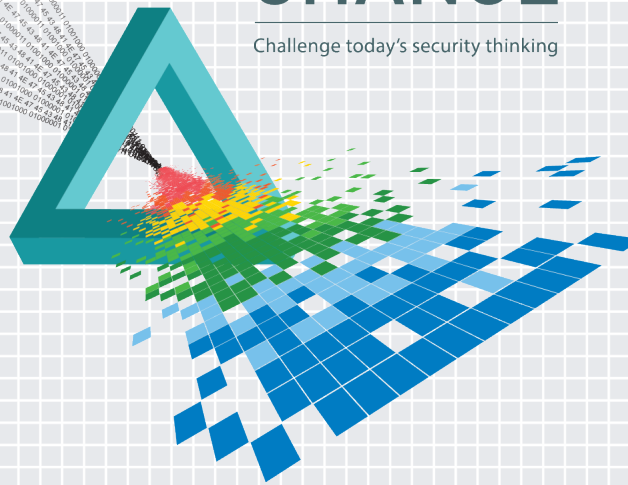
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: MBS-W03

"Your VISA has been DEACTIVATED": How Cybercriminals Cash In Via SMS Attacks

Cathal Mc Daid

Head of Data Intelligence & Analytics
Adaptive Mobile Security
@mcdaidc

Seen this?

(Auburn University FCU) 24HRS ALERT: Your VISA Check Card #413809 is deactivated. Please call our 24 hours line (334) 209-[****]

Spot the difference

Variant 1

DEACTIVATED

Variant 2

DEACTIVATED

Spot the difference

Variant 1

deactivated

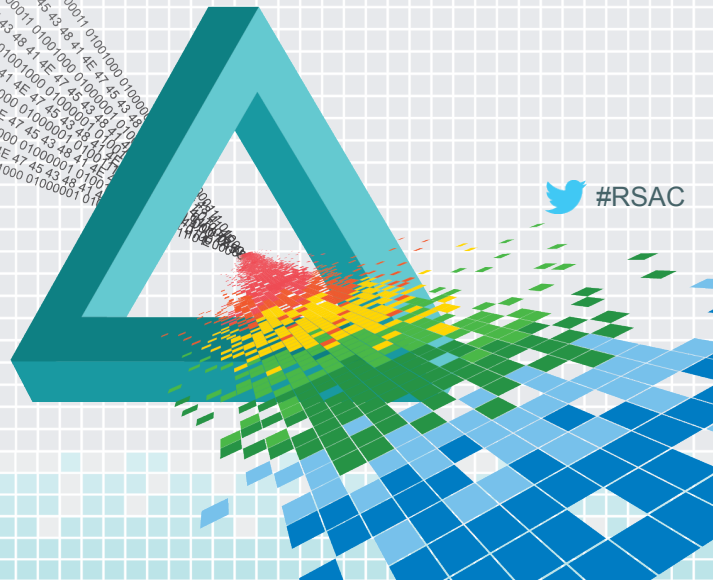
Variant 2

deactIvated

RSAConference2015

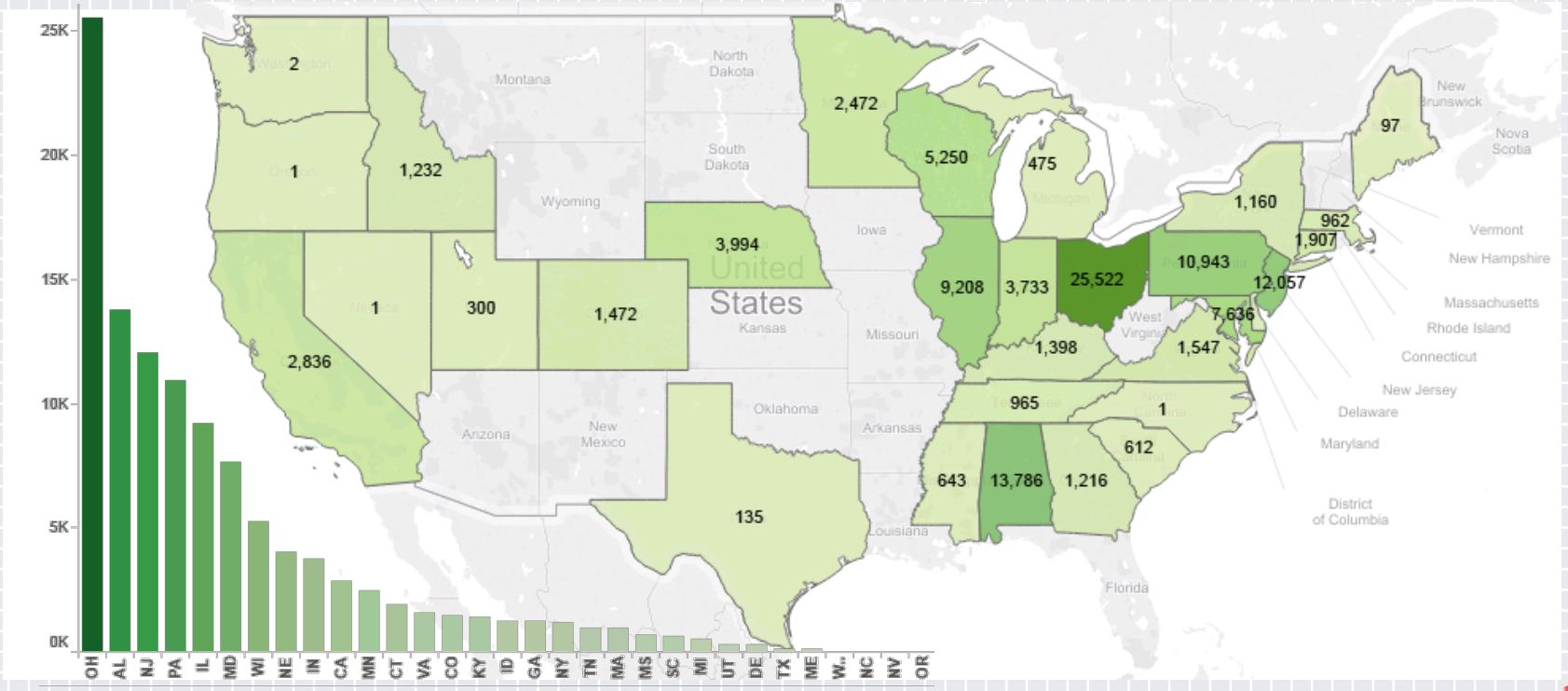
San Francisco | April 20-24 | Moscone Center

Call recording

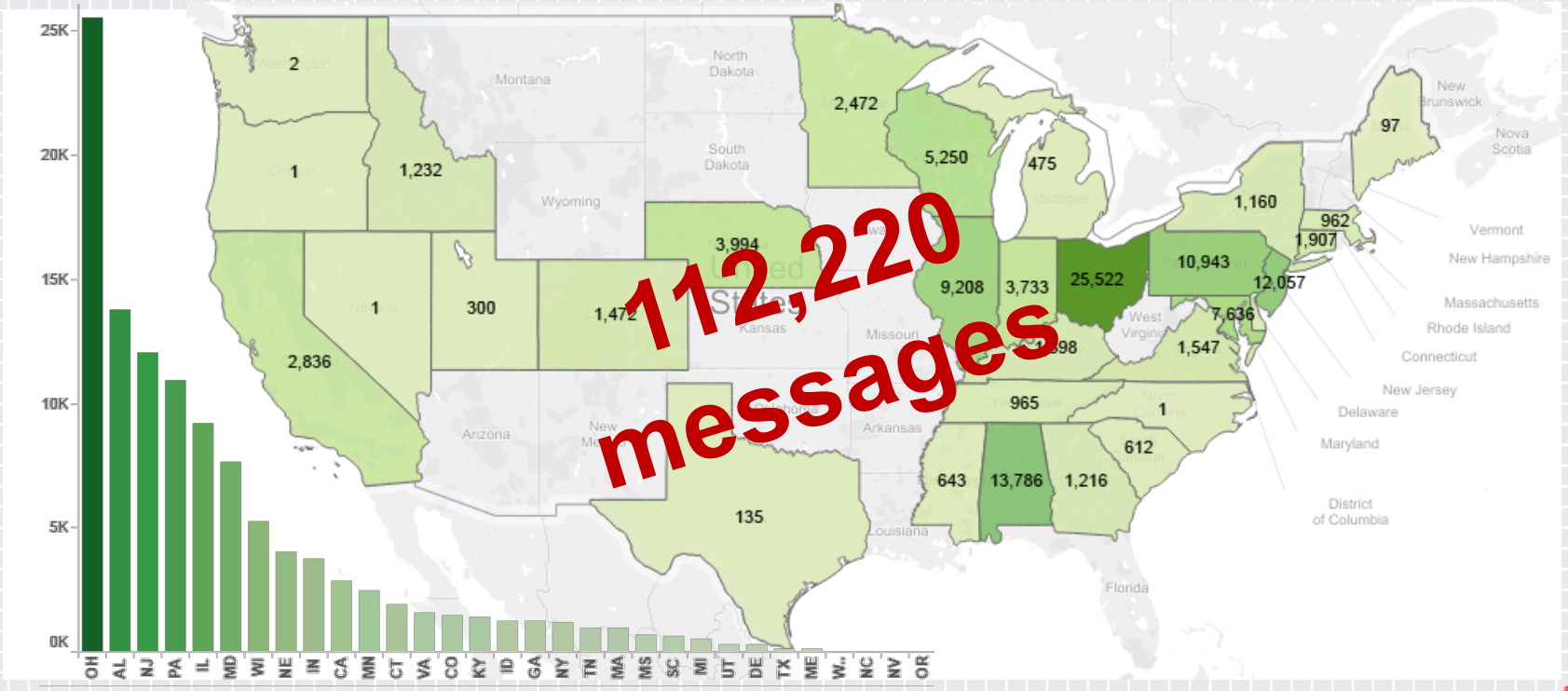


Getting the digits

Geographic distribution of attacks Oct ’14 -> Jan ‘15

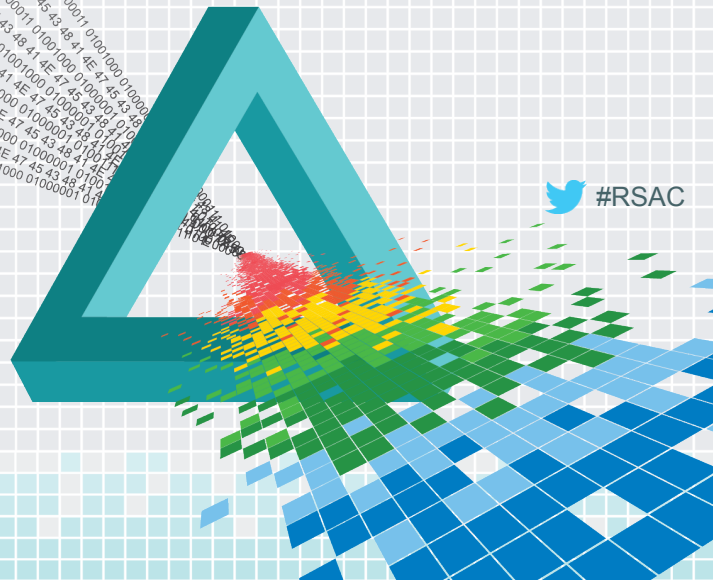


Geographic distribution of attacks
Oct ’14 -> Jan ‘15



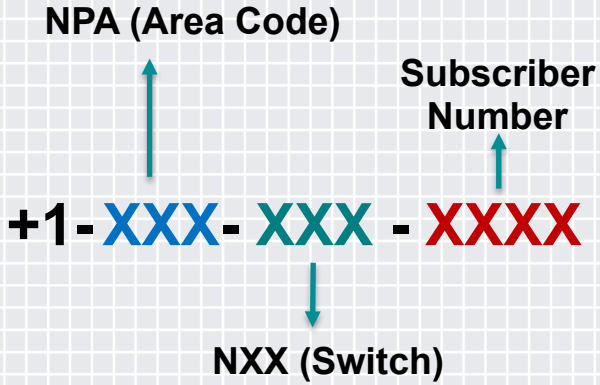
Geographic distribution of attacks
Oct ’14 -> Jan ‘15

