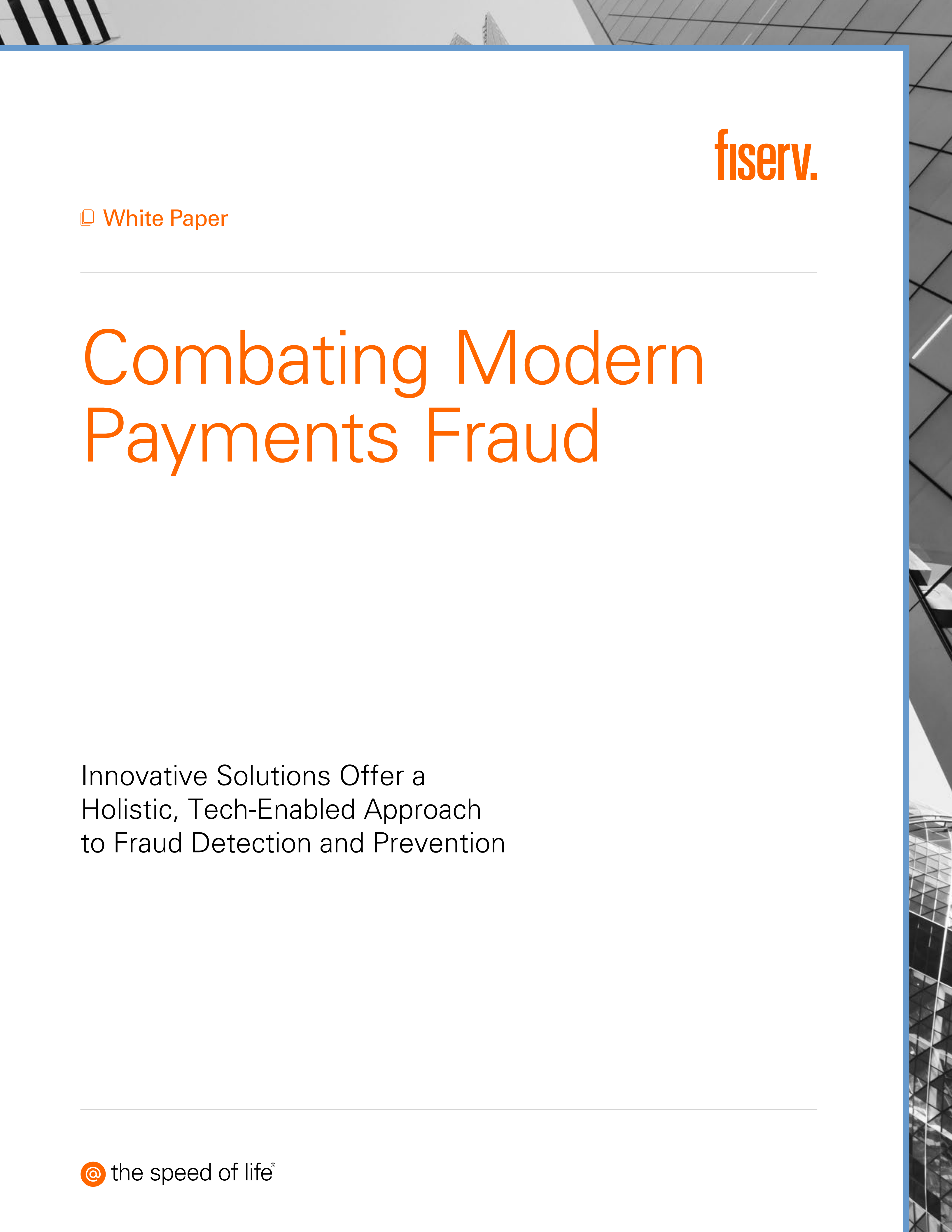


fiserv.

