



What you will learn on this deck

- Why did we acquire Iris?
- What is IBM Counter Fraud Management for Safer Payments?
- What does IBM Safer Payments do?
- Why do banks need IBM Safer Payments?
- How does IBM Safer Payments achieve this level of fraud protection?
- Who are IBM Safer Payments client references?
- Where does IBM Safer Payments fit in the CFM portfolio?
- Existing Customers
- Who is the competition?
- How we compare to the competition?
- Who do we sell to and what do we ask them?
- Key capabilities

*Slides 4-12 are sales presentation focused

**Speaker Notes contain relevant information



Helping to Bring Financial Crime Prevention Into The Cognitive Era: A Human-Machine Collaboration

IBM acquires IRIS Analytics

Press release <http://ibm.co/1SS1Ted>

Why is this significant for IBM and our customers?



Industry dynamics mandate step change in speed, scale, adaptability

The entire payment ecosystem must adapt more readily to rising, episodic fraud schemes by being able to rapidly develop and deploy counter measures supporting growing data volumes and faster response rates with available skills



IBM has multiple businesses that use Iris technology to add customer value

Proven real-time payments fraud solution using advanced machine learning techniques enhances IBM's Counter Fraud Management and IBM Payments portfolios and integrates with IBM Security.



What is IBM Counter Fraud Management for Safer Payments?

Powered by IRIS, IBM Counter Fraud Management for Safer Payments is a software product for real-time **fraud prevention** in any kind of cashless* payment system through any channel**.

The system covers both detection of fraud and case management of resulting alerts

* **Cashless** such as cards, ACH, wires, SEPA, Chip & Pin, immediate payments and alternative payments solutions

** Any **channel** such as a merchant terminal, ATM, online, or mobile

IBM Counter Fraud Management for Safer Payments

*Bringing Financial Crime Prevention Into The
Cognitive Era*





What: Safer Payments enables IBM to deliver more control and transparency to combat financial crimes for players in the payments ecosystem



Fraud prevention in the cashless payment system through many channels



Bulletproof availability, operating at 99.999% availability



“White Box” anti-fraud models supporting creation/modification of ad-hoc models



Superior Industry real-time performance with latencies of a few milliseconds



Low false positive rates of 1:1-1:3 using big data analytics*



5* Performance varies but we have seen clients, such as Cartes Bancaires/STET achieve 1:1 to 1:3



Why: New payment products and channels, less time to evaluate risk, and more sophisticated fraudsters

A changing cashless payments industry...

Faster payments, rise of alternate payment methods and the adoption of new payment regulations (US adoption of Chip and Pin)

is under attack with new and sophisticated modalities...

Fraudsters are increasingly technologically sophisticated and organized, systematically probing to spot vulnerabilities and exploit them

where time to react is dramatically shorter...

There's less time to evaluate risk, so it is vital to adapt faster, spot new patterns quickly, and have the control to apply countermeasures.

and current defences are hard to adapt

Legacy solutions are often hard to adapt "black box" solutions, do not look across payment types and channels, generating too many false positives



FOR FINANCIAL SERVICES: Pressures abound to deliver an optimal Fraud Prevention Program while supporting a bank's omni-channel strategy to help drive business growth

A changing cashless payments industry...

We are moving to immediate payments, the rise of alternate payment methods, and the adoption of new payment regulations (US adoption of Chip and Pin)

is under attack with new and sophisticated modalities...

Fraudsters are increasingly technologically sophisticated and organized, systematically probing to spot vulnerabilities and exploit them

where time to react is dramatically shorter...

There's less time to evaluate risk, so it is vital to adapt faster, spot new patterns quickly, and have the control to apply countermeasures.

and current defences are hard to adapt

Legacy "black box" solutions are often hard to adapt, do not look across payment types and channels, and generate too many false positives



IBM is pioneering new cognitive capabilities to mitigate payment fraud

Exceptionally High Performance

Ultra-low false positives

Proven in real-world environments with industry-leading false positive ratios in the 1:1-1:3 range

Superior industry real-time performance

Process thousands of transactions per second with latencies of a few milliseconds

Exceptional availability

Operates at high availability, active-active-active

Cognitive computing

Democratize modeling

Machine Learning with automated model generation, limiting need for scarce data scientists

White Box approach, adapt faster

Customers can change models in minutes, understanding both lift and false positives

Virtual Analyst

Advanced analytics techniques allowing rules experts to build models with machine assistance

Payments Industry ready

Multi-tenancy with PCI-DSS

Single software installation and fully Payment Card Industry-Data Security Standard **certified**

No Downtime

Inspect the rules, use production data, review the outputs and evaluate a rule's effectiveness without stopping the system