The scam is in the detail



North American Number Plan

- US, Canada, Caribbean Islands share numbering plan
  - All numbers – mobile and landline are geographically allocated
  - ‘Helps’ mobile spammers & phishers target local areas

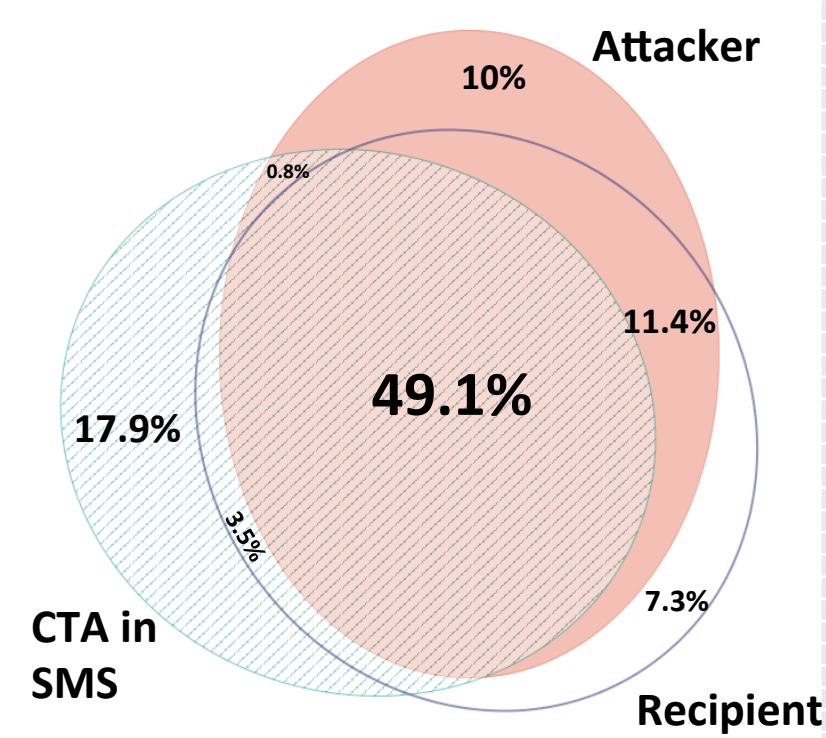


North American Number Plan

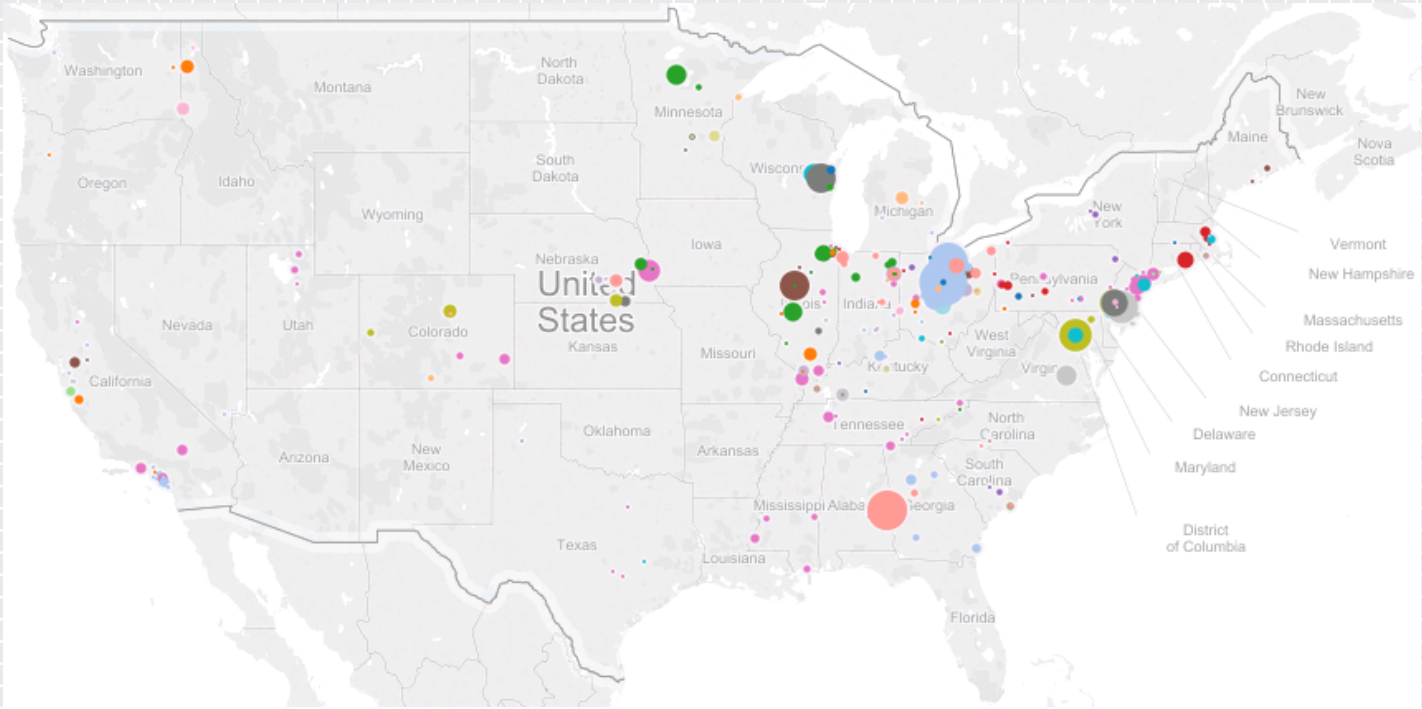
- US, Canada, Caribbean Islands share numbering plan
  - All numbers – mobile and landline are geographically allocated
  - ‘Helps’ mobile spammers & phishers target local areas
- Additional use by bank attackers:
  - Sender and CTA number often have **same area code as recipient**
- Sender: 1-**309**-361-XXXX Recipient: 1-**309**-363-XXXX
  - All 309 numbers located in Peoria, Illinois

This is an automated alert from South Side Bank. *VISA Debit/Card #43315201 reactivation required. Please call 24hrs (309) 282-6411