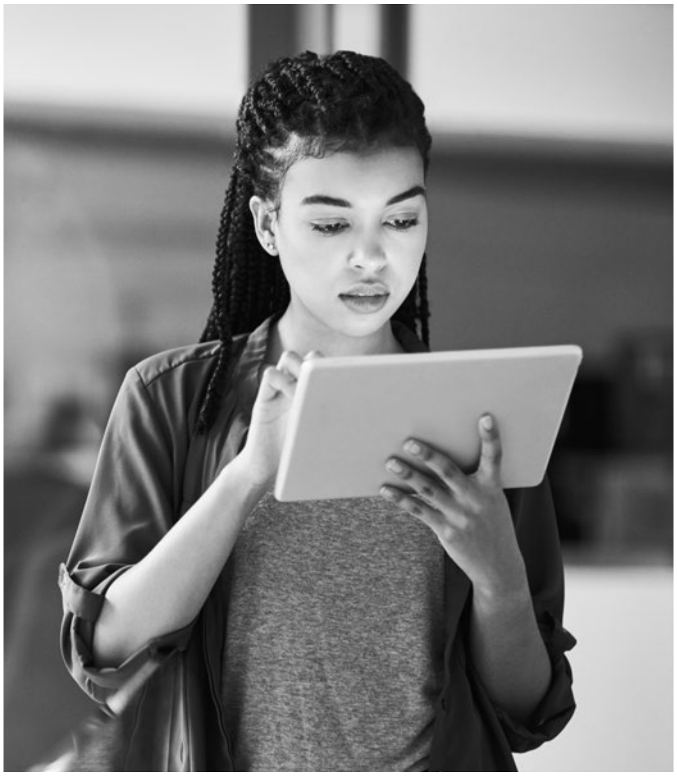
White Paper

Combating Modern Payments Fraud

Innovative Solutions Offer a Holistic, Tech-Enabled Approach to Fraud Detection and Prevention

the speed of life®

Financial institutions use anomalies to find and prevent payments fraud. When something unusual happens, it raises red flags, suspends transactions and launches mitigating actions. But what happens when typical behaviors change, such as when the pandemic shifted everyone's banking behaviors seemingly overnight? To protect accountholders without causing frustration or disrupting business operations, financial institutions need the ability to quickly redefine "normal" and adapt their security responses accordingly.



In a world of faster payments and real-time settlement, fraud prevention must move as fast – or faster than – criminals. Prevention efforts must now sync with consumer behaviors. That requires a holistic, tech-enabled approach to fraud detection and prevention.

New Risks, New Approach

Historically, fraud detection systems were designed for specific transaction types, such as card payments or ACH. But siloed efforts don't protect consumers' full financial assets and channel-specific protections have too many blind spots in a global, multichannel, multirail world.

New payment schemes, including real-time payments, forced financial institutions to rethink their approach to fraud. Securing real-time payments isn't about deploying the same risk management solutions faster. Every step of the transaction life cycle, including fraud detection, must be fast and in sync.

Similarly, financial institutions protect a range of payment methods simultaneously: ACH, checks and wires, for example. Modern fraud prevention needs to be inclusive and adaptable, enabling financial institutions to make quick and appropriate determinations based on payment methods' relative value, volume and risk.

How Prevalent Is Payment Fraud

According to the 2021 AFP Payments Fraud and Control Survey Report, 74 percent of organizations were targets of payment scams in 2020. The payment methods most affected by fraud activity continue to be checks (66 percent) and wire transfers (39 percent).

Enhanced Fraud Responses

For financial institutions, three factors can orchestrate faster, more behavior-centric fraud responses.

Integrated Organizational Data

Financial institutions reach better conclusions about fraudulent activity when they consider data points from across an organization instead of just one channel or only payment transaction data. A holistic view of customer behavior leads to more accurate detection, stronger protection and a frictionless user experience.

For example, a financial institution could look at a combination of transaction types or multiple accountholders' activities to detect malicious activity. Nonmonetary data can also provide powerful inputs, such as the type of device being used or a user's IP address and location. Previous or ongoing investigations can also influence an institution's fraud response.

Advanced Data Analytics Capabilities

Holistic and integrated information also means more information. Advanced technologies help financial institutions leverage broader data sets from multiple sources. The volume and velocity of data should be an asset for financial institutions, not an impediment.

