SECUREPAYMENTS • ACADEMY
AMERICA'S PAYMENTS EXPERTS

Symposium on Securing the IoT

www.securepaymentsacademy.com

FRAUD PREVENTION EMPLOYING NEW ALGORITHMS FOR BIG DATA ANALYTICS

by Mansour Karimzadeh

March 7, 2018

Topics

Introductions

- IoT Security & Fraud
- IoT Security Technologies
- Multi Layered Conceptual Security Model
- Big Data Analytics
- Big Data Rules - Algorithms
- Data Analytics Examples
- Future of Fraud Prevention

IoT Security

"The cybercriminals who initiated the attack managed to commandeer a large number of internet-connected devices (mostly DVRs and cameras) to serve as their helpers".

IoT network security: Protecting and securing the network connecting IoT devices to back-end systems on the internet.

What is Fraud

- Fraud is a moving target
- As new security systems are created, fraudsters become more aggressive
- In banking - cardholder Primary Account Number is the main target, in other devices IDs
- There are many different types of fraud
- There is no one solution to combat all types of card fraud
- Different techniques must be used to counter the fraudulent activities

Examples of Fraud

Online/ Intercept

Counterfeit

Lost/Stolen

ID Theft

Mail non-received

IoT Security Technologies

Network Security: securing the network connecting IoT devices to back-end systems on the internet.

Authentication: Providing the ability for users to authenticate an IoT device

Encryption: Encrypting data at rest and in transit between IoT edge devices and back-end systems.

PKI: Providing complete X.509 digital certificate and cryptographic key and life-cycle capabilities.

Security Analytics: Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting.

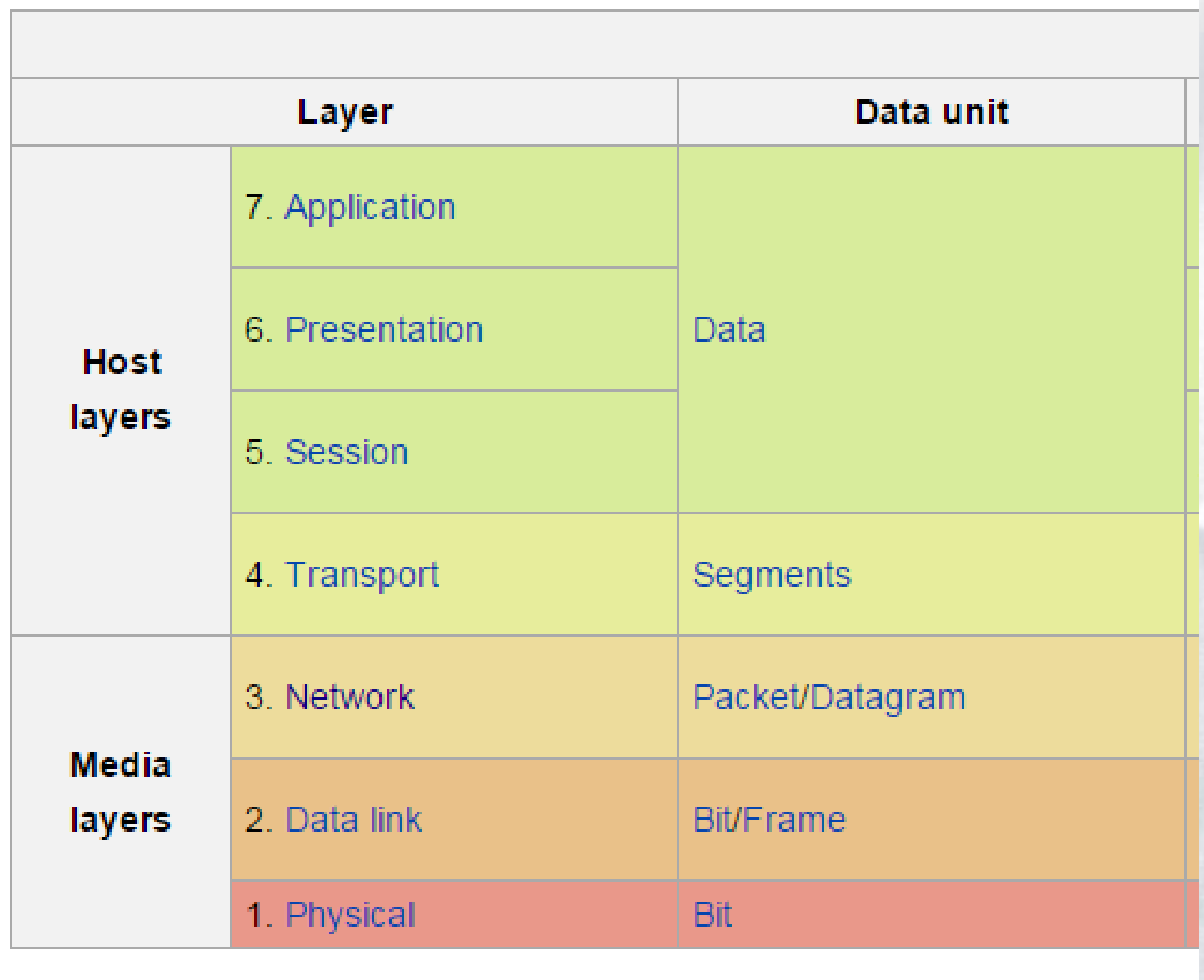
API Security: Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST-based APIs.