Short Installation Cycle

Implement in full production in weeks vs months with light footprint*

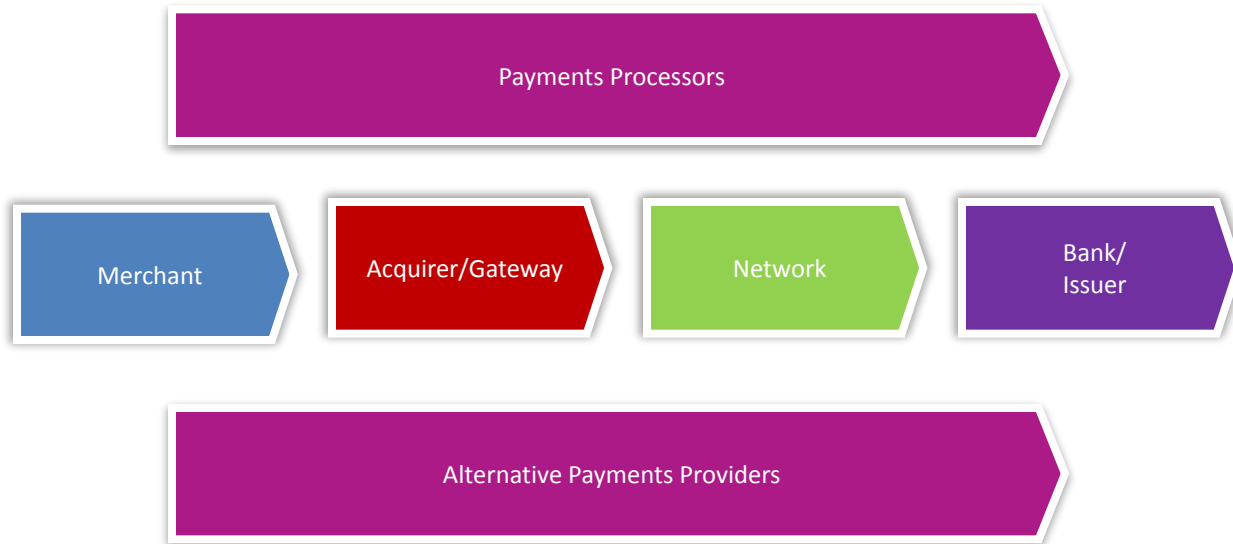


How: IBM Safer Payments create a Human-Machine partnership, enabling clients to react more quickly to evolving threats and helping make more precise decisions

Cognitive Computing approach: Helps bridge the gap between expert-driven rules and traditional predictive modeling by applying artificial intelligence to partner with human experts in suggesting best fit analytics interactively.




- **Adapt Faster (minutes, no downtime):** Adapt faster to address new episodic threats by rapidly developing, testing, and deploying countermeasures
- **More Control:** “White box” approach to analytics helps gives organizations visibility into model results, control to adapt models quickly without vendor inputs, and flexibility to apply new countermeasures in minutes by themselves without advanced skills.
- **High Speed, Scale, and Accuracy:** Process more data at faster speeds with better false positive ratios than existing fraud detection systems
- **Democratizes Modeling:** Does not require advance data science skills

