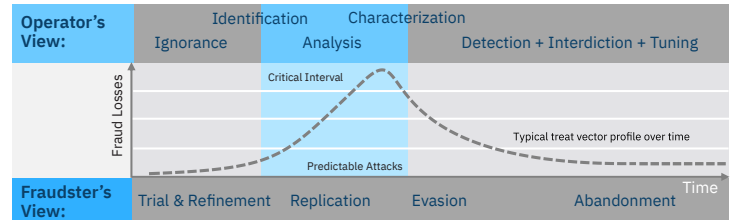# IBM Safer Payments

Real-time settlement without clawback presents fraudsters with new opportunities to innovate and attack. Dated technologies leave you exposed to exploitation. It's time for a better approach…
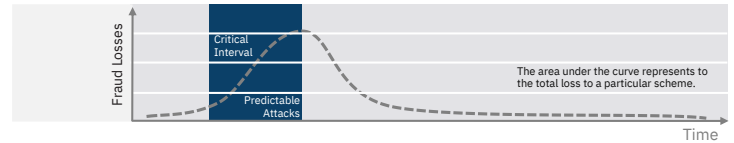

It's time for Safer Payments' Cognitive AI

Next generation Safer Payments uses purpose-built fraud detection AI to narrow the window of opportunity fraudsters have to exploit you.

Typical Fraud Scheme

Operator's View:	Identification	Characterization	
	Ignorance	Analysis	Detection + Interdiction + Tuning

Critical Interval

Typical treat vector profile over time

Predictable Attacks

Fraud Losses

| Fraudster's View: | Trial & Refinement | Replication | Evasion | Abandonment |

Time

Safer Payments' Cognitive AI

Critical Interval

Predictable Attacks

The area under the curve represents to the total loss to a particular scheme.

Fraud Losses

Time

A typical fraud scheme starts with the bad guys trying and confirming their attacks. When perfected, they hit hard and for as long as they can before a bank can put in mitigating controls. Safer Payments' Cognitive AI enables you to identify there schemes more quickly, and it suggests effective controls which can be readily deployed to production. The net result: better detection, lower false positives and a low friction client experience.
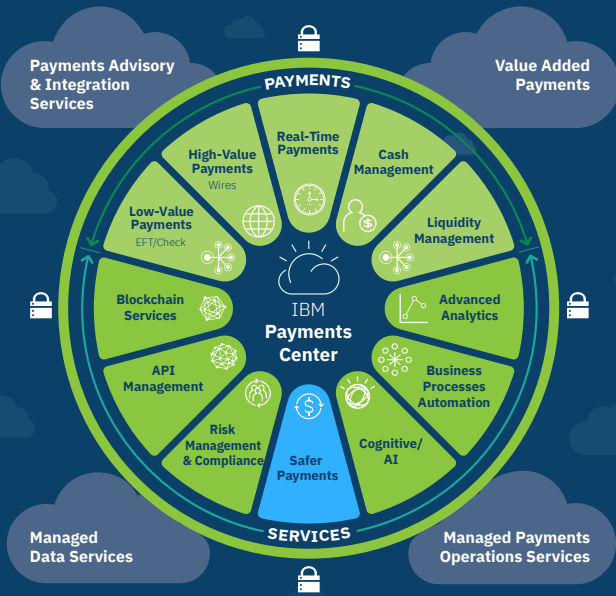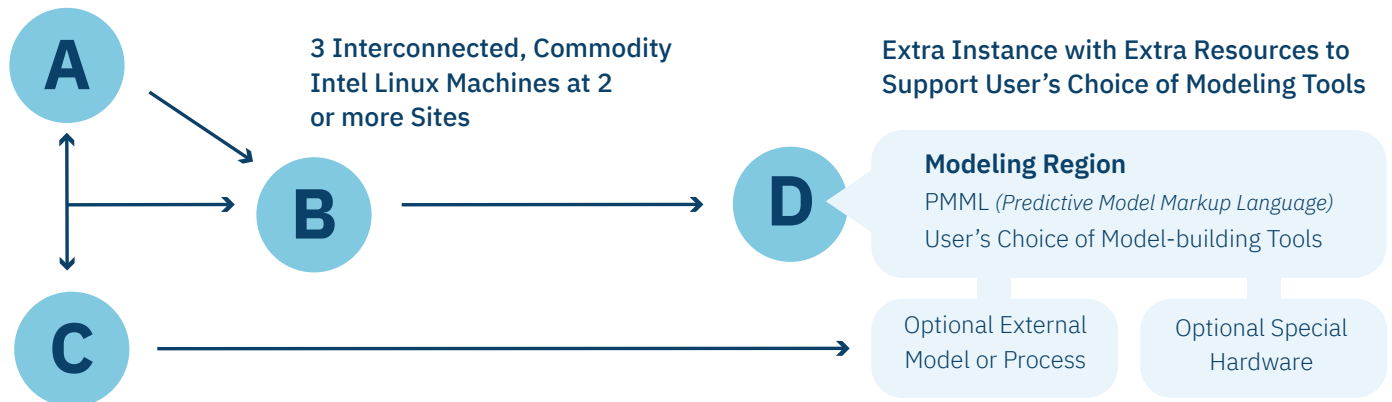