Multi Layered Approach

- To combat different types of fraud, multi layered approach is needed
- The technologies that play vital role and are based encryption are:
  - Chip – physical/logical (HCE)
  - Tokenization
  - Big Data Analytics

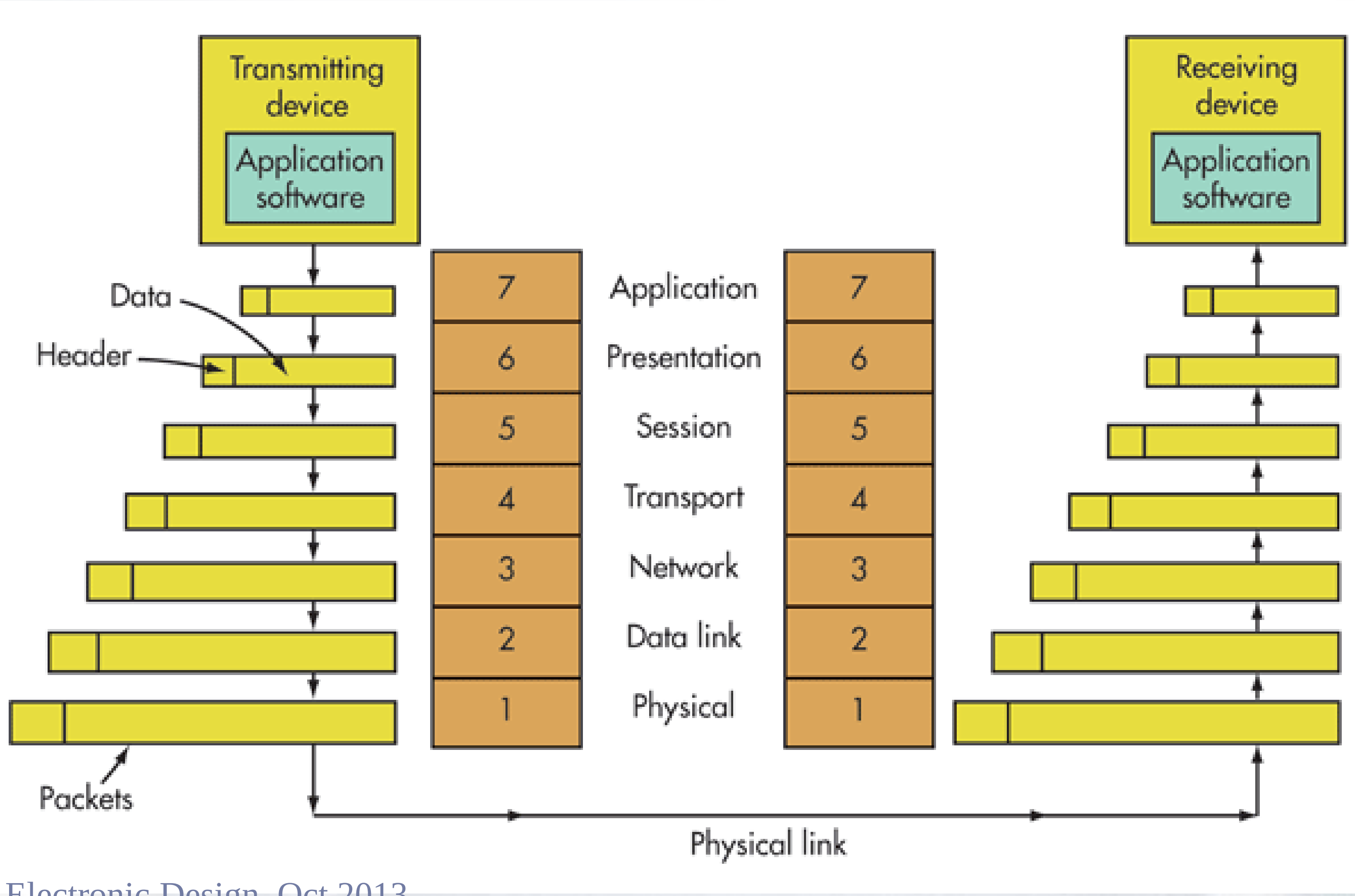
Conceptual Model for Communications

- Allows any two different systems to communicate, regardless of underlying structure
- Facilitates communications between different systems
- Does not require changes to the logic of underlying hardware or software
- Not a protocol
- A Model for a flexible, robust and interoperable network