IBM CFM for Safer Payments: Helping to protect the payments ecosystems



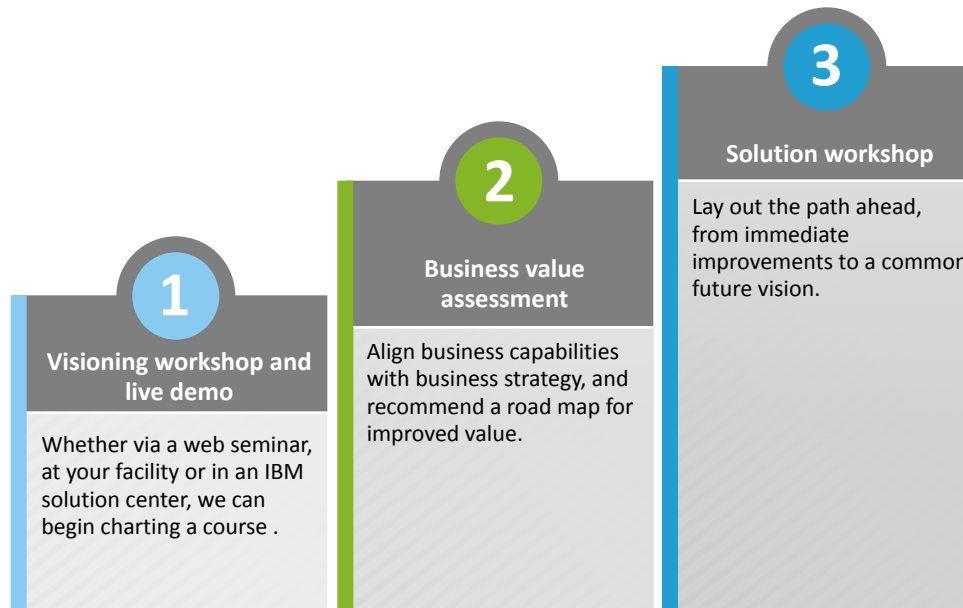


Clients who have improved their operations with IBM CFM for Safer Payments

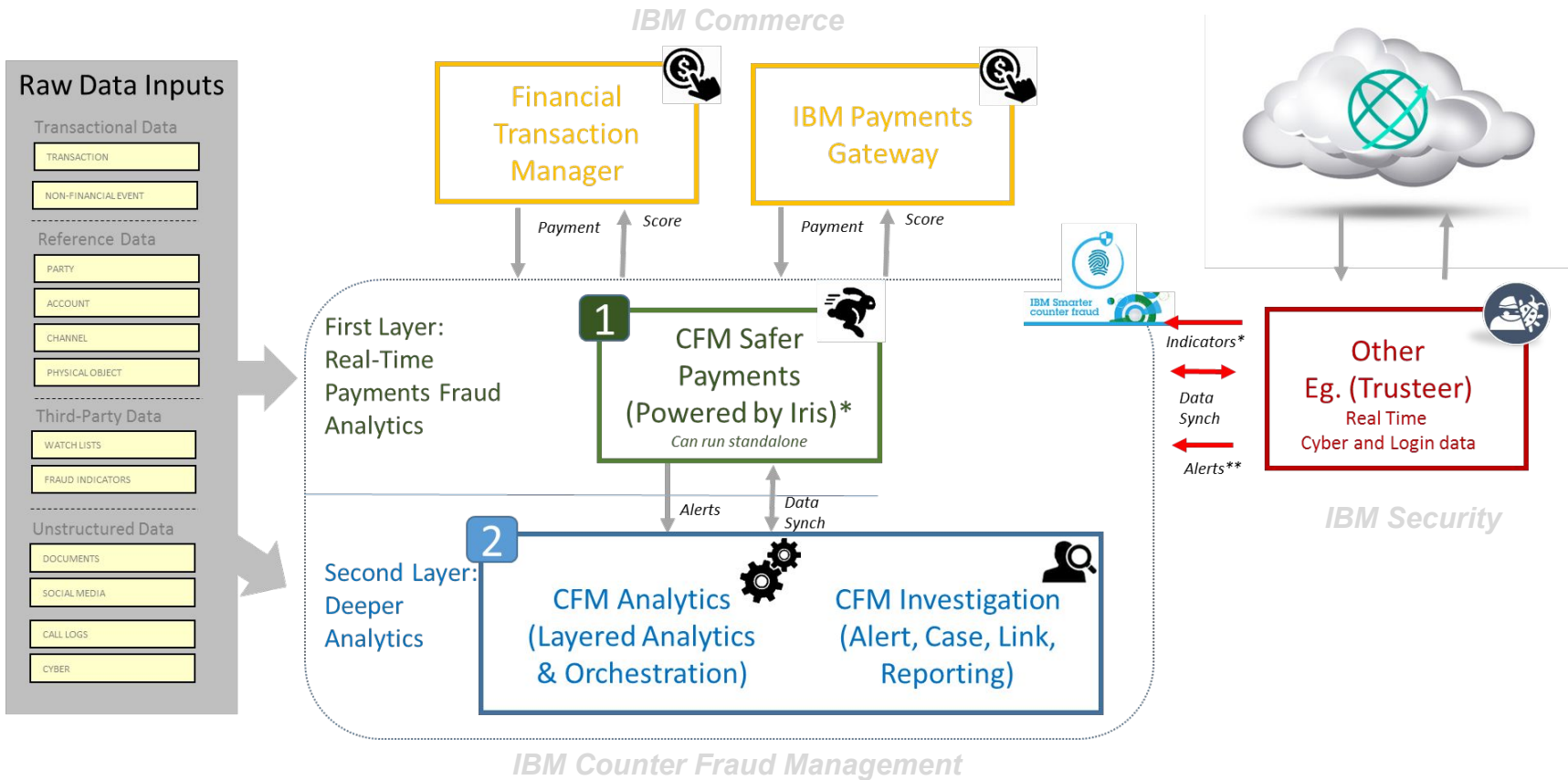
 <p>STET</p>	<p>STET the National Payment Switch for France, Live: April 2014</p> <p>€185 million annual fraud reduction</p> <p>Ultra low false positives: <1 false alarm per hit</p> <p>750 transactions/sec Sized for 4000 TPS 4.7B Card Transactions >58,500 ATMs 1.8M Merchants 61M Cards 75% of French Payments</p> <p><i>With an average response time of less than 5 milliseconds per transaction even during peak periods, IRIS (CFM Safer Payments) does not add any notable overhead to our service. In essence, we increase security while maintaining a smooth payment experience for our customers.</i> <i>Pierre Juhen, Deputy CEO STET re 01/2016 IBM Press release</i></p>
 <p>COMDATA FLEETCOR</p>	<p>The 9th biggest commercial card issuer in US including Credit, Pre-Paid Debit, Private Label cards and on-line vouchers. Live: 2007</p> <p>1BP fraud on Private Label, 2BP fraud on Mastercard branded cards</p> <p>Delivering 3x more fraud loss protection compared to industry average (5.8 BP)</p> <p>Multi-Channel Fraud Prevention \$17B - Annual Transactions 15M Cards Convenience Cheques AML Compliance First Party Fraud Prevention</p>
 <p>QIWI</p>	<p>A leading provider of next generation payment services in Russia and the CIS. Live: June 2014</p> <p>Maintained Service under large scale fraud attacks</p> <p>Stayed open while the competition had to shut down their networks</p> <p>Episodic Fraud Prevention 70M Customers 167K Kiosks 15.5M E-Wallets Visa Pre-Paid Cards 49B Rubles in Payments/Month</p>



