Catch them in the Act

Fraud Detection in Real-time

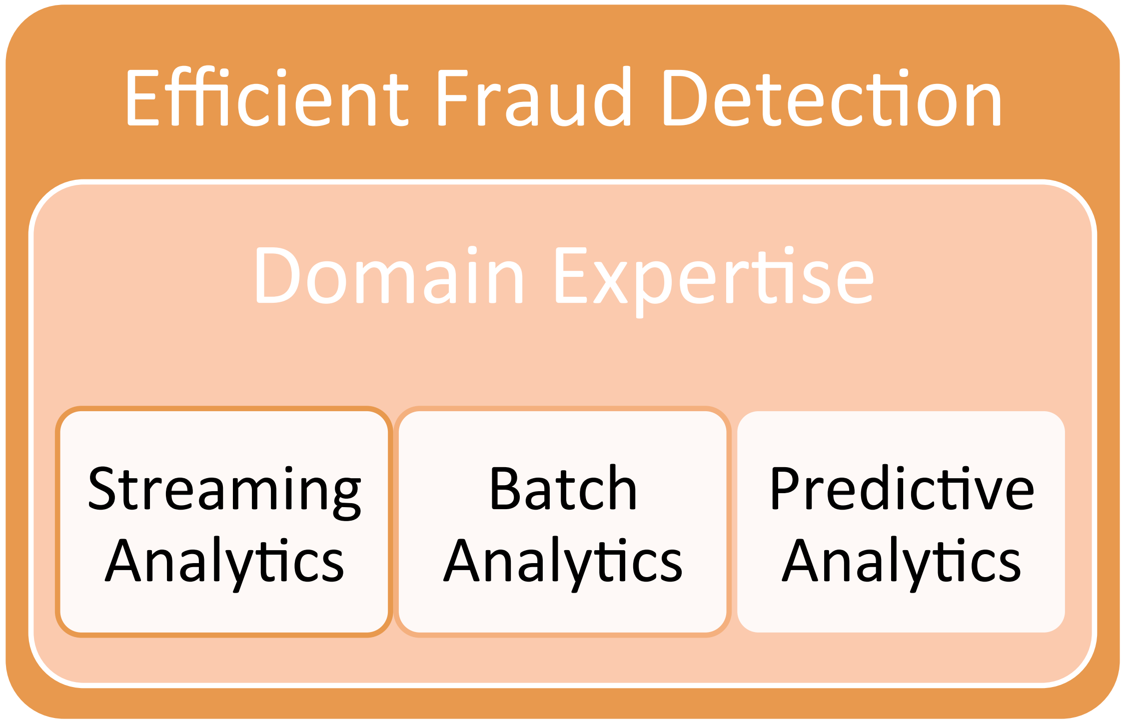
Seshika Fernando

Technical Lead, WSO2

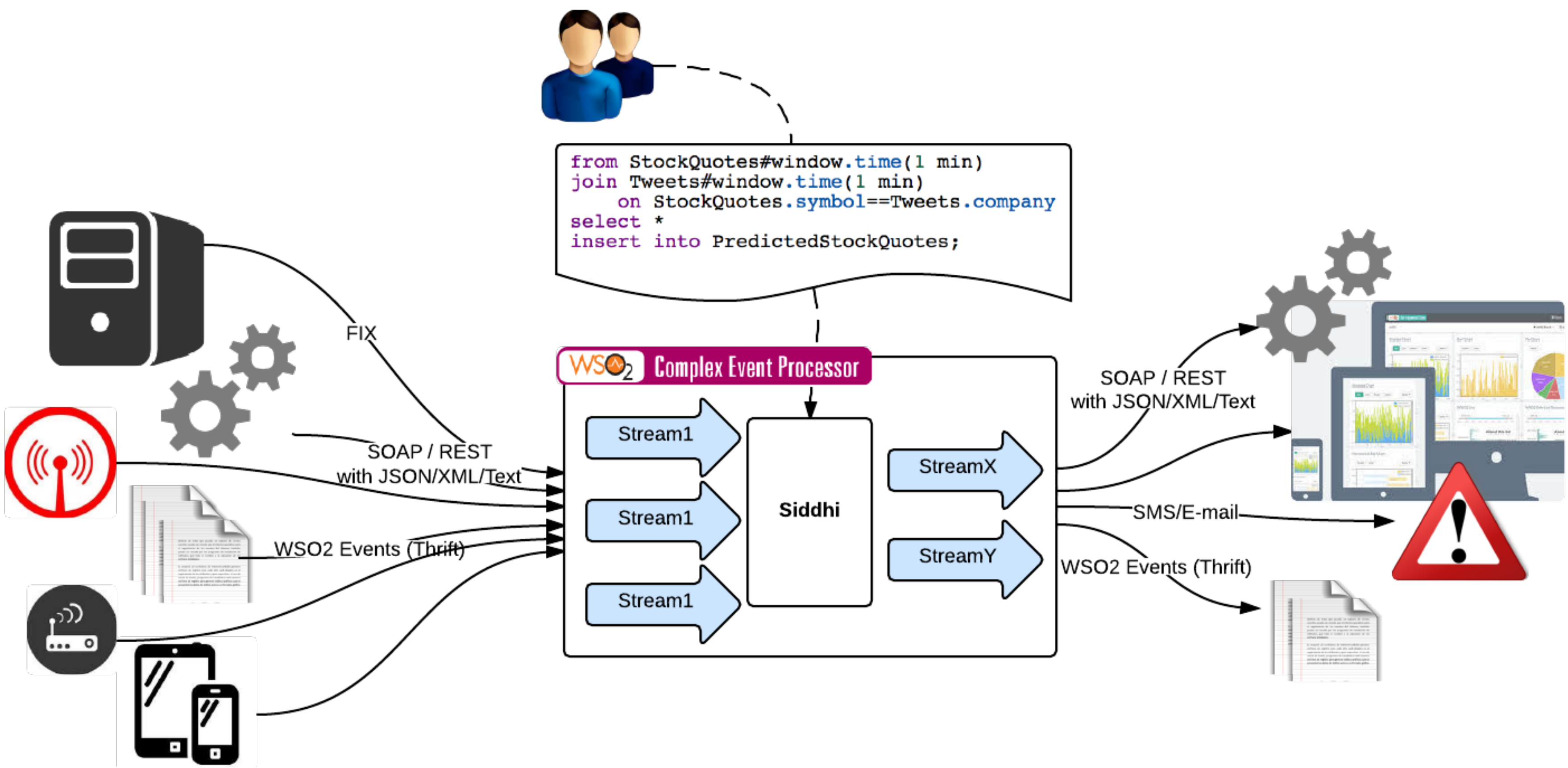
seshika@wso2.com

$4 Trillion in Global Fraud Losses

That's 5% of Global GDP


Efficient Fraud Detection
Domain Expertise
Streaming Analytics
Batch Analytics
Predictive Analytics

Complex Event Processing



Notify if there is a 10% increase in overall trading activity AND the average price of commodities has fallen 2% in the last 4 hours

Many ways

- Generic Rules
- Fraud Scoring
- Markov Models
- Machine Learning

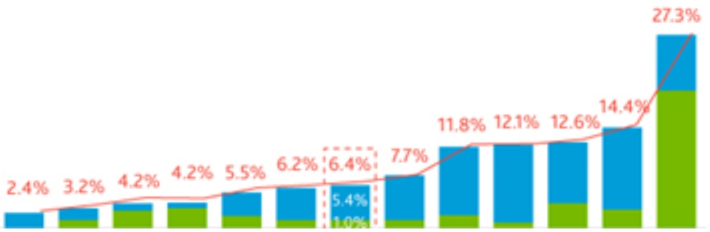
Domain Expertise → Generic Rules

Typical Credit Card Fraudster

- Use stolen cards
- Buy Expensive stuff
- In Large Quantities
- Very quickly
- At odd hours
- Ship to many places
- Get rejected often

→ CEP Queries

Moving Averages




```
from TransactionStream#window.time(60 min)
select itemNo, avg(qty) as avg, stdev(qty) as stdev
group by itemNo
update AvgTbl as a
on itemNo  ==  a.itemNo;


from TransactionStream
[itemNo== a.itemNo and qty > (a.avg + 2*a.stdev) in AvgTbl as a]
select *
insert into FraudStream;
```

Transaction Velocity

```
from    e1 = TransactionStream ->
        e2 = TransactionStream[e1.cardNo == e2.cardNo] <2:>
within 5 min
select e1.cardNo,  e1.txnID,  e2[0].txnID,  e2[1].txnID
insert into FraudStream
```

The False Positive Trap

◉ So what if I buy Expensive stuff	Rich guy
◉ And why can't I buy a lot	Gift giver
◉ Very Quickly	Impulse Shopper
◉ At odd hours	Night owl
◉ Ship to many places	Many girlfriends?