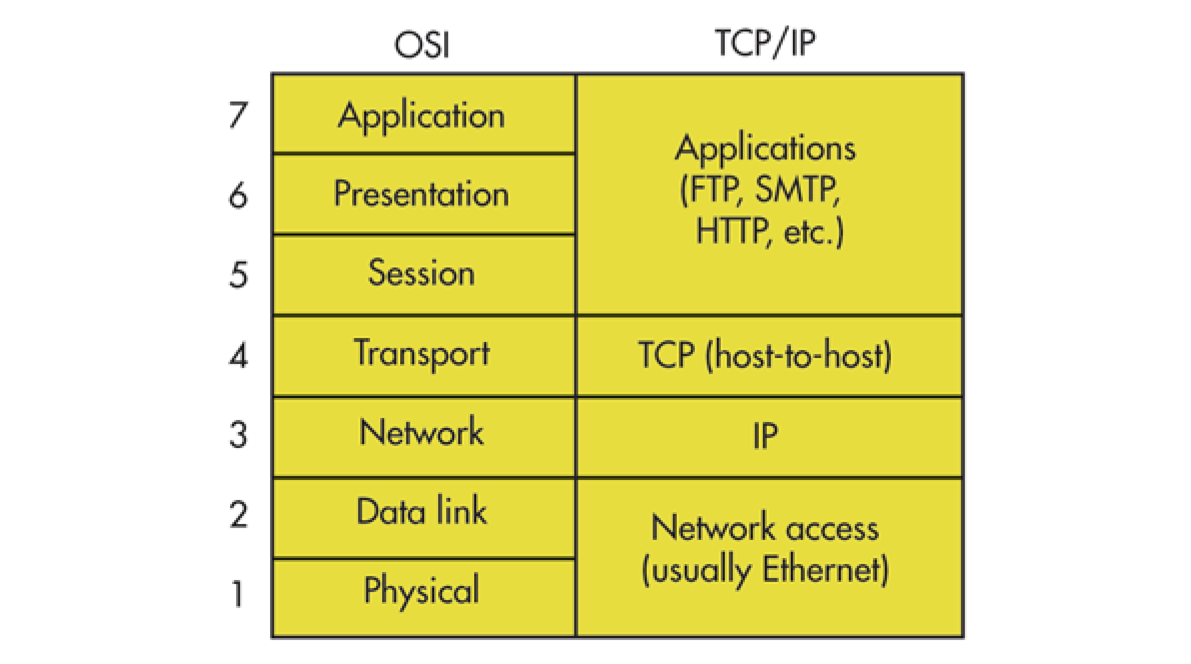
Layer		Data unit
Host layers	7. Application	Data
	6. Presentation	
	5. Session	
	4. Transport	Segments
Media layers	3. Network	Packet/Datagram
	2. Data link	Bit/Frame
	1. Physical	Bit

Communications Model Security Detail



Lou Frenzel, Electronic Design, Oct 2013

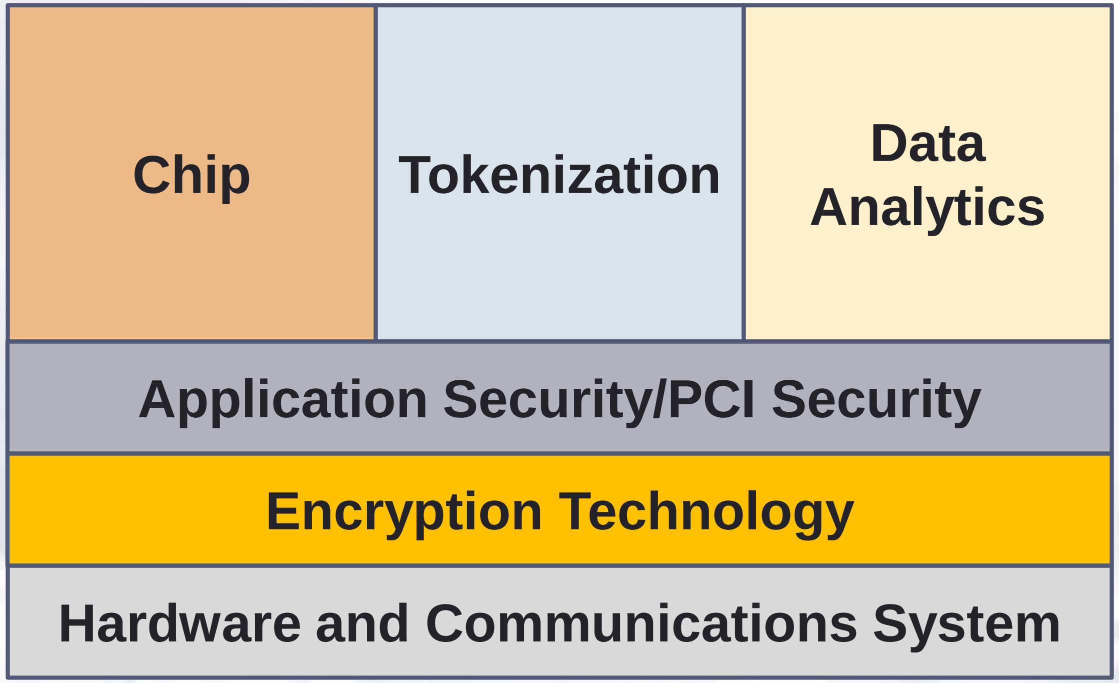
Comparison of OSI Model with LAN Model



	OSI	TCP/IP
7	Application	Applications (FTP, SMTP, HTTP, etc.)
6	Presentation	
5	Session	
4	Transport	TCP (host-to-host)
3	Network	IP
2	Data link	Network access (usually Ethernet)
1	Physical	

http://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip

Conceptual Security Model – Example Payment



Chip

Tokenization

Data Analytics

Application Security/PCI Security

Encryption Technology

Hardware and Communications System

Big Data Analytics

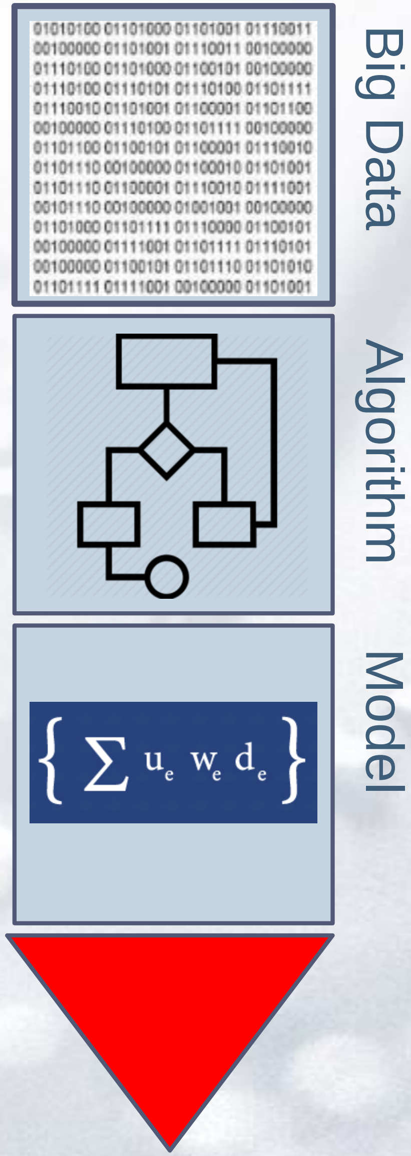
- Typically considered for petabytes of data
- As storage costs shrink, storage of all data becomes relatively cheap
- Using data you have
- Do not throw away details
- Real time and Retrospective Analysis
- Reports on Trends, Unusual Behavior or Activities
- Alerts