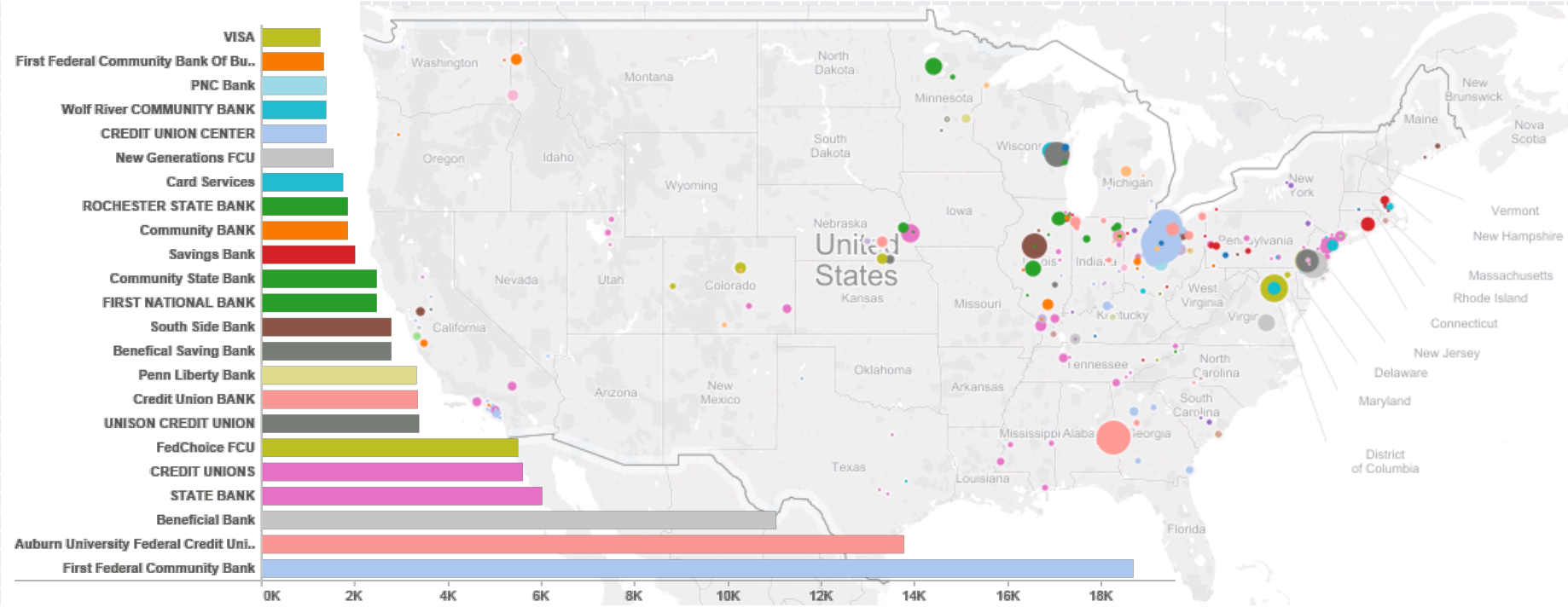
Your neighbour is your friend



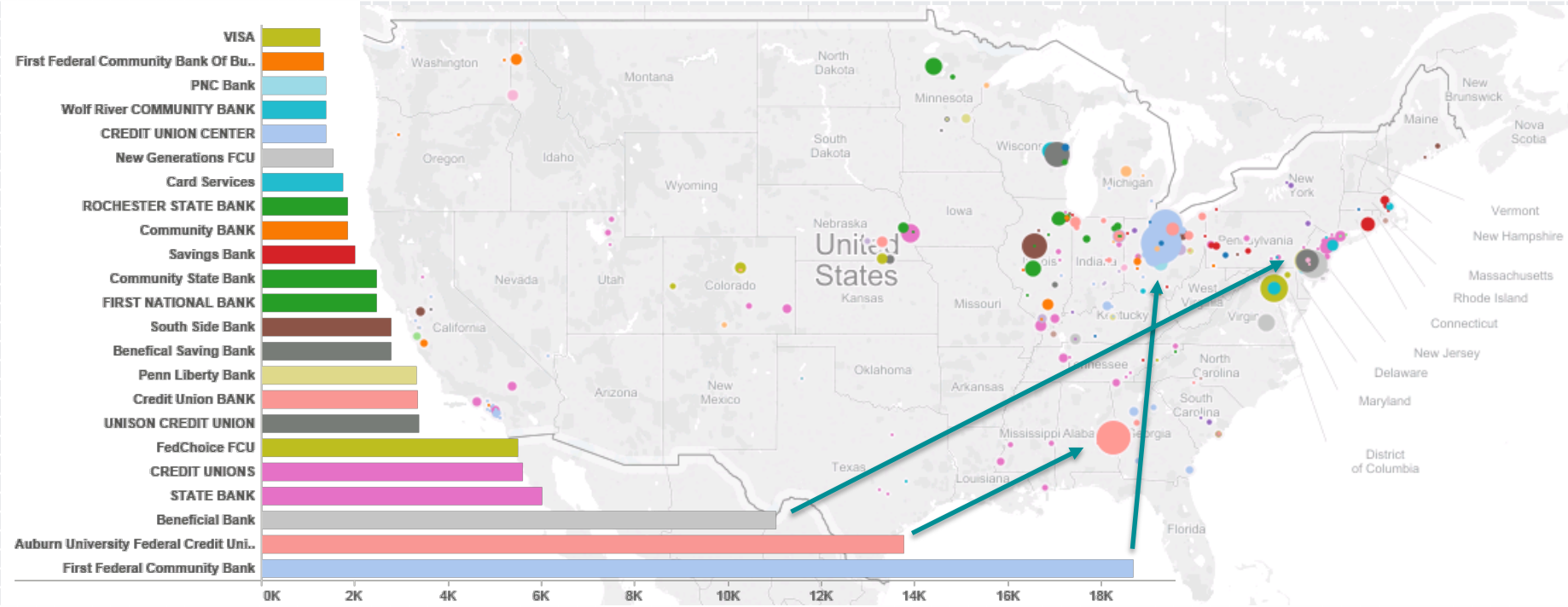
Geographic distribution of bank attacks



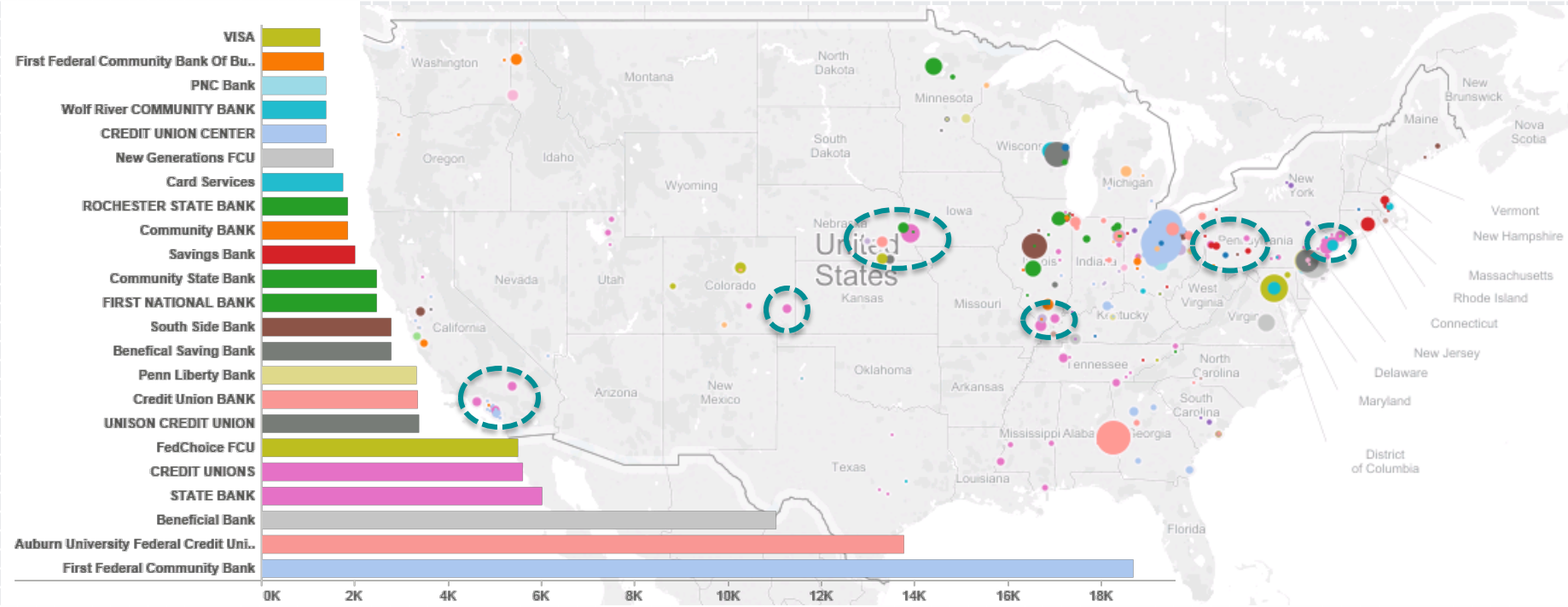
Geographic distribution of bank attacks



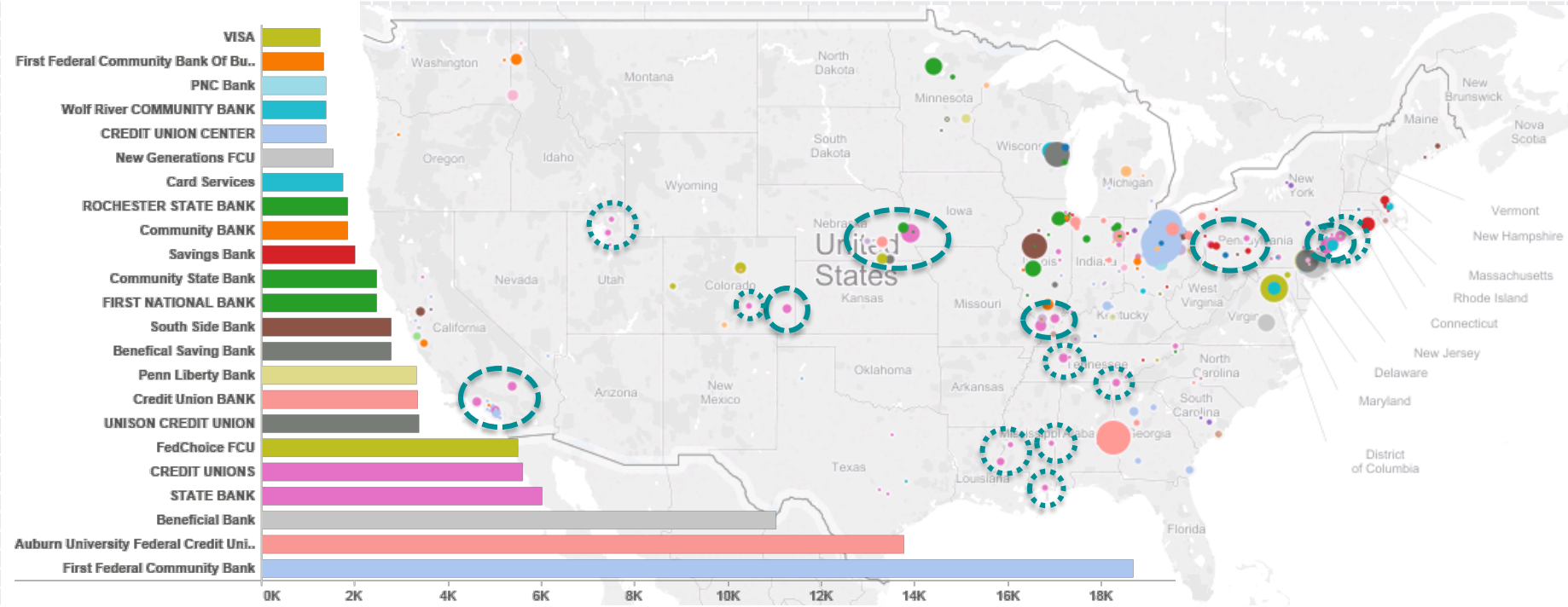
Geographic distribution of bank attacks



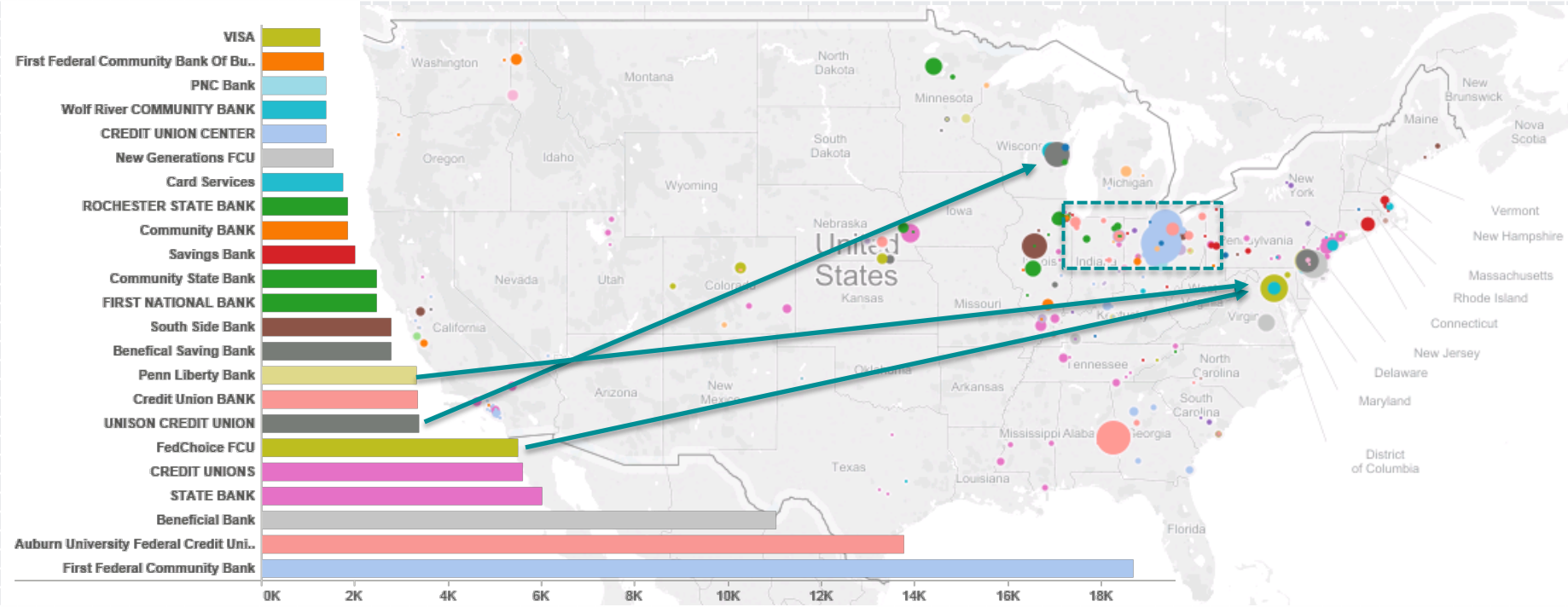
Geographic distribution of bank attacks



Geographic distribution of bank attacks