Blocking genuine customers could be counter productive and costly

How to avoid False Positives

- Use combinations of rules
- Give weights to each rule
- Single number that reflects many fraud indicators
- Use a threshold to reject transactions

- You just bought a Diamond Ring?
- You bought 20 Diamond Rings, in 15 minutes at 3am from an IP address in Nigeria?

How to score

Score =

0.001 * itemPrice

+ 0.1 * itemQuantity

+ 2.5 * isFreeEmail

+ 5 * riskyCountry

+ 8 * suspicousIPRange

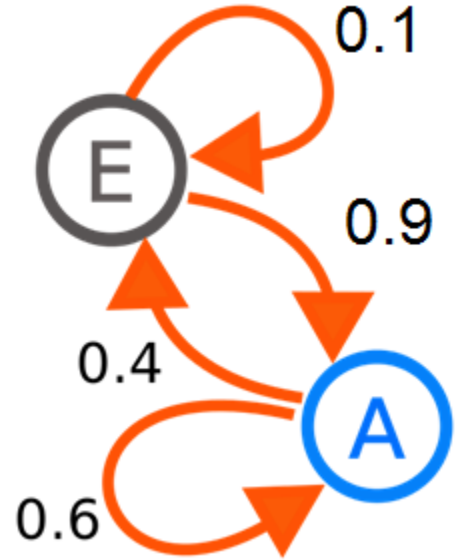
+ 5 * suspicousUsername

+ 3 * highTransactionVelocity


Are we safe ?

Markov Models

- Model randomly changing systems
- Detect rare activity sequences using
  - Classification
  - Probability Calculation
  - Metric Calculation



Markov Models: Classification

Each transaction is classified under the following three qualities and expressed as a 3 letter token, e.g., HNN

- *Amount spent: **L**ow, **N**ormal and **H**igh*
- *Whether the transaction includes high price ticket item: **N**ormal and **H**igh*
- *Time elapsed since the last transaction: **L**arge, **N**ormal and **S**mall*

Markov Models: Probability Matrix

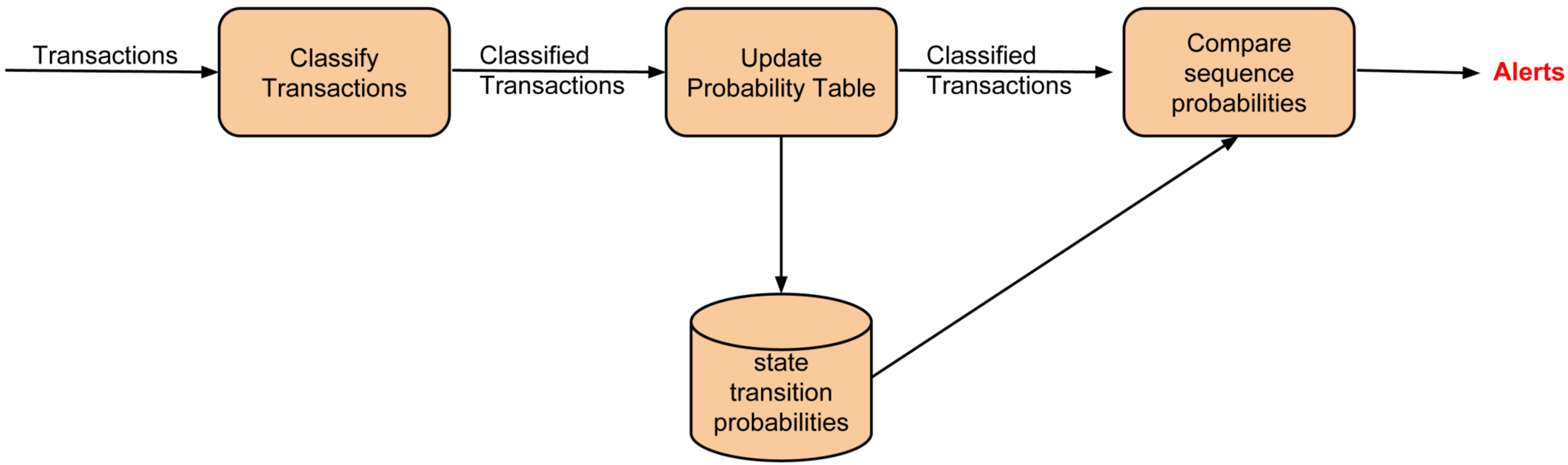
- Create a State Transition Probability Matrix