Phases of Big Data Analytics

- Data Collection
- Monitoring by Rules, Algorithms
- Alerting Anomalies when outside Rules

Big Data Rules - Algorithms

- Data by itself is useless - data must be analyzed, interpreted, and acted on to be useful
- Algorithms or Rules — not data sets — that will prove transformative.
- Rules allow system to monitor many aspects of a service.
- Critical, potentially critical, and seemingly inconsequential events can be automatically monitored, eliminating the potential for operator error.
- Alerts can be created as the event happens.
- Both simple and complex rules can be built allowing a service to be defined and monitored.   Rules can be combined.
- Multiple actions can be configured to run when a rule is broken.



Monitoring Rules Action

- Actions are associated with a rule and will execute if it breaks.
- Various actions can be configured:
  - Send a message (e:Mail / SMS)
  - Run a Batch file.
  - Run a script.
  - Execute a program.
  - Generate an SNMP trap.
  - Send a message to another Enterprise Manager.
- A rule may have any number of actions configured.

Alerts

- Employed when a rule is broken to alert specific operators.
- Alerting Roles define shift patterns.
- They consist of a number of Alert Users.
- Each Alert User has an associated Alert Period.
- Each Alert Period has an Alert Method.
- Analytics Systems can handle multiple Alerting Roles.
- Alerting Roles are used to determine what operator is alerted when a rule is broken.

Big Data Analytics

Things We Can Do with Big Data:

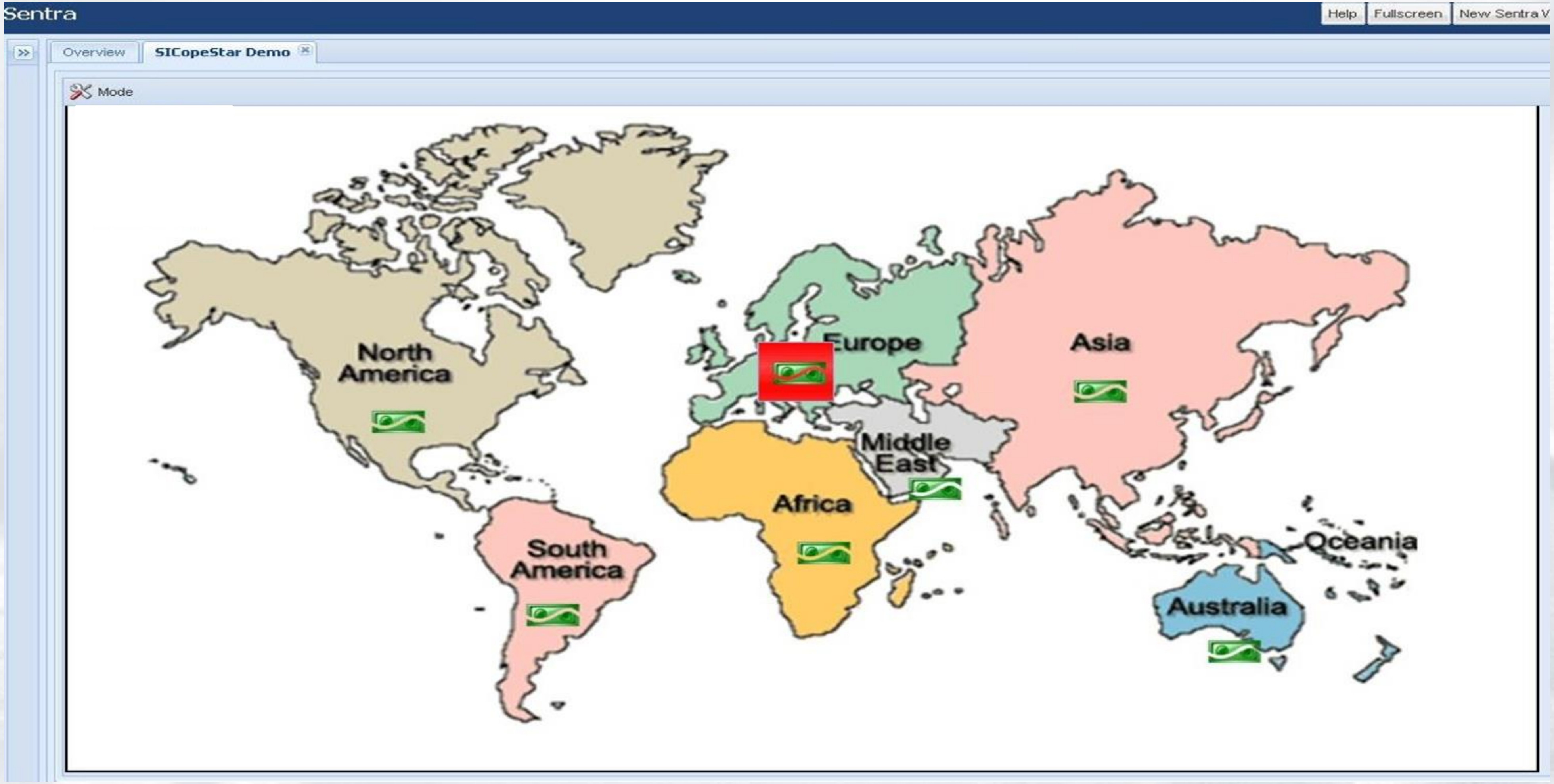
- Anticipate User Behavior and Patterns
- Integrate to Add Greater Value
- Initiate Action on fraud as it Commences
- Incorporate Social Media and Alert to Changing trends
- Monitor the Complete infrastructure