IBM Safer Payments puts modern machine learning in the hands of on-site fraud management teams, significantly improving their effectiveness and enabling them to:

- Regain autonomy to modify models and rules on demand without the long lead time and arduous data requirements traditional vendors require.

- Rapidly recognize and mitigate new fraud attacks across diverse channels and instruments.

- Protect multiple payment channels sharing data between them.

- Participate confidentially in industry collaborative initiatives: your data is secured, and your mitigation efforts benefit from the shared experiences.

- Build profile variables with point-and-click ease.

- Leverage look-back profile variables that adapt for relevance to the current transaction.

- Build neural networks, random forests, decision trees, and regressions, using your preferred tools and score transactions with comprehensive Safer Payments ensemble models.

- Improve detection by combining short-view models focused on recent fraud attacks for lowest false-positives, with long-view models trained on behavior regularities for high detection rates.

- Monitor thousands of payments per second.

- Deliver 99.999% availability for typical installations.

- PCI PA-DSS certified data protection.
- Nation-scale throughput of thousands of transactions per second.
- Cognitive tools for novice through to expert model builders.
- In-memory transaction history for rapid model and rule building, testing and deployment.

- Pin-point detection accuracy with AI generated English-language rules.
- Supports one or hundreds of concurrent tenants isolated or with controlled sharing.
- Continuous, performance monitoring with user-configured dashboards.
- Rich alert and case management with customizable workflows.

A typical on-prem configuration for nation–level volume using IBM Safer Payments

Multiple Payment Types					Multiple Payment Channels				Account Information
Wires	AFT	Immediate Payments	Cards		Mobile	Online Banking	File/API		Account Changes

A

B

C

D

3 Interconnected, Commodity Intel Linux Machines at 2 or more Sites

Extra Instance with Extra Resources to Support User's Choice of Modeling Tools

Modeling Region
PMML *(Predictive Model Markup Language)*
User's Choice of Model-building Tools

Optional External Model or Process

Optional Special Hardware

- Three identical Intel Linux virtual or physical server host duplicate Safer Payments instances. All instances are sized to handle peak volume alone, and are updated and ready to process transactions.
- Instance D is hosted on a machine with additional resources (especially disk space) to support the user's modeling tools and intermediate data files.
- All four instances have duplicate, continuously updated, in-RAM copies of the last year (configurable) of monitored transactions. Models constructed on and imported into instance D that are promoted to production are propagated to the other instances for real-time, triply redundant production operation.
- A switch to new models or rules is accomplished by switching production message flow to different instances so that no interruption of full-speed production monitoring is needed.

To learn how IBM Safer Payments can help your business, contact us:

Andrew Higgins
Leader
IBM Payments Center
ahiggins@ca.ibm.com

Monika Stilicha
Associate Partner
Digital Payments
monika.stilicha@ibm.com

Neil Ringwood
SME-Fraud & Financial
Crimes Management
ringwood@ca.ibm.com

Margaret C. Winmill
Associate Partner
Financial Services Sector
margaret.winmill@ca.ibm.com

Twitter @IBMFinTech
Learn More ibm.com/saferpayments

IBM