	LNL	LNH	LNS	LHL	HHL	HHS	HNS
LNL	0.976788	0.542152	0.20706	0.095459	0.007166	0.569172	0.335481
LNH	0.806876	0.609425	0.188628	0.651126	0.113801	0.630711	0.099825
LNS	0.07419	0.83973	0.951471	0.156532	0.12045	0.201713	0.970792
LHL	0.452885	0.634071	0.328956	0.786087	0.676753	0.063064	0.225353
HHL	0.386206	0.255719	0.451524	0.469597	0.810013	0.444638	0.612242
HHS	0.204606	0.832722	0.043194	0.459342	0.960486	0.796382	0.34544
HNS	0.757737	0.371359	0.326846	0.970243	0.771326	0.015835	0.574333

Markov Models: Probability Comparison

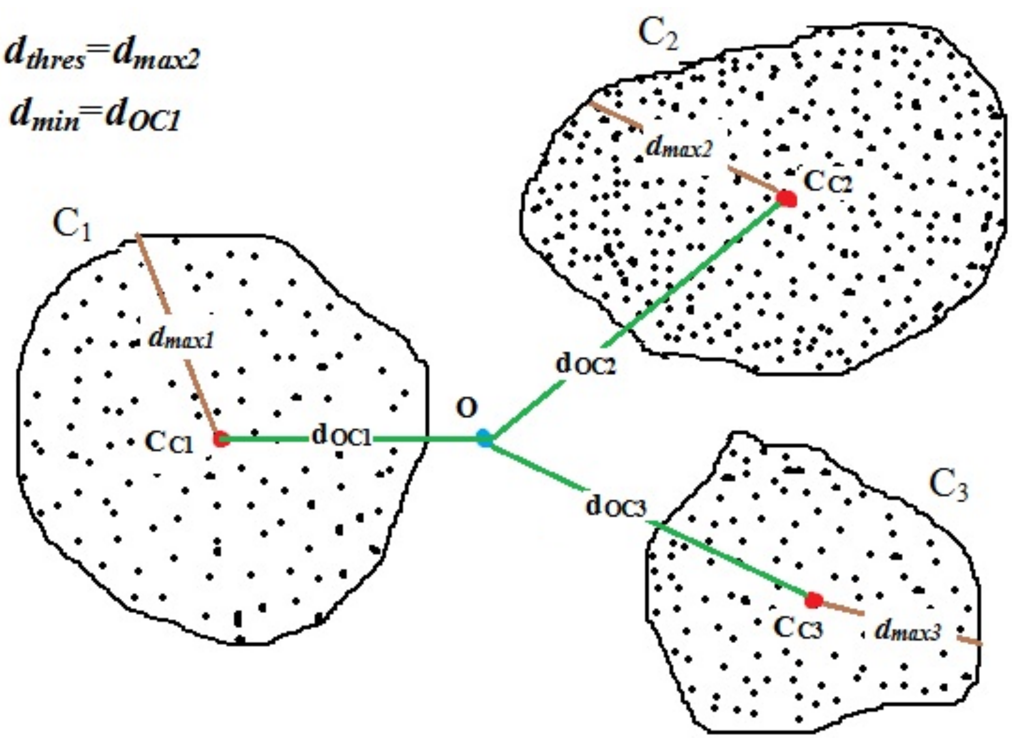
- Compare the probabilities of incoming transaction sequences with thresholds and flag fraud as appropriate
- Can use direct probabilities or more complex metrics
  - Miss Rate Metric
  - Miss Probability Metric
  - Entropy Reduction Metric
- Update Markov Probability table with incoming transactions