Examples – Retail Banking

- In the retail banking sector, Big Data analytics is used to track and to interrogate a continuous stream of authorization transactions from POS and ATM devices.
- The volume of such transactions typically reaches >300 transactions per second. The systems are benchmarked at over 1,000 transactions per second
- It forms a front-line business tool for real-time analysis and anti-fraud treatment of the whole “flow”

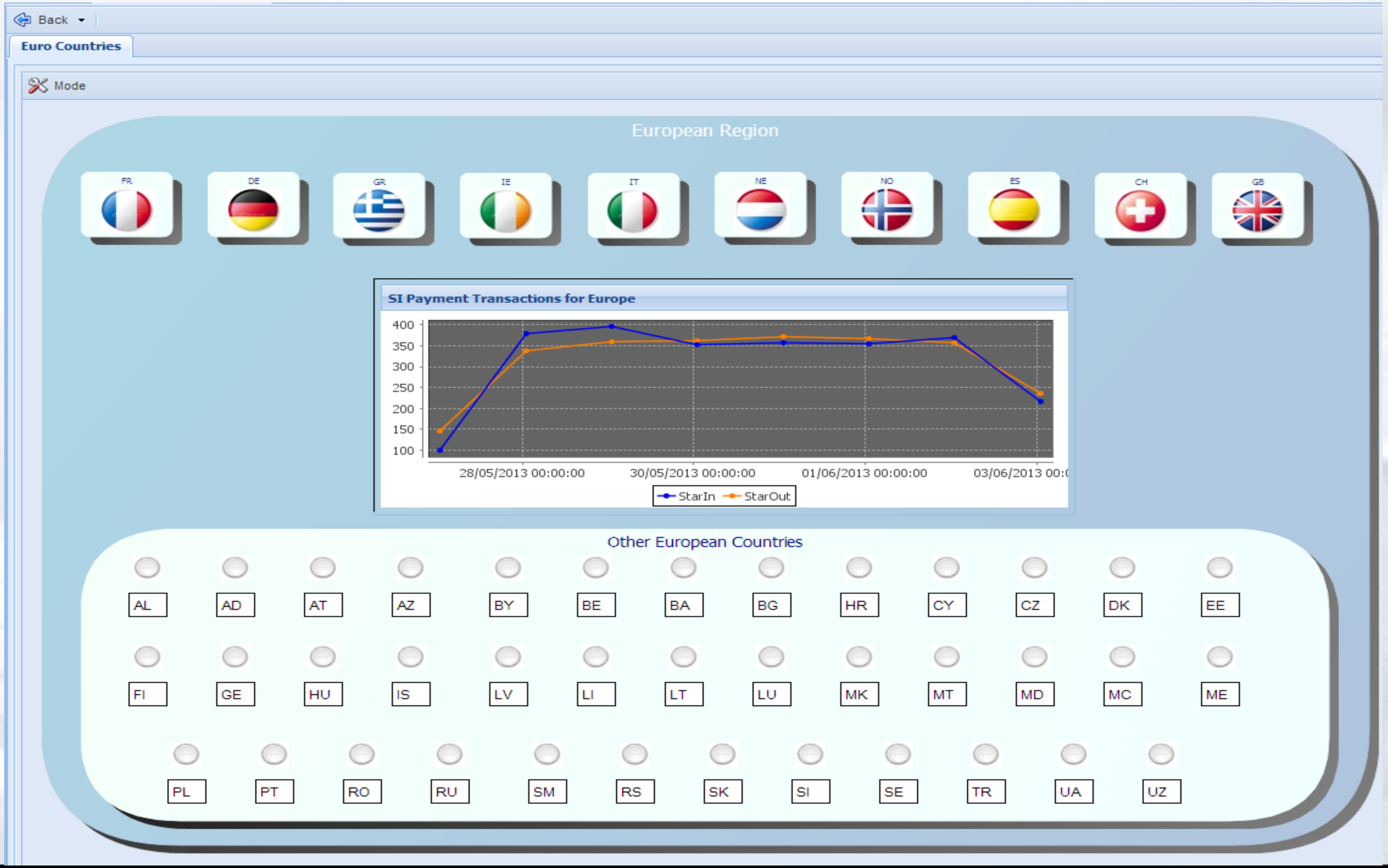
Highlighting Payment Problems by Region

Global payment operations can be monitored from a single view.



