

# RSA<sup>®</sup>Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: IDY-F01

## Alerts for Digital Identity System Operation and Fraud Detection



Connect **to**  
Protect

### Andrew Nash

CEO  
Confyrm, Inc  
@winemaker

### Marcel Wendt

Founder / CTO  
Digidentity  
@MarcelWendt



#RSAC

# Data breaches, identity theft, and online fraud



#RSAC



... all the trends are heading in the wrong direction

# Google knew before AOL



#RSAC

Sad News...Gillian Kerr

Inbox x



Gillian Kerr

to me

6:30 AM (1 hour ago) ☆



**This message could be a scam.** The sender's account may have been compromised and used to send malicious messages. If this message seems suspicious, let us know and then alert the sender as well (in some way other than email). [Learn more](#)

[Report this suspicious message](#) [Ignore, I trust this message](#)

Hi,

I'm writing this with tears in my eyes, my family and I came over here to Manila, Philippines for a short vacation. Unfortunately, we were mugged at the park of the hotel where we stayed, all cash and credit card were stolen off us but luckily for us we still have our passports with us.

We've been to the Embassy and the Police here but they're not helping issues at all and our flight leaves in few hours from now but we're having problems settling the hotel bills and the hotel manager won't let us leave until we settle the bills. Well I really need your financial assistance. Please, Let me know if you can help us out? Am freaked out at the moment.

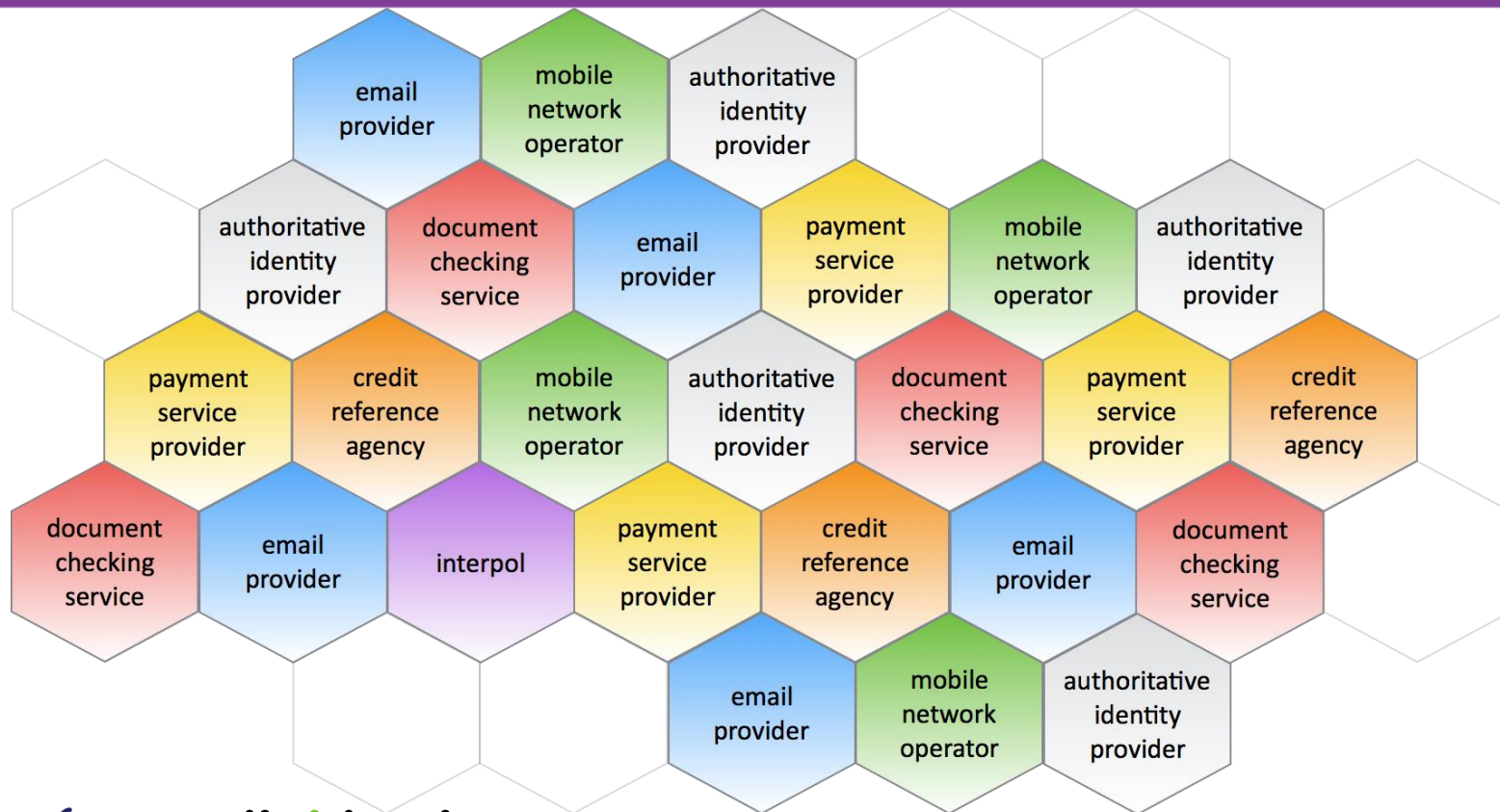
...