Recommended next steps: A deep dive session with an IBM CFM for Safer Payments expert



Where: IRIS powers “CFM Safer Payments” for real-time payments fraud, including standalone & integrated offerings





Key Capabilities

Ultra High Performance

Ultra-low false positives

Proven in real-world environments with industry-leading false positive ratios in the 1:1-1:3 range*

Ultra-high real-time performance

Process thousands of transactions per second with latencies of a few milliseconds

Bulletproof availability

Operates at high availability, active-active-active

Cognitive computing

Democratize modeling

Machine Learning with automated model generation, limiting need for scarce data scientists

White Box approach, adapt faster

Customers can change models in minutes, understanding both lift and false positives

Virtual Analyst

Advanced analytics techniques allowing rules experts to build models with machine assistance

Payments Industry ready

Multi-tenancy with PCI-DSS

single software installation and fully Payment Card Industry-Data Security Standard **certified**

No Downtime

Inspect the rules, use production data, review the outputs and evaluate a rule's effectiveness without stopping the system






















Short Installation Cycle

Implement in full production in weeks vs months with light footprint



IBM Safer Payments provides clients with the tools to build detection models off their own data, and immediately deploy to detect emerging types of fraud in real time

“White Box” models; no down time, faster counter measures

		AML & Fraud vendors	Payments Fraud vendors	Pure Analytics vendors
Proven, multi-channel payments analytics and detection capabilities				
White box modelling supported by simulation (respond to episodic fraud)				
Real Time Performance & Multi-tenant scalability				
Complementary Payment Systems and Fraud Prevention capabilities				
Ability to disrupt existing players, market and client buying patterns				



How to identify and qualify an opportunity?

The Buyer



Victor

SVP of Fraud Prevention

- Prevents revenue losses due to fraud
- Manages fraud prevention organization
- Manages efficiency and effectiveness of program
- Collaborates with channel managers

*“As a SVP of Fraud Prevention, I need to keep **fraud losses**, **cost of prevention**, and **speed of response** within predictable boundaries. My boss measures me on ROI—meaning both losses and how much I spend on preventing them. I need to ensure that that ratio remains acceptable so I don’t stop the business from growing & innovating. My goal is to drive fraudsters to attack the bank next door. As **payments become faster**, EMV forces criminals to new areas, the business innovates in new higher risk channels (online, mobile), and fraudsters use technology scale up more sophisticated attacks more quickly, **my ability to keep my business predictable is getting harder.**”*

Other job titles:

- Chief Risk Officer (CRO)
- Chief Finance Office (CFO)
- SVP Fraud
- Head of Digital Banking
- Head of Digital Channels
- Head of Transaction Banking



1. Can you identify and prevent newly emerging fraud patterns?
2. How quickly can you respond with appropriate measures?
3. How easy is to test your fraud detection models before implementing them in production?
4. Do you depend on your vendor to update analytical models?
5. Can you predict the fraud detected and the false positive ratios of your detection model **before** you deploy it?
6. Are you happy with the false positive ratios in your current system?
7. What system do you use for Card fraud?
8. Are you concerned about Card-not-present fraud?
9. Who in your business deals with Corporate Cards?



Next steps and who to contact?

- Read the IBV Study: Winning the face-off of fraud
 - ibm.biz/fightingfraud
- IBM Press Announcement
 - <http://www-03.ibm.com/press/us/en/pressrelease/48788.wss>



BACKUP SLIDES



Notes on the Sales Cycle to new IBM Safer Payments Business Partners

- Ensure the solution value is clear to the prospect early in the cycle.
- Contact an IBM sales or tech sales professional to progress your opportunity to *qualified* status.
- A Safer Payments prospect is considered *validated* only after only after the pending purchase has been confirmed. A discovery call with the IBM Safer Payments team can be scheduled upon validation.
- A deal with 10 million annual transactions requires at least \$300K license and implementation budget.
- Qualifying to sell or implement an IBM Safer Payments solution requires 1 sales mastery certification and 2 technical certifications within the product group. Upon passing the IBM Counter Fraud Management Sales Mastery Test, Business Partners will be able to partner with the IBM Safer Payments team to develop and implement the sales strategy.
- Contact IBM Lab Services or GBS to complete deploying the solution.
- Contact IBM Safer Planet sales when you have an insurance industry prospect in need of a fraud solution.