Markov Models for Fraud Detection



Learn from Data

- Apply **Predictive** Analysis on **Batch** Data and provide Classifiers to **Streaming** Analytics



Dig Deeper using Big Data

- Provide access to historical data to dig deeper
- Make querying and filtering easy and intuitive
- Provide useful visualizations to isolate incidents and unearth connections

Visualize

Fraud Detection Toolbox

Home | Dashboard

June 1, 2015 - June 30, 2015

Card #

Search

Transaction ID	Card #	Item #	Transaction Amount	Quantity	Currency	Shipping Address	Email	Origin (IP)	Date / Time	Delete
10275	5010822463108860	I0012	50	1	USD	17 Le Duan District 1,Ho Chi Minh City, 070000, Vietnam	fletcher.flosi@yahoo.com	2.132.0.5	02/17/2015 6:40:00	✖
10273	4030823453103050	I0012	50	1	USD	Jiefang Ave, Zhengxiang, Hengyang, Hunan, China	takethree@yahoo.com	2.132.0.5	02/17/2015 6:40:00	✖
10276	5010822463108860	I0012	50	1	USD	Krasnyy pr., 52, Novosibirsk, Russia	fourdays@yahoo.com	2.132.0.5	02/17/2015 6:40:00	✖
10278	5010822463108860	I0012	50	1	AUD	200 Broadway Av WEST BEACH SA 5024 AUSTRALIA	fletcher.flosi@yahoo.com	2.132.0.5	02/17/2015 6:40:00	✖
10990	3772822463100050	I0011	1200	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	105.235.192.0	01/04/2015 9:00:00	✖
10112	3772822463100050	I0011	68	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	170.20.11.116	01/04/2015 9:00:00	✖
10116	3772822463100050	I0011	50	2	USD	Butler Library, Columbia University, New York, NY, USA	laurel_reitler@reitler.com	143.58.3.25	01/09/2015 8:23:06	✖
10113	3772822463100050	I0011	68	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	170.20.11.116	01/04/2015 9:00:00	✖
10112	3772822463100050	I0011	68	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	170.20.11.116	01/04/2015 9:00:00	✖
10273	4030823453103050	I0012	50	1	USD	Jiefang Ave, Zhengxiang, Hengyang, Hunan, China	takethree@yahoo.com	2.132.0.5	02/17/2015 6:40:00	✖