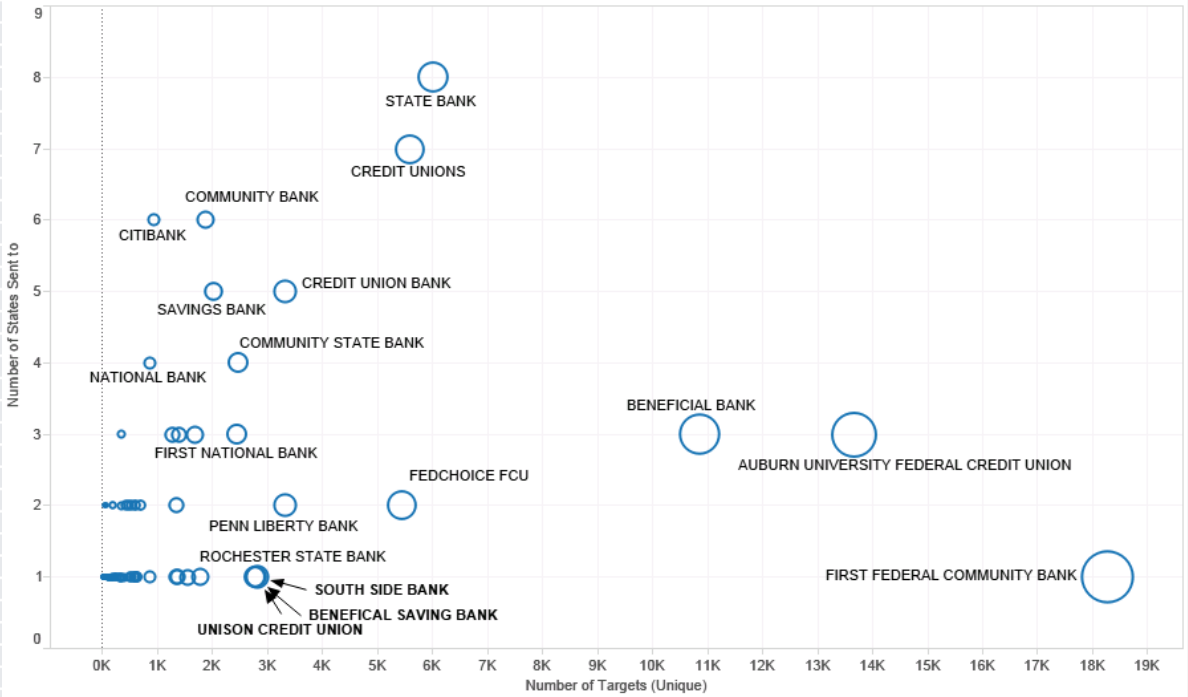


Geographic distribution of bank attacks



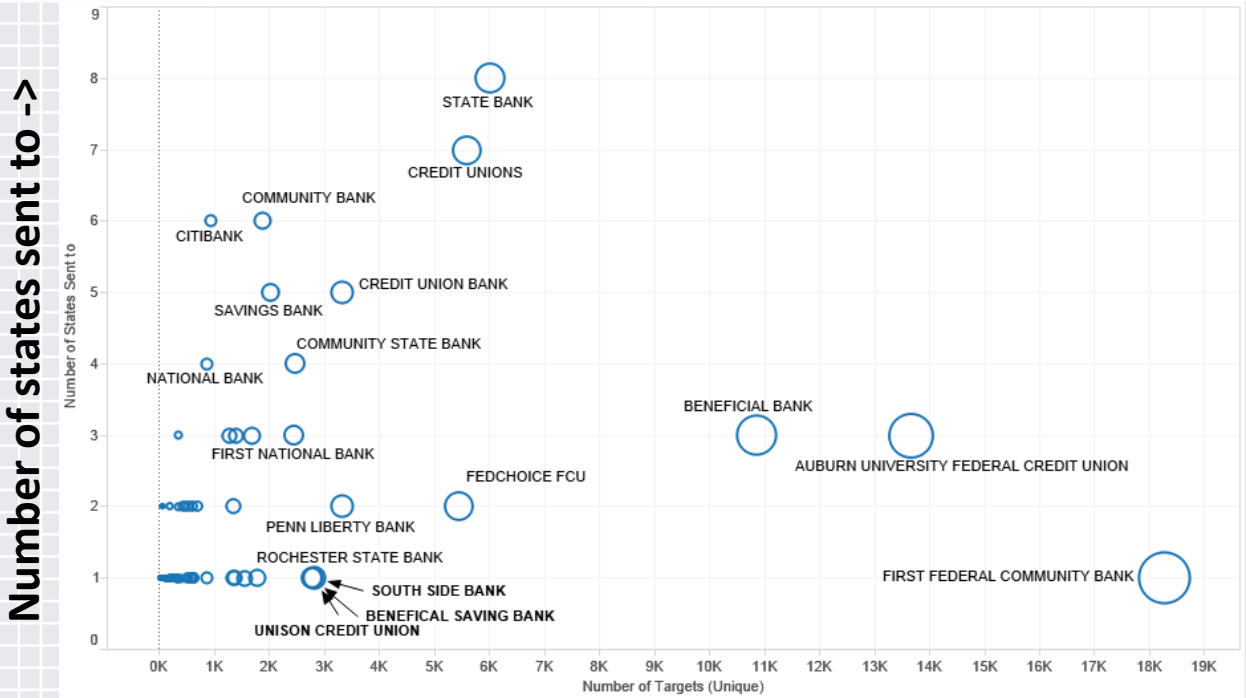
Go Local & Large OR National & Bland

Number of states sent to ->



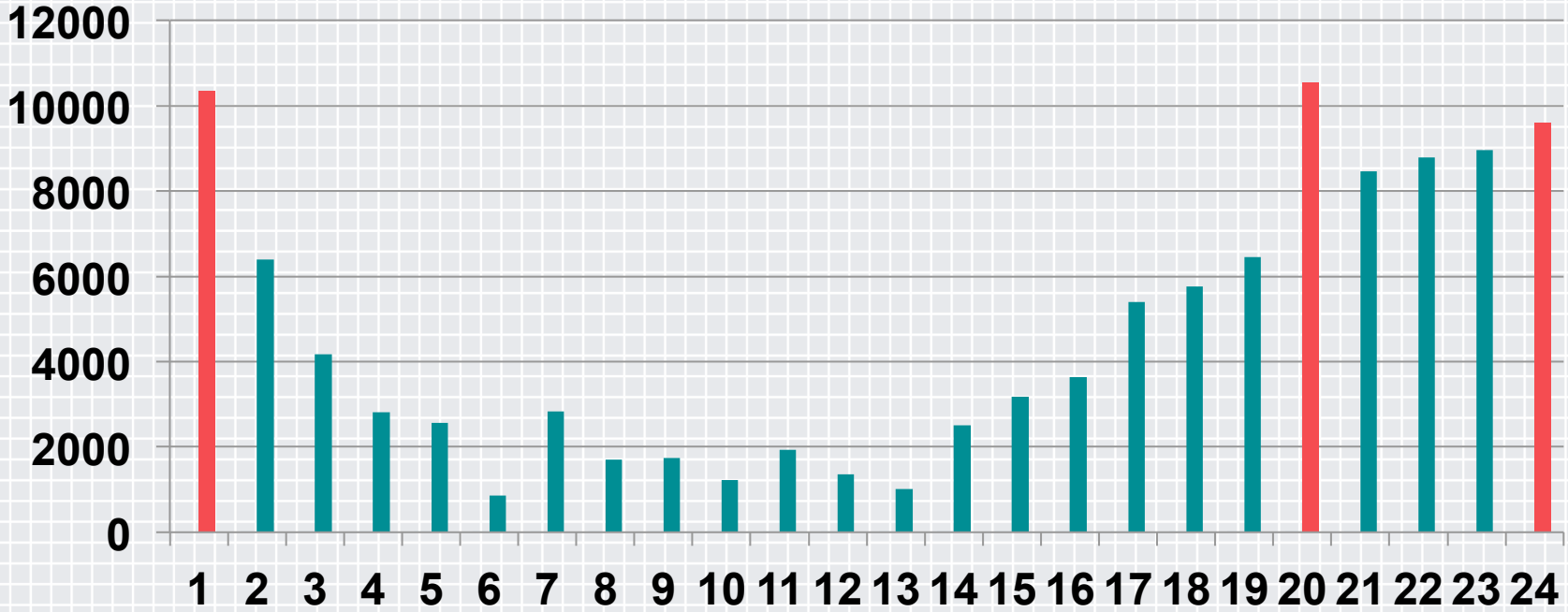
Number of targets (unique) ->

Go Local & Large OR National & Bland



- More widespread -> more generic
  - Exception: Citibank
- Focus on local area
- Main national banks are not the target

Business hours (EST)