Helping to Bring Financial Crime Prevention Into The Cognitive Era: A Human-Machine Collaboration

IBM acquires IRIS Analytics

Why is this significant for IBM and our

Press release <http://ibm.co/1SS1Ted>

customers?

What do clients need?

The entire payment ecosystem (Banks, Card issuers, Traditional and non traditional Payment Providers, ecommerce gateways) need to adapt more readily to rising, episodic fraud schemes by being able to rapidly develop and deploy counter measures, in real time

Why did IBM do this acquisition?

To enhance IBM's Counter Fraud Management (ICFM) Portfolio by introducing real-time payments fraud prevention using advanced machine learning techniques,. This rich function will also be incorporated into IBM Financial Transaction Manager and IBM Payments Gateway products

Why did IBM selected IRIS?

IRIS develops and delivers a real-time fraud analytics engine that leverages machine learning to generate rapid anti-fraud models while also supporting the creation and modification of ad-hoc models. IRIS is a leading player in the pan European payment fraud prevention segment and has implementations across multiple banks, payment processors and cooperatives

What do IBM and IRIS provide together?

The combination of ICFM and IRIS functionality, deployed in a 'white box approach, helps clients to spot new financial crime patterns earlier, adapt sooner and have additional control to apply countermeasures to help fight the episodic nature of constantly evolving fraud themes This helps to position IBM Counter Fraud Management as one of the industry's most comprehensive approach to enterprise financial crime management



The Value to IBM Clients

IRIS enhances the Counter Fraud Management portfolio to help enable customers to make step change improvements in effectiveness, efficiency, and adaptability in fighting fraud—and to achieve these improvements faster and at lower operating costs.

Effectiveness:

Helps to find more fraud faster using real-time detection at industry-leading speeds and scale, with clients achieving throughputs of several thousand TPS and latencies under 10 ms on tens of billions of transactions.*

- Only 56% believe they are in reasonable control of fraud and Only 16% can detect fraud as it is attempted

Efficiency:

Drastically reduces the overhead cost from processing false alerts (proven to significantly reduce false positives at top issuing banks to industry leading ratios of 1:1-1:3)*

Adaptability:

Accelerates detection strategy updating and implementation to keep pace with criminals (implemented in weeks rather than months, change models in minutes rather than days or weeks)

- 81% say it takes over 4 weeks to discover a new pattern, then another 4 weeks to adjust the scoring engines. Exposure remains, fraud still occurs

– IBM Institute for Business Value Study of Top Financial Institutions**



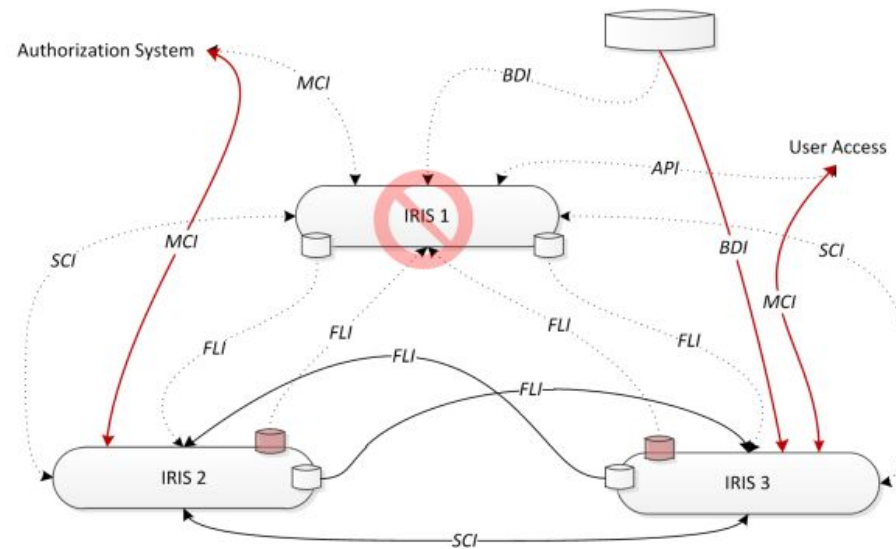
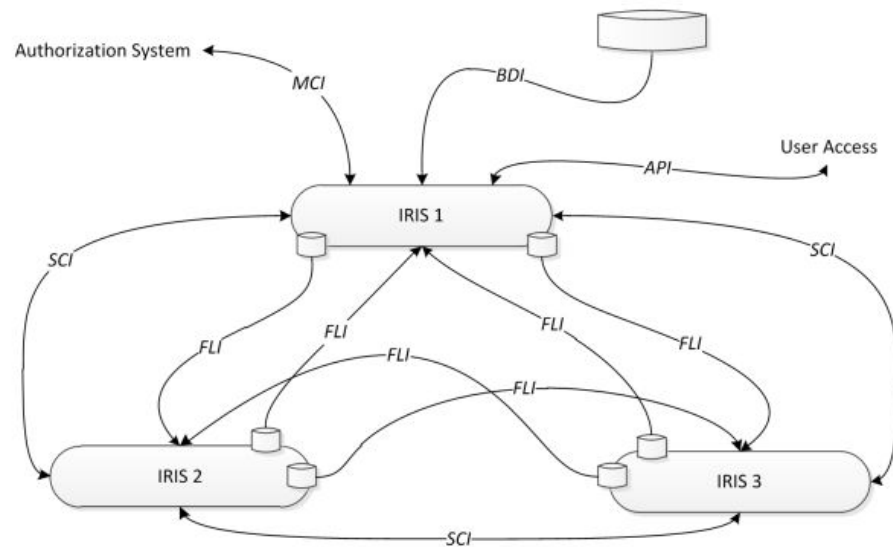
IRIS's cluster architecture

