

Preventing Real-Time Fraud in Real-Time Payments

Agility and Speed Can Help
Financial Institutions Reduce Risk

In response to the rising expectations of consumers and businesses, money is moving domestically and internationally faster than ever. More than 50 countries around the world are live on real-time payment systems, with more to come.

As the speed of payments increases along with real-time settlement, financial crime risks are on the rise along with the pace of change in fraud attacks. To offer payment services securely, financial institutions must be agile and able to respond faster to protect themselves and consumers from fraud.

Securing real-time payments requires more than simply deploying the same risk management and fraud prevention solutions faster. When it comes to real-time payments, every step of the transaction-processing life cycle, including fraud detection, must be completed in fractions of a second.

That requires a fraud risk management approach designed for real-time. It means employing up-to-date processes and technologies to meet increasing consumer and business expectations while managing financial crime risk effectively.

Keep Pace With Expectations and Regulations

Consumers and businesses expect quick and seamless transactions. They want to initiate real-time payments whenever and wherever they choose and receive immediate confirmation that the payment is complete. If there is a problem, they want immediate resolution.

The move to real-time payments requires financial institutions make support and fraud teams available 24/7, both to assist accountholders and to detect and protect them from threats that emerge outside of traditional banking hours, a growing consideration in an increasingly global economy.

In that dynamic business and risk environment, financial institutions want a fraud solution to help them make timely decisions that significantly improve fraud detection rates, reduce false positives, optimize operational costs, and drive efficiency and customer satisfaction.

Employ a Holistic Approach

Real-time payments make the risk of loss different than with other types of transactions. Once a real-time payment has been accepted by the payee's financial institution, the transaction is often considered irrevocable.

While real-time payments are applicable across a broad range of transactions, fraud detection systems have historically been designed for a specific type of transaction. The siloed approach can limit fraud detection and is not necessarily the best approach for real-time payments monitoring. Effective real-time payment fraud prevention requires solutions able to detect many possible types of fraud across all electronic-funds transfer channels and payment-origination mechanisms.

Those solutions must be fully connected and able to use data across payment types and channels to help analyze, detect and prevent fraud. Threats continue to evolve and increase in number and financial institutions cannot afford to implement fraud prevention tools in a piecemeal fashion.

So what works? Leveraging new technologies focused on data and analytics and using machine learning can manage risk and reduce false alerts. That helps financial institutions balance risk management obligations with the delivery of a better experience, which is critical in a highly competitive financial services environment.

Here are three innovative strategies to consider:



1 Get Smarter With Data



2 Learn Over Time



3 Adapt to Changing Landscapes



Strategies 1:

Get Smarter With Data

With ISO 20022 being adopted as the industry standard for electronic data exchange between financial institutions, real-time payments can carry much more data. While that can help determine if a real-time transaction is fraudulent, the analysis can take time using traditional fraud detection systems, which aren't equipped to process all the incoming data and use it to tackle fraud.

The ability to quickly consume, analyze and act on huge amounts of data covering channels, transactions and multiple convergence points is critical to managing fraud risk.



Strategies 2:

Learn Over Time

Financial institutions can leverage those broader data sets by adopting machine learning technologies. Those technologies can perform millions of fraud checks within seconds and continuously learn from the data to become more accurate and effective over time.