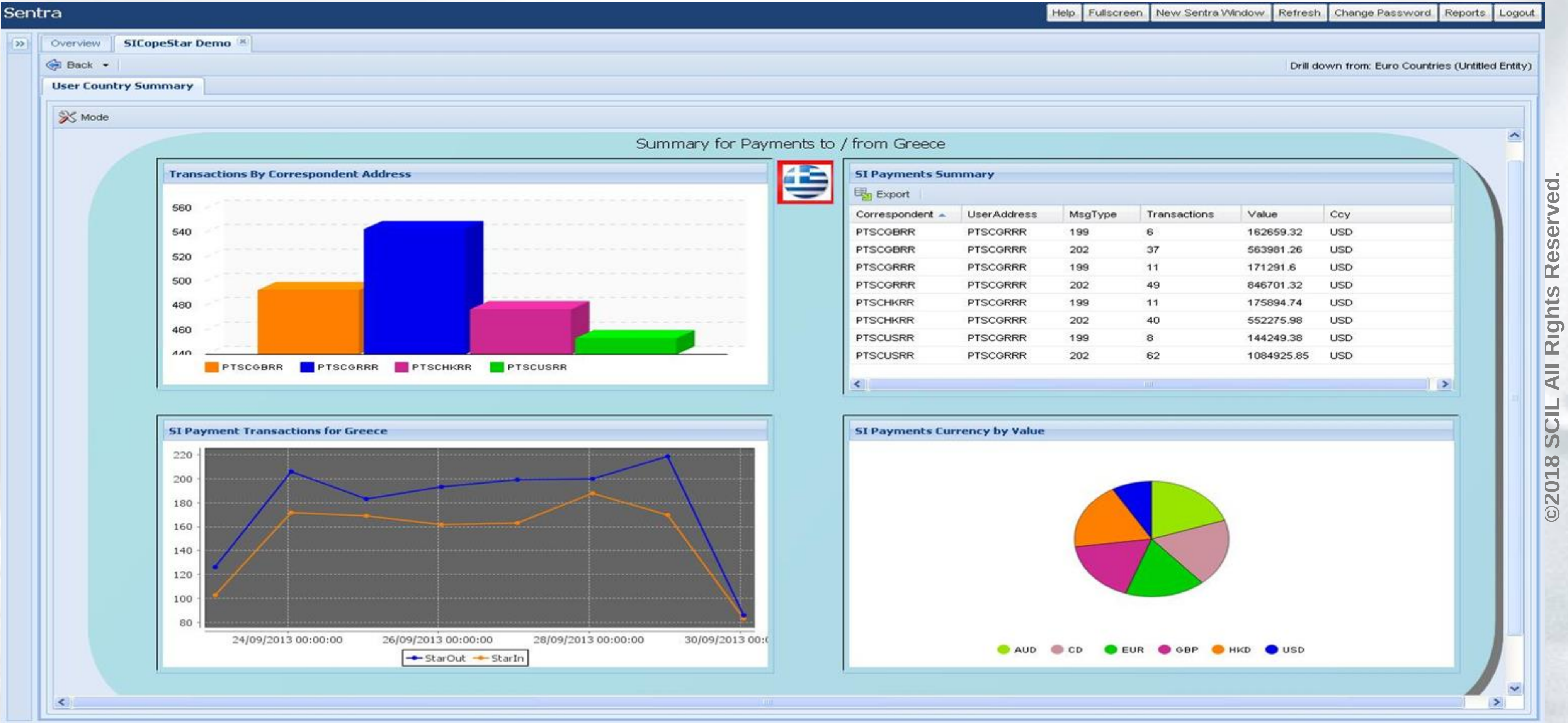
Viewing Transaction by Country

- Drilldown to EU region to view incoming and outgoing transactions by country.
- Primary EU countries are provided at the top of the view.
- Row-level security can be configured , e.g. so that regional departments only see data relevant to their country + region



Control Dashboard

Drilldown to individual country to view more detailed transaction data.