- Cluster of commodity servers provides 99.999% availability
- Architecture model similar to Google search engine
- Fully automatic failover, replication, and synchronization, no admin intervention needed
- Maximum horizontal and vertical scaling

Normal Operations



Failover





Safer Payments Concepts: Interfaces

Interfaces Overview

The IBM Safer Payments service provides multiple interfaces:

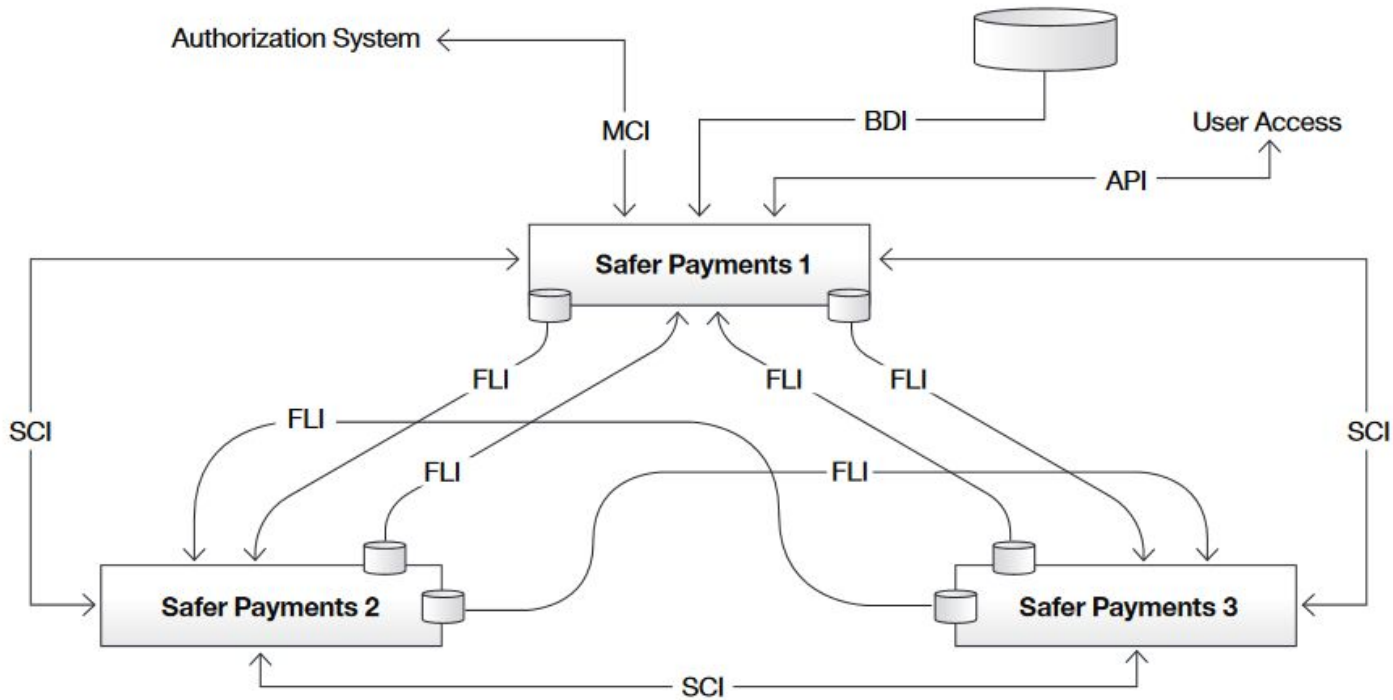
- MCI (Message and Command Interface) real-time
- API (Application Programming Interface) user access
- BDI (Batch Data Interface) files
- SCI (Status and Control Interface) cluster control
- ECI (Encrypted Communication Interface) exchanging secrets
- FLI (FastLink Interface) redundancy
- RDI (Relational Database Interface) database
- AMI (Alert Message Interface) email

While MCI, API, SCI, FLI, and AMI are IP message based message interfaces, BDI and RDI interfaces are file based for batch data.