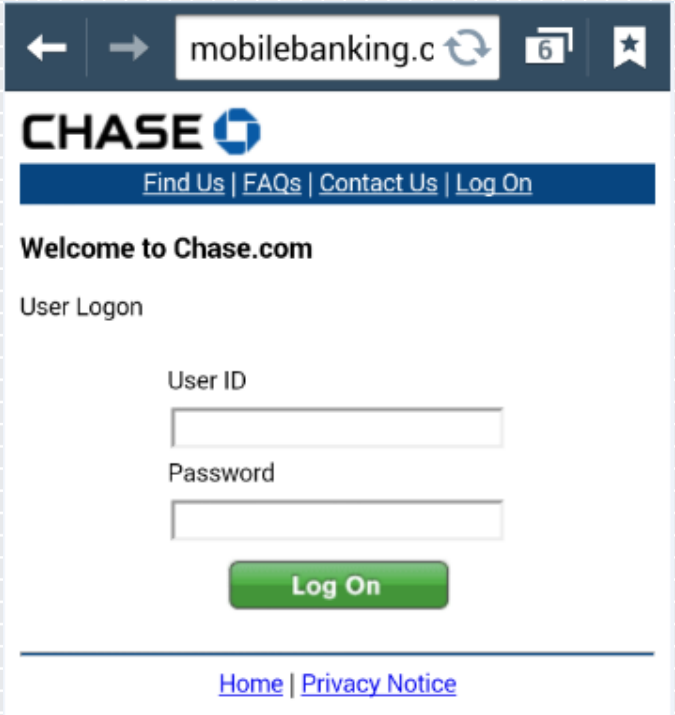


URL as a CTA

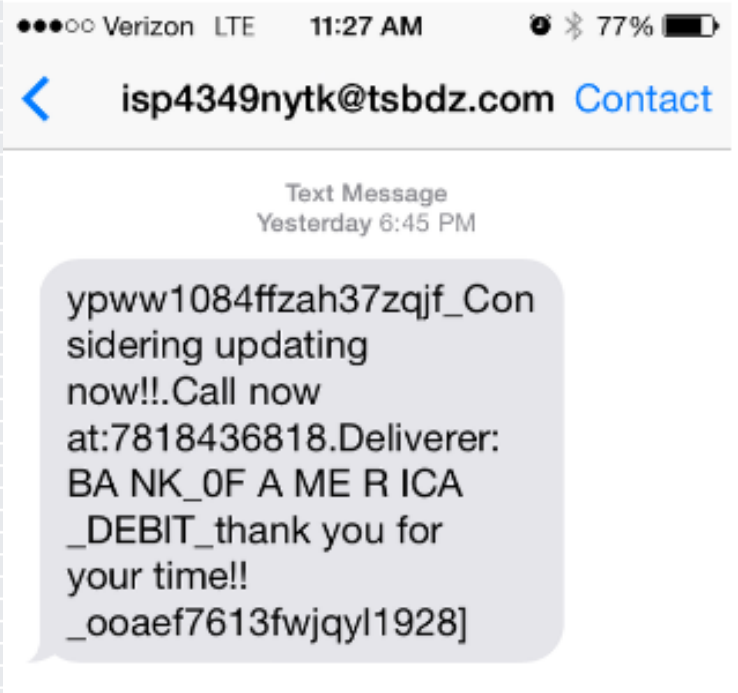
- Phone number CTA **pros**
  - Works for all phones
  - More accepted by age groups
  - Pseudo-authentication
  - ‘Official’ sounding
- Phone Number CTA **cons**
  - IVRs are expensive to hack/setup

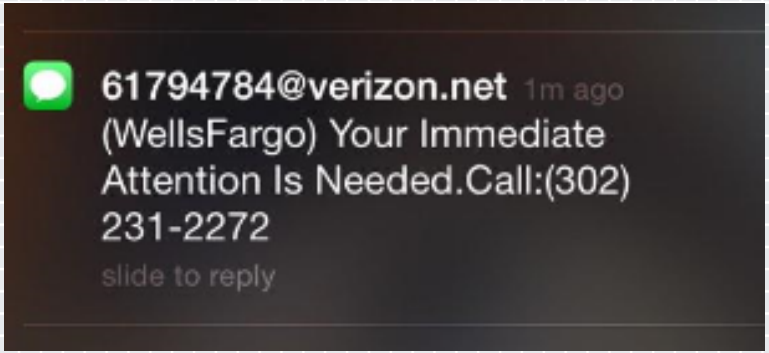
You have a new alert regarding your Citibank account. Please click the link bellow to read it: http://online.citibank.com.us-wl.com***

JP Morgan phishing attack, October 1st



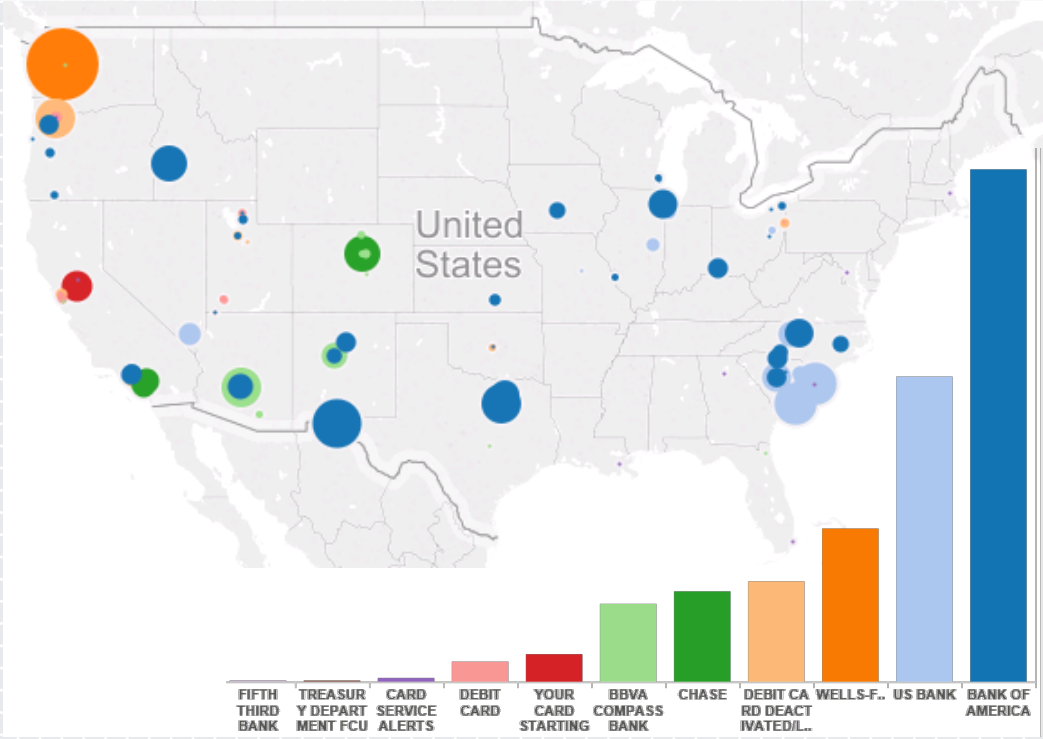
But wait - my bank spam looks different?





Sources:
https://twitter.com/DanversPolice/status/541957769344331776
https://twitter.com/BBB_CVA/status/566334669030178817

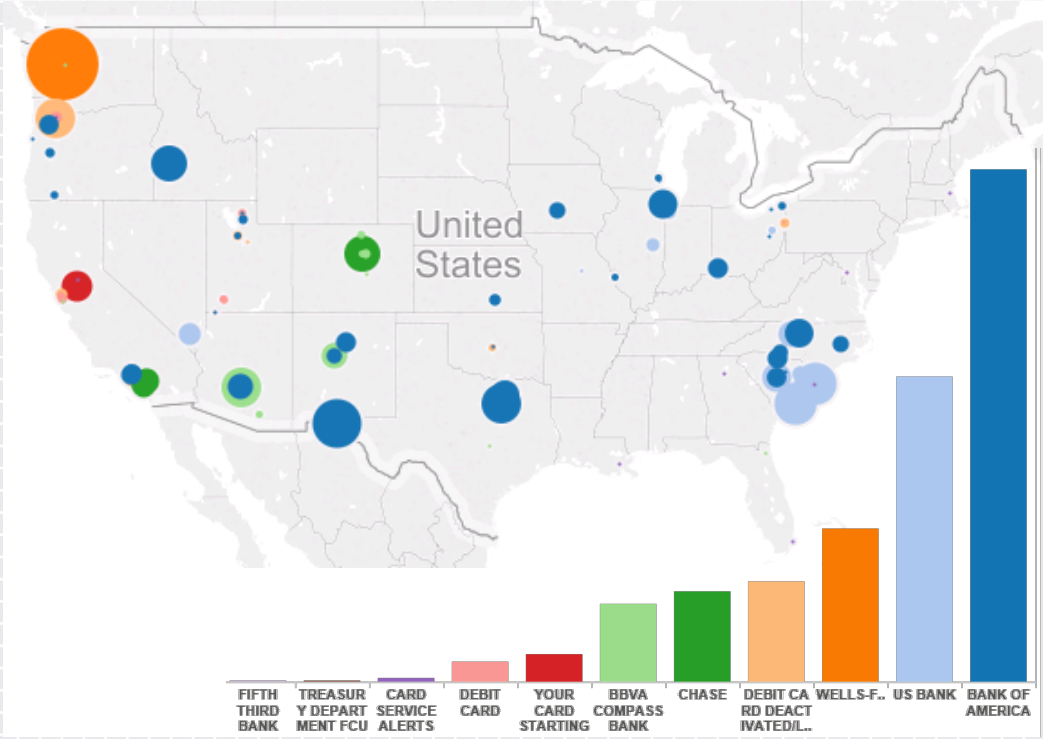
Different priorities. West coast



Plot of ‘Reflected’ Email attacks per bank in 2 month period in 2013

Different priorities. West coast

- Targets include much larger banks
- Cross state activity
- Use URLs more frequently
- Sender Email address is random
- Hacked IVRs usage as the CTA number