With modern analytics approaches such as artificial intelligence (AI) and machine learning, financial institutions can apply data toward secure channel authentication and large-scale, fast fraud scoring. Real-time alerts and accurate predictive scoring help financial institutions fight fraud efficiently and effectively, while AI and machine learning help detect emerging anomalies and new, sophisticated schemes in time to protect accounts or mitigate damages.

Enhanced Collaboration

Data and intelligence are stronger when they're shared. People, processes and technology must work together to deter crime. United, they can provide better protection for accountholders and institutions.

When fraud teams, anti-money laundering programs, and IT and information security departments share data and link process, it makes it harder for fraudsters to slip through the cracks. Corporate teams should also work closely with branch staff and call center representatives. Everyone in an organization is responsible for fraud protection so everyone needs to know the red flags for fraud and be empowered to protect consumers.

Enhanced collaboration applies to the greater financial ecosystem, too. By sharing emerging threats as well as lessons learned with regulators and industry peers, financial institutions can build a stronger defense against payments fraud. Collaboration between the private and public sectors can help find and fight financial crime.

Effective Fraud Management Benefits

A successful formula for fraud protection combines integrated data, technology and collaboration. As those elements converge, they create a more holistic, timely and accurate view of the person behind the payment.

Advanced technology holds the three elements together. Technology enables advanced analytics, handles large quantities of data and facilitates collaboration. That's why advanced technology is necessary for fraud prevention to expand and adapt with the data. AI, machine learning and analytics tools help financial institutions react to consumer behavior and make optimal decisions.

With those tools, financial institutions can:

Consume and monitor huge amounts of data across channels, payment rails and devices. Evaluating massive amounts of internal and external data can help financial institutions quickly evaluate information in the context of security.

React to fraud faster and proactively. Financial institutions can use technology to halt fraudulent payments before any harm is done. AI and machine learning can spot new fraud attacks faster because they incorporate data from across the organization, instead of from just one account or accountholder.

Self-learning tools continually adapt to changing behaviors among consumers and financial criminals. That means new attack patterns are automatically incorporated as they become a threat.

Detect fraud more accurately. Analytics tools create a better baseline of "good" behavior to help financial institutions determine which payment activities should be allowed. With a larger pool of "good" and "bad" behavioral patterns to draw from, financial institutions can make better decisions.

Provide frictionless security and enhance customer satisfaction. Speed is important to the customer experience and in financial crime risk management. Financial institutions benefit from the ability to profile a transaction or accountholder and evaluate risk in real time, without delaying legitimate payments.

Modern data analytics tools can monitor and analyze huge sets of data and react to threats in milliseconds. The costs of getting it wrong – or responding too slowly – are steep. In addition to financial losses and reputational damage, financial institutions risk losing customers and members. With advanced technology and modern detection tools, financial institutions can reduce the rate of false positives and safely offer speed, convenience and security to consumers.

Work more efficiently. Adaptive, self- learning tools flag truly concerning anomalous activities, whereas traditional tools only compile lists of rule-breaking transactions. Staff don't want to clear alerts all day; they want to dig into serious threats of financial crime. Analytics tools reduce the number of required manual reviews so staff can focus on the most urgent cases.

Technology also helps pinpoint the right problem – not just the consequences of an event. And with integrated data, staff can investigate fraud faster and with more accurate outcomes.

Because AI and machine-learning tools learn from experience, financial institutions can continually enhance fraud protection without reinvesting in or manually updating their fraud management systems.

Securing the Future of Payments

Financial crime prevention strategies must scale easily with future changes even if financial institutions don't see those changes coming. Additional fraud checks need to be completed quickly while maintaining or increasing accuracy and operational efficiency.

It's not a one-person or one-department job, nor can it be done manually. Everyone in an organization can become a financial crime fighter with the right tools and support. AI, machine learning and adaptive analytics can give financial institutions an edge over payment fraudsters.

Connect With Us

For more information about financial crime technology:

800-872-7882

getsolutions@fiserv.com

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** to learn more.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045
fiserv.com

fiserv.