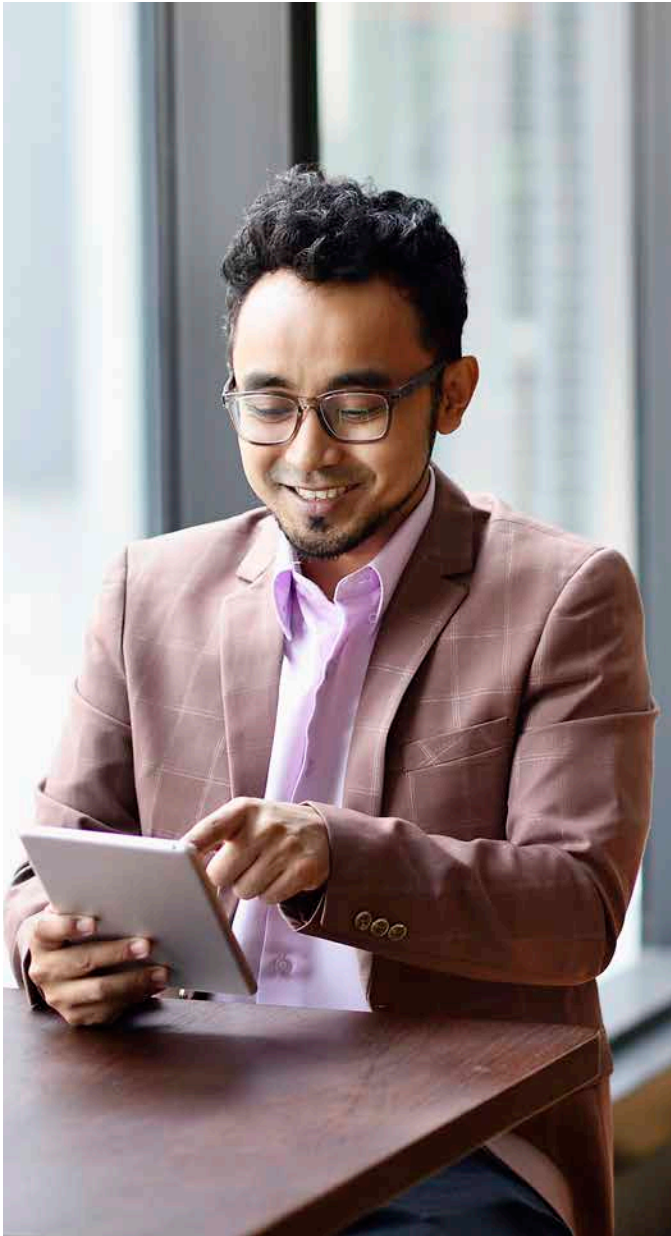
By implementing solutions that incorporate those technologies, financial institutions can be in a strong position to combat emerging threats while continuing to provide the seamless interactions that accountholders want.



Strategies 3:

Adapt to Changing Landscapes

Given the increasingly sophisticated and continually evolving nature of the threats financial services providers face, it's impossible to predict the patterns and types of fraud that can affect real-time payments. However, financial institutions can prepare for whatever comes their way by adopting solutions that offer protection for current risks with the flexibility to adapt as the threat landscape changes.



Behavioral analytics add a unique layer of protection over traditional techniques by focusing on good activity to create a baseline of what should be allowed. Anomalous deviations from that baseline help identify new fraud attacks as they emerge.

The combination of analyzing huge data sets in real-time and applying behavioral analytics enables institutions to make accurate and timely decisions, detecting and preventing fraud, and reducing friction while continually adapting to the changing behavior of consumers and financial criminals.

As financial institutions assess new solutions for combatting fraud in real-time, they may benefit from the experience of innovative technology providers. With deep expertise in technology, data science, analytics and integration, providers can become valued and trusted partners as financial services providers navigate fraud prevention in a real-time world.


The latest risk management capabilities, alongside real-time payment offerings, give financial institutions a competitive edge as they balance expectations for speed, ease and convenience with the need for secure transactions.

About the Author

Andrew Davies is vice president, global market strategy, fraud and financial crime, for Fiserv. He has 25 years of experience in financial services and risk management. In this role, he works with Fiserv customers around the world to design and deploy effective risk management solutions to mitigate financial crime risks with particular focus on compliance, money laundering and fraud.

Connect With Us

For more information about preventing real-time fraud in real-time payments:

 800-872-7882

 getsolutions@fiserv.com

 [fiserv.com](https://www.fiserv.com)

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today.

Visit [fiserv.com](https://www.fiserv.com) to learn more.