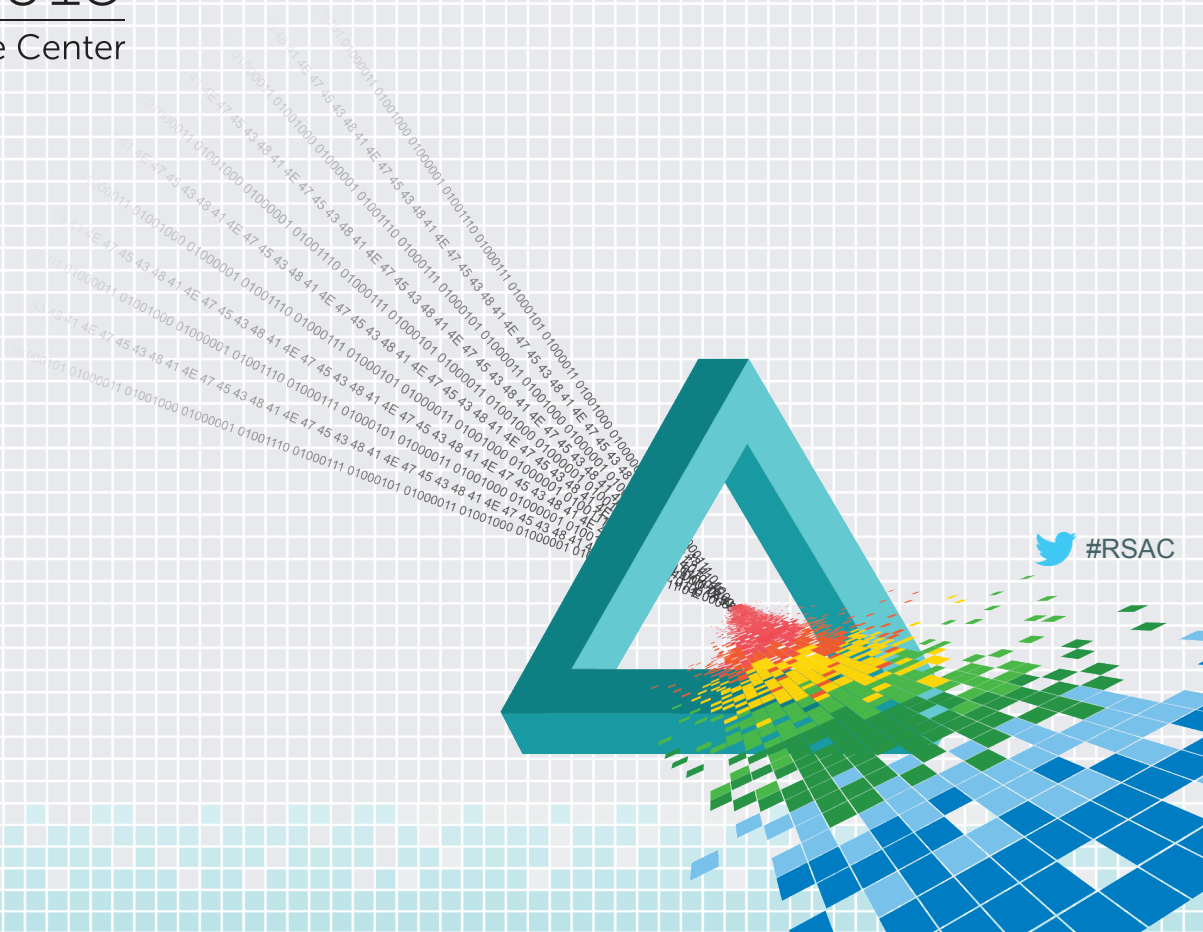
Plot of 'Reflected' Email attacks per bank in 2 month period in 2013

Different techniques – different ‘families’

A word on voice phishing

- Spam evolves when under pressure
- North America: in last 2-3 years, increasing defence against SMS phishing has lead to re-emergence of mainstream voice phishing attacks
  - Normally (**but not always**) targeting main banks
- Cost associated (slower, longer, more technical)
  - In pressure of aggressive take downs on mobile originated side, makes sense
  - Additional benefits: can easily spoof bank/credit union's caller ID
- As text protection gets better, this may increase

Attack analysis



Variant #1

(Auburn University FCU) 24HRS ALERT: Your VISA Check Card #413809 is deactivated. Please call our 24 hours line (334) 209-[****]

Variant #2

Auburn University FCU ALERT: Your VISA Check Card #413809 is deactivated. Please call our 24 hours line (334) 209-[****]

Variant #3

Auburn University FCU ALERT: Your VISA Check Card #413809 is deactivated.-Please call our 24 hours line (334) 209-[****]

Variant #4

Auburn University FCU ALERT: Your VISA Check Card #413809 is deactivated.**Please call our 24 hours line (334) 209-[****]

Variant #5

Auburn University FCU ALERT: Your VISA Check Card #413809 is deactivated.*Please call our 24 hours line (334) 209-[****]

Variant #6

Auburn University FCU ALERT: Your VISA Check Card #413809 is *deactivated. Please call our 24 hours line (334) 209-[****]

Variant #7

Auburn University FCU ALERT: Your VISA Check Card #413809 is locked.*Please call our 24 hours line (334) 209-[****]

Variant #8

Auburn University FCU ALERT: Your card #413809 is frozen.-Please call our 24 hours line (334) 209-[****]

Variant #9

Auburn University -FCU NOTICE-: Your card #413809 is -limited-. Please call our 24 hours line (334) 209-[****]

Variant #10

Auburn University -FCU NOTICE-: Your VISA #413809 is limited.*Please call our 24 hours line (334) 209-[****]

Variant #11

Auburn University FCU NOTICE: Your VISA #413809 is detained. Please call our 24 hours line 334-209-[****]

Variant #12

Auburn University FCU NOTICE: Your card starting with 4138 is deact ivated. Please call our 24 hours line 334-209-[****]

