to a new paradigm based on effective prevention. This is incredibly significant for those of us who are stewards of the financial system because criminals will always be creating and investing in new tools and methods to move dirty money faster than any rules-based approach. Adding a machine-learning layer allows us to evolve, adjust and detect more complex typologies and sophisticated networks.

Q&A 2

Micheal Sheehy of Payoneer on the role of technology in identity management and compliance (continued)

Q: So, we know that AI is not a one-size-fits-all solution — what should organizations keep in mind as they think about this technology?

A: Adding an AI detection layer to your compliance toolkit does not mean abandoning the traditional rules-based risk engines. Rather, it's an additional layer that allows us to perform further and deeper analysis of transactions going through our network. We think of it as a "canary in the coal mine," alerting us to potential danger before we have picked it up with other tools. The biggest challenge with implementing an AI system is configuring it. You have to figure out the algorithm that most effectively parses the information in your network and then tool your system so that you aren't overwhelmed with false positives.

Q: How about biometrics? Where does that fit in with a proactive compliance model?

A: Biometrics is becoming increasingly necessary as a tool to combat AML and identity-based fraud typologies. That's because, increasingly, many regulated institutions have to onboard customers in virtual settings rather than face-to-face. Ever since the Equifax data breach, in particular, we can expect that most individuals' traditional, personal identification information can be obtained somewhere on the dark web. That means biometric information, which is any unique data point for an individual that cannot be replicated by someone else, becomes the best way to ensure that the person you're dealing with is that person.

This is an area where the industry is often ahead of the regulators but given the trends we're seeing in places like Singapore, Malaysia and the European Union — which are requiring FIs like us to incorporate biometric information in our KYC programs — we expect that more regulators around the world will start to require it as well.

Q&A 2

Micheal Sheehy of Payoneer on the role of technology in identity management and compliance (continued)

Q: What about the challenges involved with biometrics?

A: There are some challenges to using biometrics. For example, not every region in the world has reliable or extensive internet coverage, which makes it difficult to gather and check biometric information. There are also places where this information is protected in such a way that it cannot be transmitted across borders. This also means there is no single global vendor that can handle a company's biometric collection needs. And last but certainly not least, we need to recognize that requiring biometric information does interrupt the customer experience by adding extra steps that can slow down the onboarding process or increase the abandonment rate.

About

PYMNTS

PYMNTS is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Payoneer

Payoneer is the world's go-to partner for digital commerce, everywhere. From borderless payments to boundless growth, Payoneer promises any business, in any market, the technology, connections and confidence to participate and flourish in the new global economy.

Since 2005, Payoneer has been imagining and engineering a truly global ecosystem so the entire world can realize its potential. Powering growth for customers ranging from aspiring entrepreneurs in emerging markets to the world's leading digital brands like Airbnb, Amazon, Google, Upwork, and Walmart, Payoneer offers a universe of opportunities, open to you.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at **feedback@pymnts.com**.

DISCLAIMER

Cross-Border Commerce Futures: How AI And Biometrics Are Transforming Global Risk Management may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.