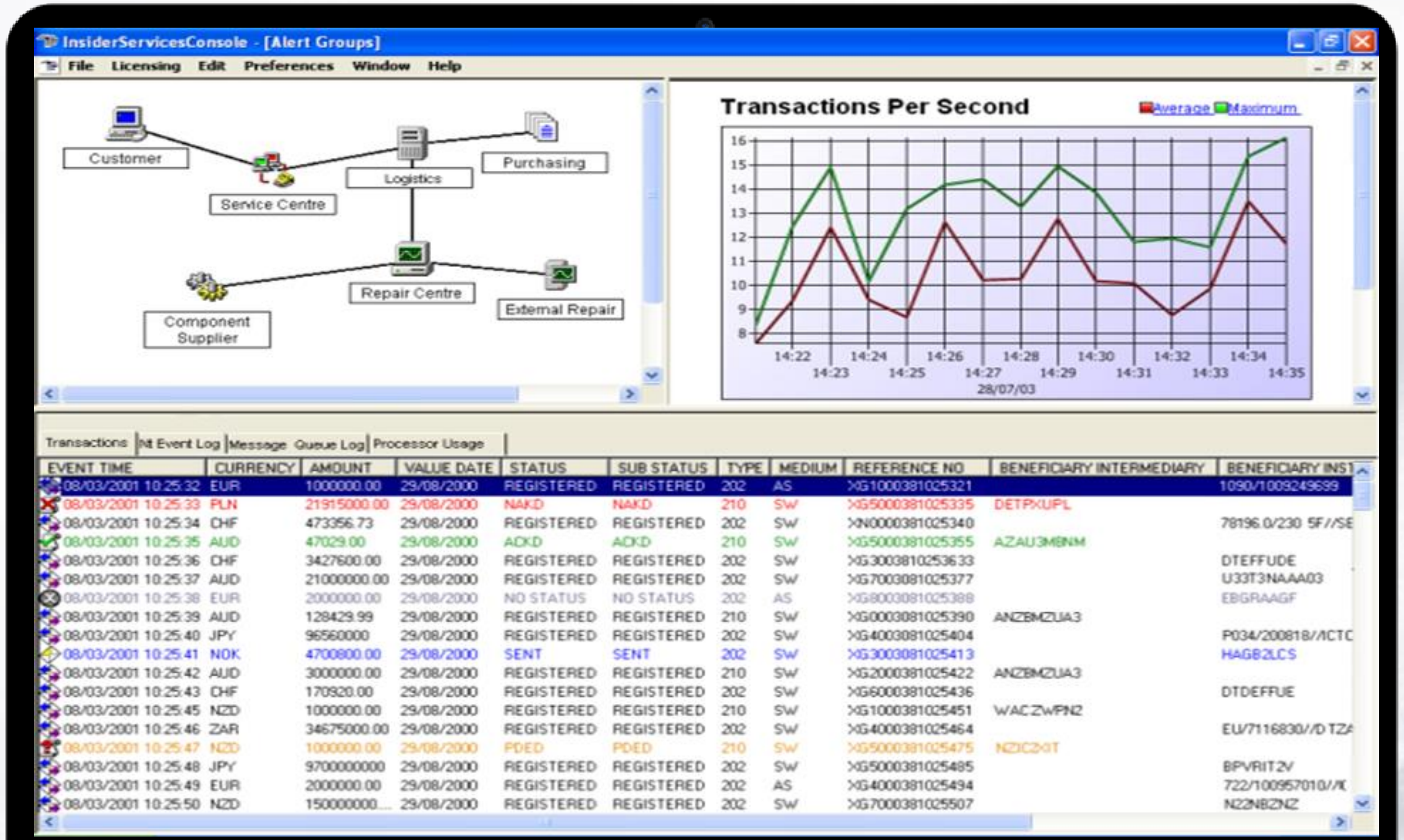


Summary for Payments to / from Greece

SI Payments Summary

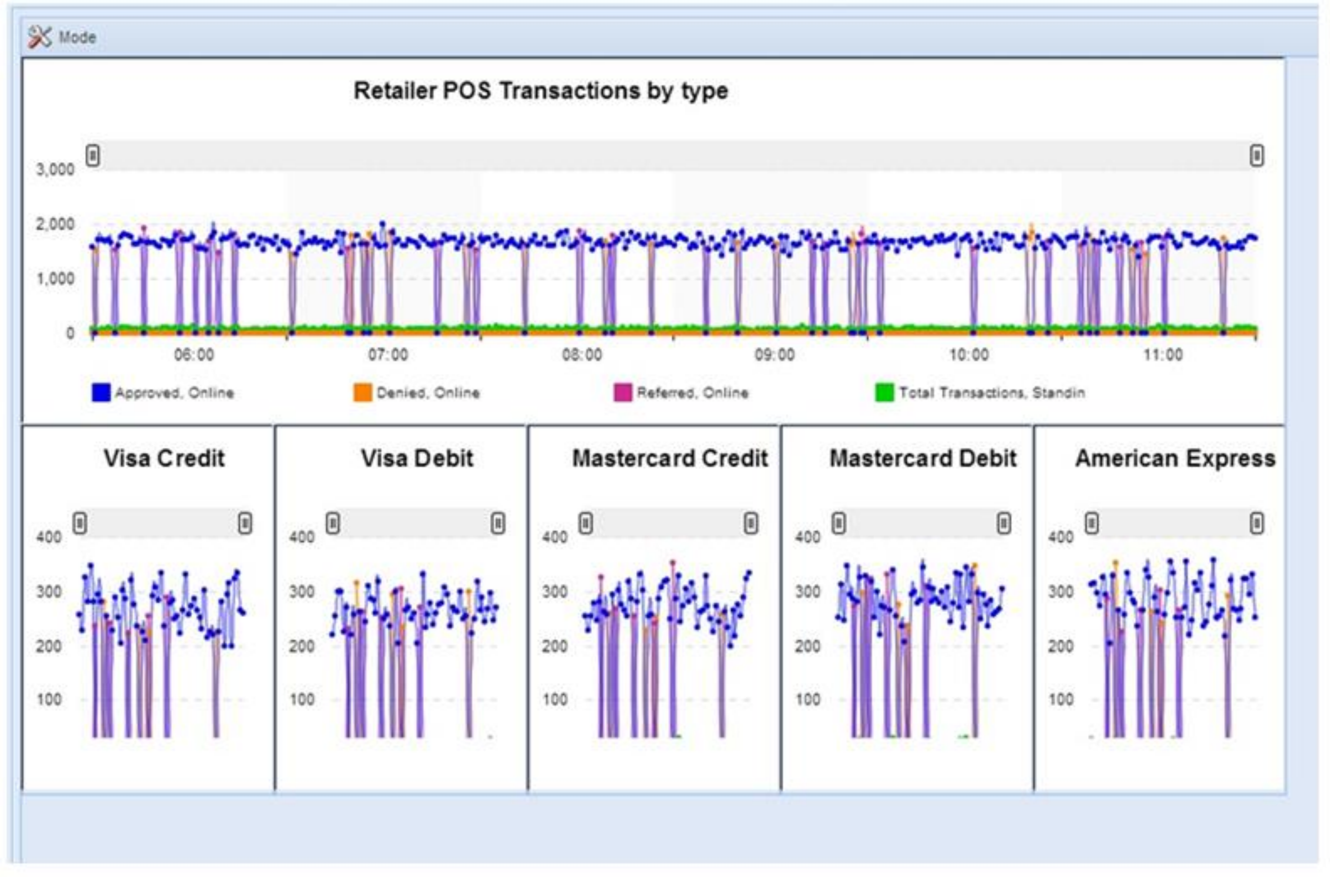
Correspondent ▲	UserAddress	MsgType	Transactions	Value	Ccy
PTSCGBRR	PTSCGRRR	199	6	162659.32	USD
PTSCGBRR	PTSCGRRR	202	37	563981.26	USD
PTSCGRRR	PTSCGRRR	199	11	171291.6	USD
PTSCGRRR	PTSCGRRR	202	49	846701.32	USD
PTSCHKRR	PTSCGRRR	199	11	175894.74	USD
PTSCHKRR	PTSCGRRR	202	40	552275.98	USD
PTSCUSRR	PTSCGRRR	199	8	144249.38	USD
PTSCUSRR	PTSCGRRR	202	62	1084925.85	USD