Bank card number format

XXXX XXXX XXXX XXXX

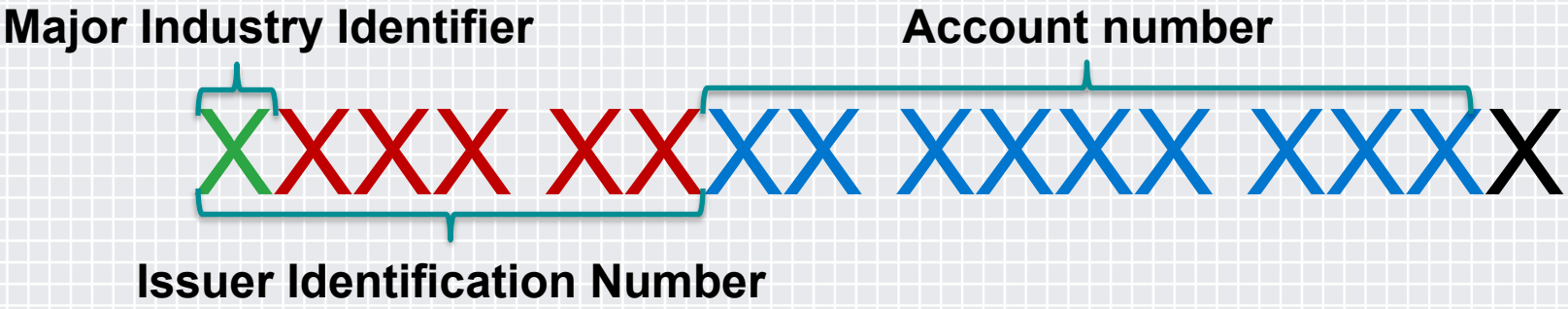
Bank card number format

Major Industry Identifier

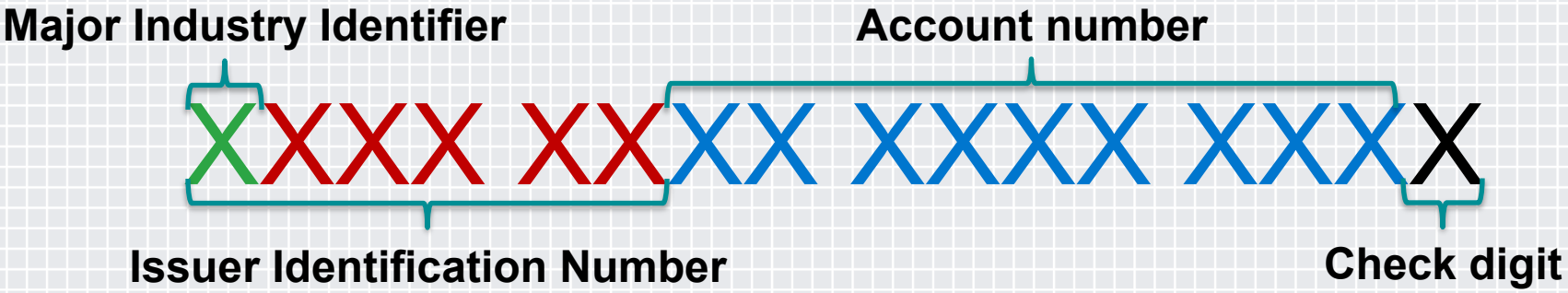
Bank card number format

Major Industry Identifier

Bank card number format



Bank card number format



Bank card number format

#4 - VISA

Major Industry Identifier

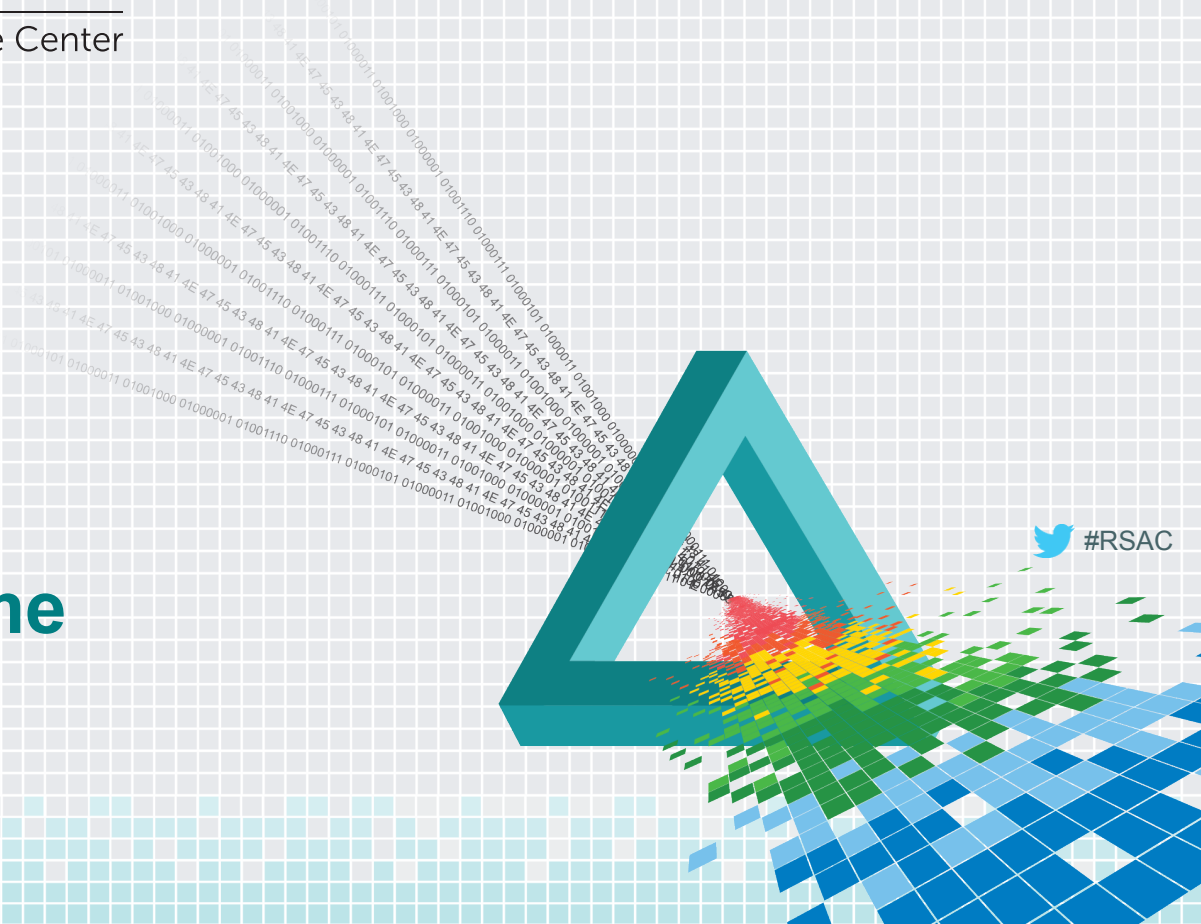
Account number

Issuer Identification Number

Check digit

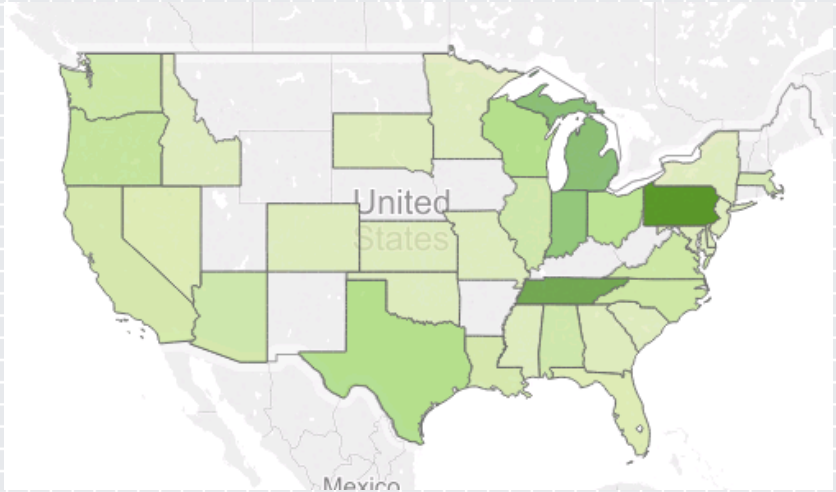
#413809 – Auburn University FCU

Evolution over time

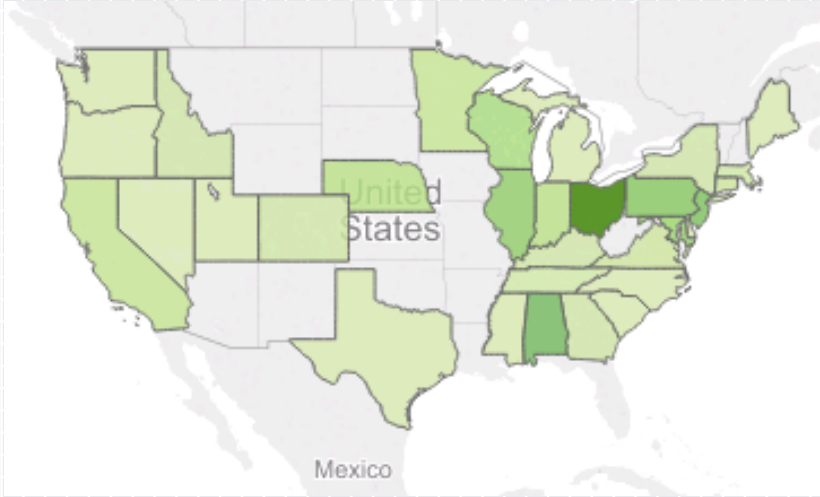


States targeted, then and now

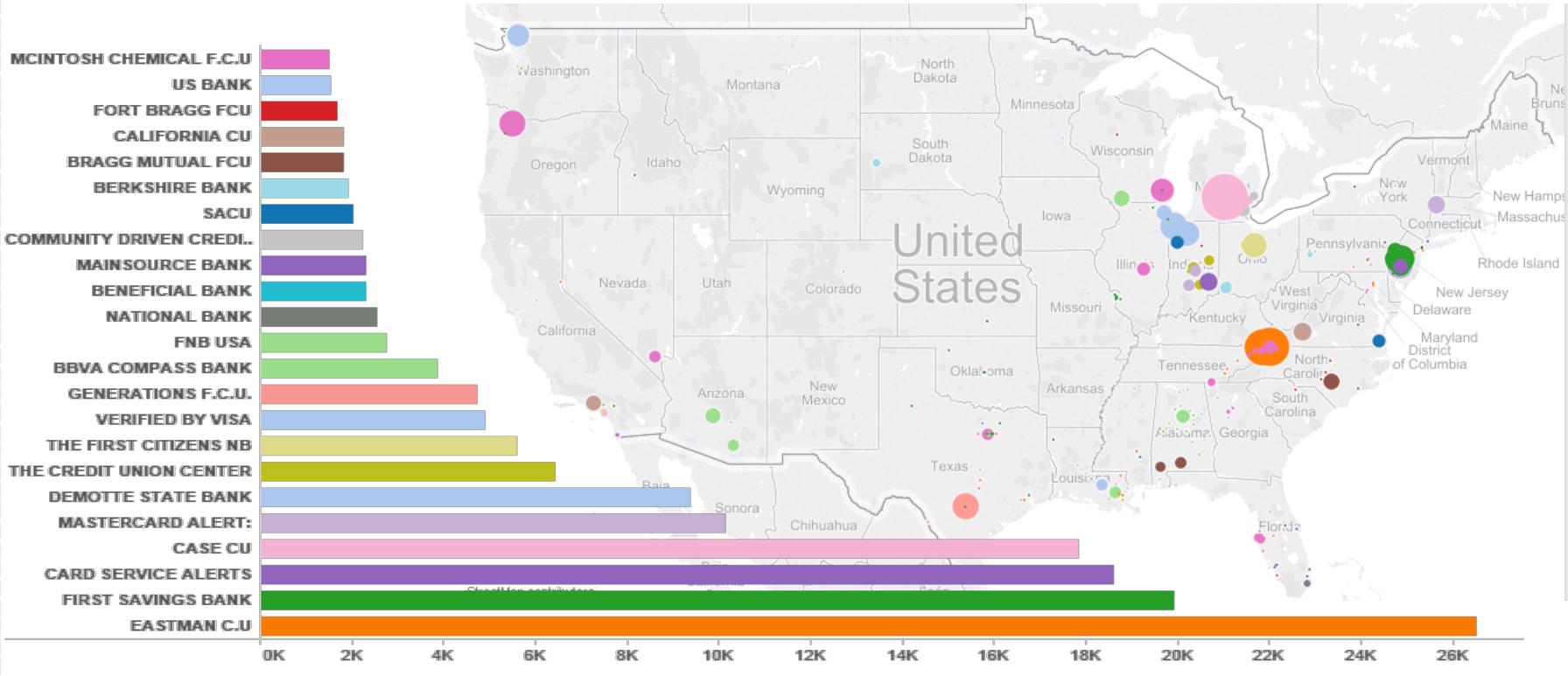
Then: Apr ‘13 -> May ‘13



Now: Oct ‘14 -> Jan ‘15



Attack distribution, Apr '13 -> May '13



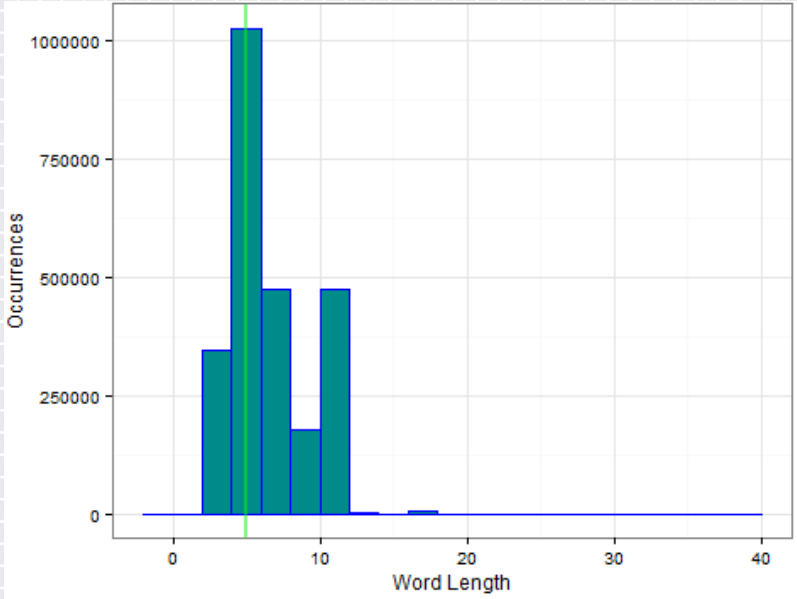
Difference (1): smaller words please

Then

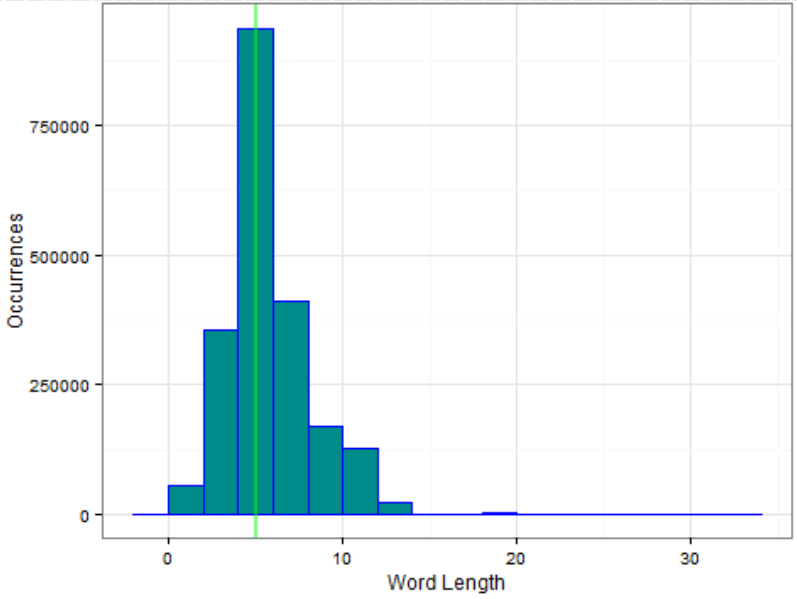
Now

Difference (1): smaller words please

Then

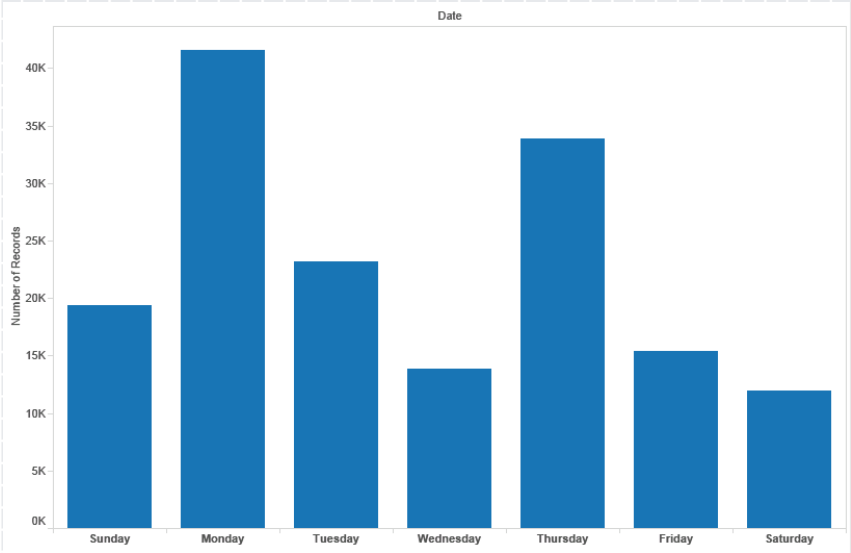


Now

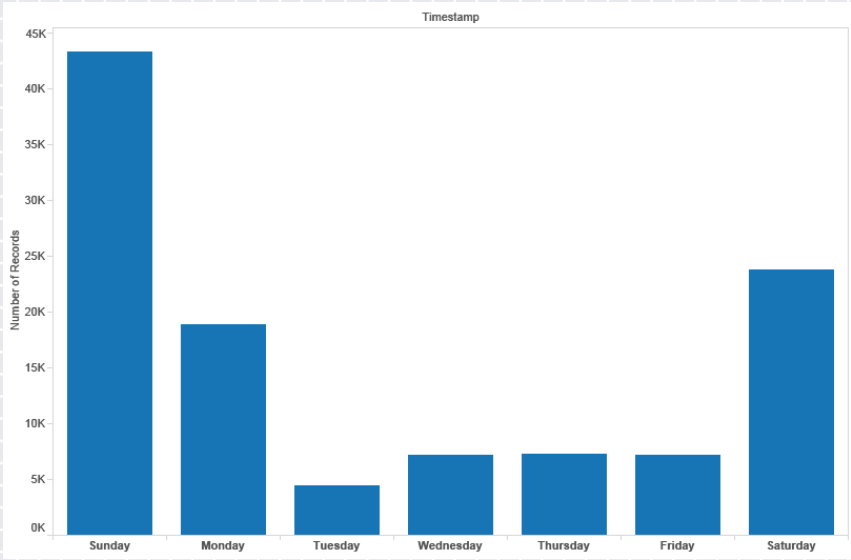


Difference (2): weekend warriors

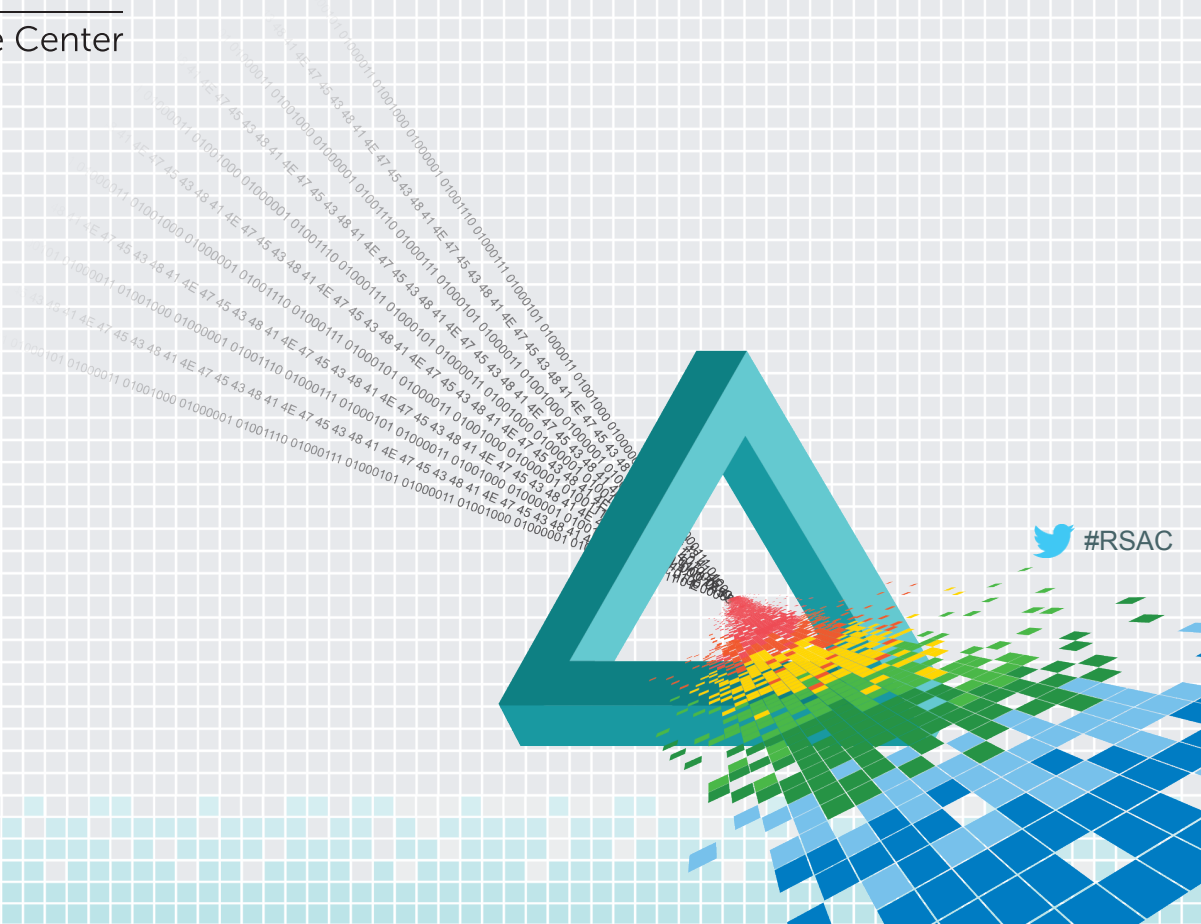
Then



Now



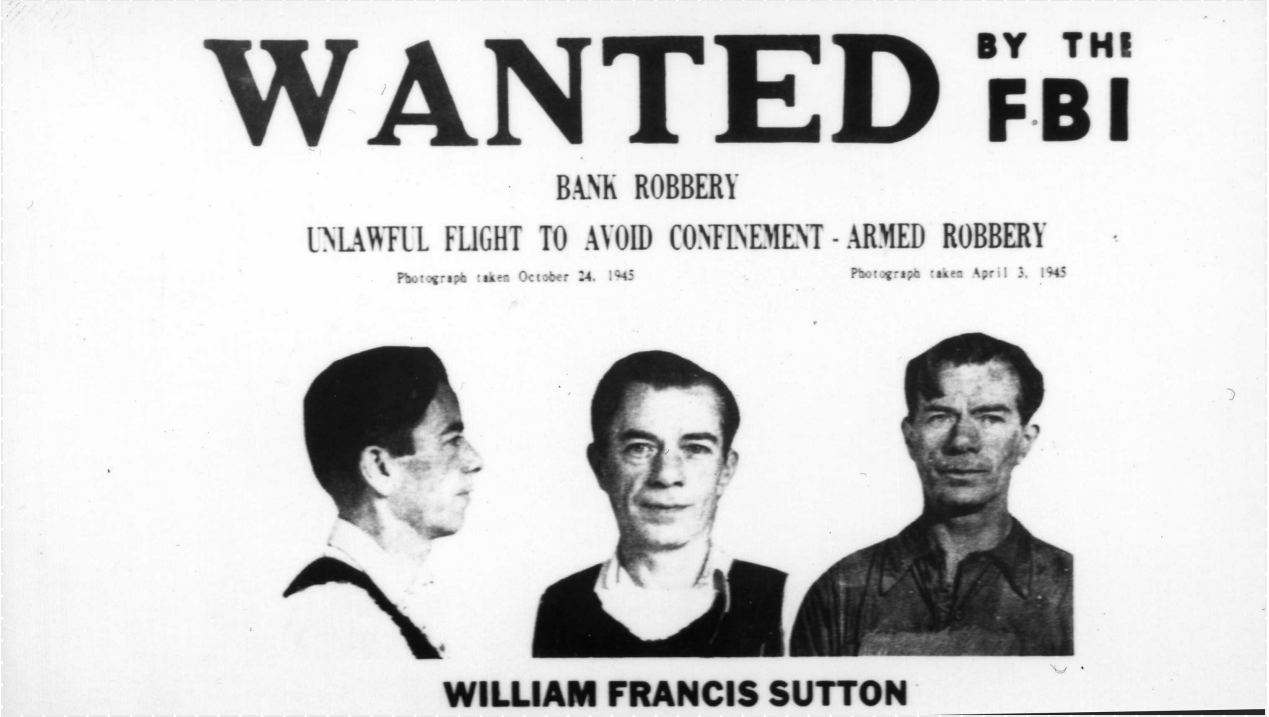
Visualization



Conclusion