Showing 1 to 10 of 28 rows 10 records per page

<< < 1 2 3 > >>

Origin Map | Intensity Map | Sequence Map

Visualize

Fraud Detection Toolbox Home Dashboard

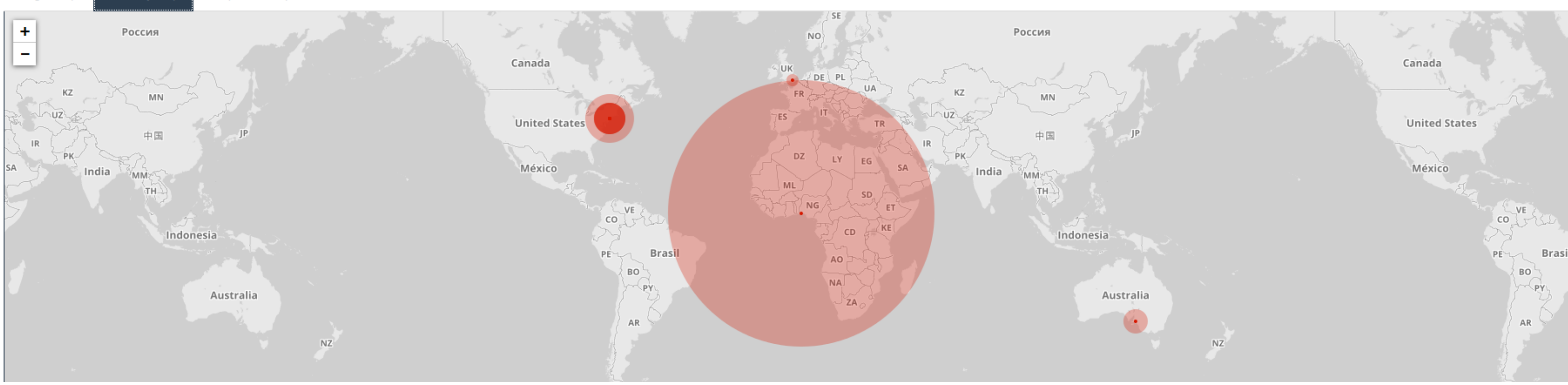
May 21, 2015 - June 19, 2015

+ Search

Transaction ID	Card #	Item #	Transaction Amount	Quantity	Currency	Shipping Address	Email	Origin (IP)	Date / Time	Delete
10217	5010822463108860	I0012	50	1	AUD	200 Broadway Av WEST BEACH SA 5024 AUSTRALIA	fletcher.flosi@yahoo.com	105.235.192.0	02/18/2015 19:10:00	✖
10178	5010823453103055	I0011	25	1	GBP	11 Belgrave Road, London, SW1V 1RB, UK	brhym@rhym.com	105.235.192.0	01/11/2015 0:32:19	✖
10204	4030823453103055	I0010	200	3	USD	256, alakija street, lagos, nigeria	johnetta_abdallah@aol.com	105.235.192.0	02/06/2015 3:10:00	✖
10112	3772822463100050	I0011	68	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	105.235.192.0	01/05/2015 22:30:00	✖
10112	3772822463100050	I0011	68	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	105.235.192.0	01/05/2015 22:30:00	✖
10112	3772822463100050	I0011	68	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	170.20.11.116	01/05/2015 22:30:00	✖
10116	3772822463100050	I0011	50	2	USD	Butler Library, Columbia University, New York, NY, USA	laurel_reitler@reitler.com	143.58.3.25	01/10/2015 21:53:06	✖
10112	3772822463100050	I0011	68	1	USD	Butler Library, Columbia University, New York, NY, USA	calbares@gmail.com	105.235.192.0	01/05/2015 22:30:00	✖

Showing 1 to 8 of 8 rows

Origin Map Intensity Map Sequence Map



North America

Cisco, ATC, Acuity Group, American Family Insurance, Children's Hospital Boston, CAA, SAIC, Institut national de santé publique Québec, MEMC, Concur, Trimble, UMUC, JPMorganChase, U.S. Army, Prudential, Verio, AAA, dg, Blue Cross of Idaho, BNY Mellon, Intermountain Healthcare, Front Porch Digital, imshealth, Boeing, StubHub!, Kaiser Permanente, UBS, Noel Group, Expedia, Tractor Supply Co, eBay, Flexera, Regions, barclaycard, NATO OTAN, neustar, west, Spectrum Health, GSA, Capital Group Companies, intel, GE, Rakuten Global Market, Front Porch Digital

Europe

BBVA, Brand Implementation Group, CINECA, Iberia, Berlin Airports, Volvo, suva, Truvo, GAD, digipolis, CSI, Soft Design, A.M.A., Alfa-Bank, Tag:, Securitas, RosEvroBank, orange, Salzburg AG, Hilti, British Airways, O_2, Alcatel-Lucent, eurotaxGLASS's, Xchanging, AllianceBernstein, House of Fraser, bpifrance

Middle East and Asia-Pacific

Commercial Credit, Sri Lanka Telecom Mobitel, Cognizant, ICTA ideas actioned, ODEL, Dialog, Sapura, plc, onesteel, Australian Government Department of Health and Ageing, JIESAI, VIB

South America

SIF, BI&P Banco Industrial & Partners

THANK YOU

GRACIAS, ARIGATO, SHUKURIA, TASHAKKUR ATU, YAQHANYELAY, SUKSAMA, EKHMET, GOZAIMASHITA, EFCHARISTO, GRAZIE, MEHRBANI, PALDIES, BOLZÏN, MERCI, DANKS, USPAXAR, KOMAPSUMNIDA, MAAKE, TINGKI

Contact us !