IBM INTERNAL AND BUSINESS PARTNER USE ONLY



Safer Payments Concepts: Interfaces



Key:
MCI (Message and Command Interface) "real-time"
API (Application Programming Interface) "user"
BDI (Batch Data Interface) "files"
SCI (Status and Control Interface) "cluster control"
ECI (Encrypted Communication Interface) "secrets"
FLI (FastLink Interface) "redundancy"
RDI (Relational Database Interface) "database"
AMI (Alert Message Interface) "email"

IBM INTERNAL AND BUSINESS PARTNER USE ONLY



Safer Payments Concepts: Interfaces

The MCI, API and FLI interfaces operate in "service mode", where each communication is initiated by the outside party and IBM Safer Payments replies to each request. With these interfaces, the IP connections typically stay open for more than one request (for reasons of efficiency). This rather simple communication scheme keeps interfacing to IBM Safer Payments easy. It follows the time tested model of most Internet protocols, where the service consumer (often a browser) polls data from the service provider (often an HTTP server) whenever it needs to. For performance reasons, all three IP based interfaces use thread pool technology.

The BDI interface is quite different from the others because it involves transferring data in and out of IBM Safer Payments via files. Because this requires IBM Safer Payments to become active at specific times to check if data to be imported is available or if data should be delivered to other systems, IBM Safer Payments features a job schedule function.

While MCI and BDI are "external" interfaces in the sense that they connect IBM Safer Payments to systems of the customer, API and FLI are "internal" interfaces in the sense that they connect IBM Safer Payments components. They buffer transaction and control negotiation between all nodes within the cluster in the case of a node failure. The API connects the IBM Safer Payments client and the IBM Safer Payments server, the FLI connects different IBM Safer Payments instances within a cluster.

The RDI is a batch file interface using SQL statements to transfer IBM Safer Payments data into a relational database.

The AMI uses SMTP to send emails and text messages to users, administrators, customers, and cardholders/merchants.

IBM INTERNAL AND BUSINESS PARTNER USE ONLY

Message Command Interface (MCI) communicates directly with the authorization system, making it the appropriate messaging interface to receive real time transactions.

Message and Command Interface

Messaging and Command Interface (MCI) connects IBM Safer Payments to authorization systems, card management systems and related data sources. Example: Consumers.

Uses TCP/IP message passing, either as “naked” XML messages or XML messages wrapped in HTTP.

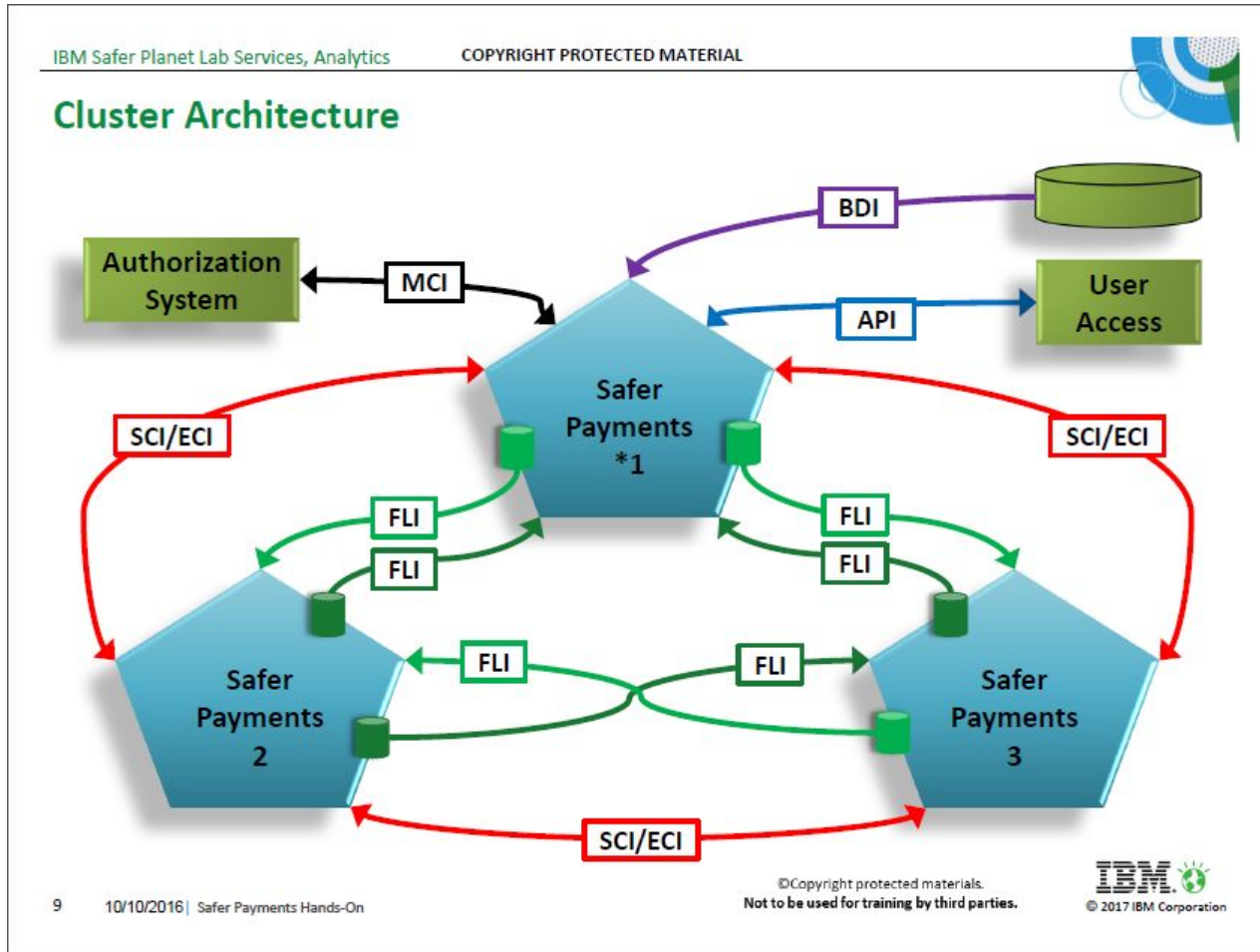
Recommended to leave the connection open between request/response pairs, as persistent connections allow for a much higher transaction message throughput and lower resource consumption.