- Overall volumes from these spammers are dropping
  - Due to faster/quicker detection techniques
  - However as other types of text attacks have dropped even more – seems to be more ‘noticeable’
- Complexity increasing:
  - Average word size decreasing, sending patterns changing
- Determined group will always remain present while favourable economics in place:
  - Cost to defeat defences << number of victims * amount stolen from victim
- However the group, must be seen in context of overall **bank phishing industry**

Captain Obvious



Apply Slide

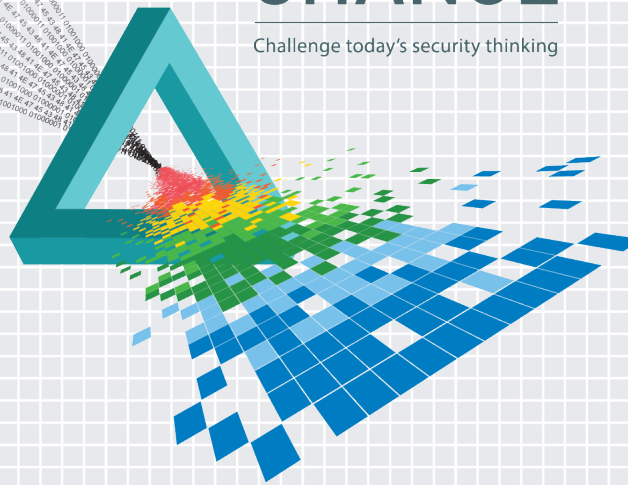
- If you're just an average phone user
  - Ignore the messages – a bank will never contact you like this
  - Report them to banks and carriers
- If you represent a carrier
  - These messages can and should be blocked to protect your customers
  - Other brands/companies are also affected - put protection in place
- If you represent a bank
  - Monitor/get intelligence so you know if an attack happens
  - Raise alerts and spread the word to your customers when it does

RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: MBS-W03

Thank you!

Cathal Mc Daid

Head of Data Intelligence & Analytics
Adaptive Mobile Security
@mcdaidc