Financial System Monitoring



EVENT TIME	CURRENCY	AMOUNT	VALUE DATE	STATUS	SUB STATUS	TYPE	MEDIUM	REFERENCE NO	BENEFICIARY INTERMEDIARY	BENEFICIARY INST
08/03/2001 10:25:32	EUR	1000000.00	29/08/2000	REGISTERED	REGISTERED	202	AS	XG1000381025321		1090/1009249699
08/03/2001 10:25:33	PLN	21915000.00	29/08/2000	NAKD	NAKD	210	SW	XG5000381025335	DETPXUPL	
08/03/2001 10:25:34	CHF	473356.73	29/08/2000	REGISTERED	REGISTERED	202	SW	XN0000381025340		78196.0/230 5F//SE
08/03/2001 10:25:35	AUD	47029.00	29/08/2000	ACKD	ACKD	210	SW	XG5000381025355	AZAU3MBNM	
08/03/2001 10:25:36	CHF	3427600.00	29/08/2000	REGISTERED	REGISTERED	202	SW	XG300381025363 3		DTEFFUDE
08/03/2001 10:25:37	AUD	21000000.00	29/08/2000	REGISTERED	REGISTERED	202	SW	XG7003081025377		U33T3NAAA03
08/03/2001 10:25:38	EUR	2000000.00	29/08/2000	NO STATUS	NO STATUS	202	AS	XG8003081025388		EBGRAAGF
08/03/2001 10:25:39	AUD	128429.99	29/08/2000	REGISTERED	REGISTERED	210	SW	XG0003081025390	ANZBMZUA3	
08/03/2001 10:25:40	JPY	96560000	29/08/2000	REGISTERED	REGISTERED	202	SW	XG4003081025404		P034/200818//ICTC
08/03/2001 10:25:41	NOK	4700800.00	29/08/2000	SENT	SENT	202	SW	XG3003081025413		HAGB2LCS
08/03/2001 10:25:42	AUD	3000000.00	29/08/2000	REGISTERED	REGISTERED	210	SW	XG2000381025422	ANZBMZUA3	
08/03/2001 10:25:43	CHF	170920.00	29/08/2000	REGISTERED	REGISTERED	202	SW	XG6000381025436		DTDEFFUE
08/03/2001 10:25:45	NZD	1000000.00	29/08/2000	REGISTERED	REGISTERED	210	SW	XG1000381025451	WACZWPN2	
08/03/2001 10:25:46	ZAR	34675000.00	29/08/2000	REGISTERED	REGISTERED	202	SW	XG4000381025464		EU/7116830//D TZA
08/03/2001 10:25:47	NZD	1000000.00	29/08/2000	PDED	PDED	210	SW	XG5000381025475	NZICZXIT	
08/03/2001 10:25:48	JPY	9700000000	29/08/2000	REGISTERED	REGISTERED	202	SW	XG5000381025485		BPVRIT2V
08/03/2001 10:25:49	EUR	2000000.00	29/08/2000	REGISTERED	REGISTERED	202	AS	XG4000381025494		722/100957010//K
08/03/2001 10:25:50	NZD	150000000...	29/08/2000	REGISTERED	REGISTERED	202	SW	XG7000381025507		N22NBZNZ

Transaction Types in Data Analytics



The Future of Security

- Security goes hand in hand with all internet transactions
- As transactional information evolves into new channels, innovative security techniques are created
- The distinction between physical and online interactions becoming less
- As these new transactional channels re created, security will need to keep up
- Big Data Algorithms will use more Machine Learning and AI to detect fraudulent behavior

ABOUT SCIL/Secure Payments Academy

- Full sales, marketing and technical consultancy and software solutions provider
- Specialist expertise in:
  - Payment transaction processing systems
  - EMV credit/debit smart card solutions
  - Mobile payments and enterprise security
- Services:
  - Payments Training workshops
  - Consultancy
  - Business requirements studies
  - Marketing, sales and business development

CONSULTING SERVICES

Presenter

Mansour A. Karimzadeh

- Brings nearly 25 years of experience and leadership - including implementation of smart card based payment and transaction processing systems in the financial industry.
- Implementation of many large secure card and payment processing projects worldwide specializing in EMV cards and systems - including projects in the UK, Canada, USA, Latin America, Middle East and Australia.
- Served as Board member of Global Platform.
- Served as Board Member of the EMV Migration Forum’s (now US Payments Forum - USPF) Steering Committee. USPF is tasked with harmonizing and promoting the rollout of EMV in the U.S. Currently Co-Chair of its Communications & Educations Committee.
- Previously served as VP of Operations and Director of EMV and Smart Cards Unit at ACI Worldwide.

CONTACTS

- Stewart Chalmers, Executive Director & CMO
- Secure Payments Academy:
- +1-818-681-3588
- stew@emvacademy.com

- **www.securepaymentsacademy.com**

- Mansour A. Karimzadeh, CEO & Program Director
- Secure Payments Academy
- +1-516-338-8880
- mansour@emvacademy.com