Normal operating conditions, IBM Safer Payments will never close a connection. However, certain error conditions may cause IBM Safer Payments to close the connection. For instance a malformed message request. Closes connection as it cannot tell when the next message starts, so it cannot parse it. FastLink buffer is filled above critical threshold.

Consumer must implement watchdog approach. If IBM Safer Payments has not replied to a request within allotted time or closes the connection, the service consumer must send the message to the next available IBM Safer Payment instance.

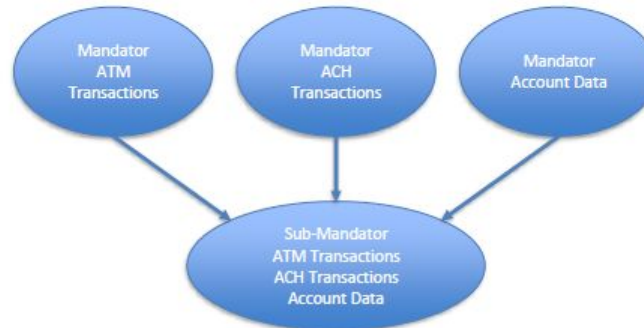


FastLink Interface (FCI) maintains transaction synchronization between all nodes in the cluster.





Mandator/Sub-mandator



Mandator: Also known as the “Top Mandator”. Represents a logical (often also physical) unit that combines model revisions, access privileges, investigation, users, query and reports. Typically represents a customer of a processor or a sub-portfolio.

Sub-mandator: A composition or subset of a mandator or multiple mandators.



Competition

Approach	Vendor	Website
Analytics Real-time neural network; extensive profiling; rules overlay; adjustment models; case mgt. Random Forests model	FICO	http://www.fico.com/en/about-us
	ACI	http://www.aciworldwide.com/products-and-services/payments-fraud/fraud-detection-and-aml/proactive-risk-manager.aspx
	SAS	http://www.sas.com/en_us/industry/banking/fraud-management.html
	Feedzai	https://www.crunchbase.com/organization/feedzai#/entity
	NuData	https://nudatasecurity.com/nudetect/
Rules and Profiling Generally have strong profiling, hierarchical rules management, external statistical tuning easier to configure for multiple channels.	Actimize	http://www.niceactimize.com/fraud-detection-and-prevention/payment
	BAE Systems	http://www.baesystems.com/en/cybersecurity/capability/financial-crime
	Accertify	http://www.accertify.com/en/solutions/fraud-management/
Merchants	Cybersource	https://www.cybersource.com/products/fraud_management/decision_manager/
	Kount	http://www.kount.com/products/kount-central



IBM's Commitment to Counter Fraud Management

Value to Clients Delivering more power in fighting fraud

Improvements in effectiveness, efficiency, and adaptability all while doing it faster and at lower total cost.



Advancing State of the Art Technology in Financial Crime

IBM extends its vision for applying layers of advanced analytics to achieve an enterprise wide, holistic approach to controlling fraud



Immediate Impact, Future Potential

Today tackle payments fraud space with IBM CFM and Payments portfolios.
Tomorrow, Next-generation for Anti Money Laundering and non-financial transactions





THANK YOU