Gillian...

# Identity Ecosystem



#RSAC



- Open Identity Exchange
- UK Identity Assurance Programme
  - Shared Signals white paper (Sept 2013)
  - Discovery Project (Summer 2014)
- Google Internet Identity Workshop proposal (Oct 2014)
- National Strategy for Trusted Identities in Cyberspace (Sept 2014)
- Open Identity Exchange RISC working group (May 2015)
- UK Verify Pilot with Commercial Identity Providers (Oct 2015)

# Trusted Communications Channels




- Trusted communication paths:
  - Email
  - SMS
  - Device ID
- Assumed level of Trust
- Currently the protections at email providers is the “real security” level associated with highly trusted accounts
- Every operational mechanism leverages them:
  - Username / Password
  - Multi-factor Authentication
  - Biometrics





# The Account Reset Pattern




Current password 

Don't know your password?

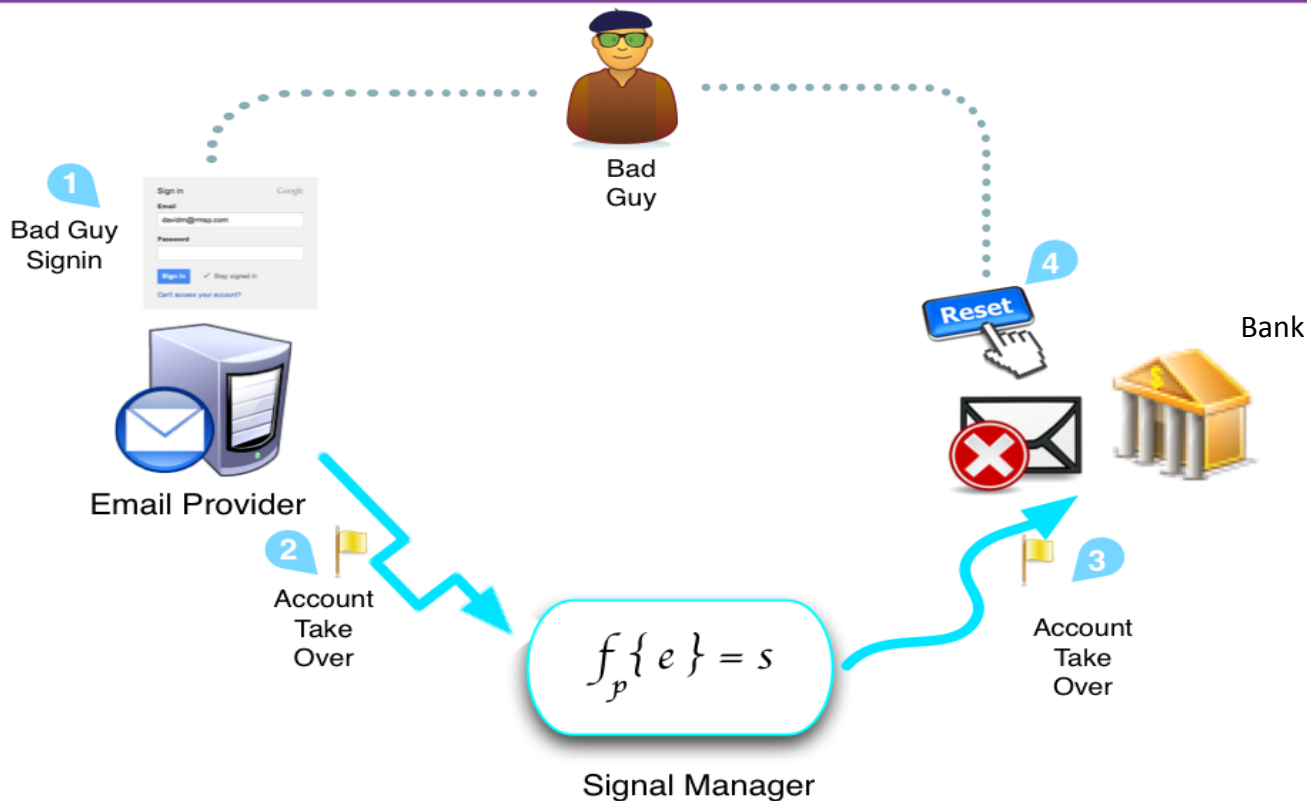
New password 

Confirm new password 

 [Change Password](#)

# Loose / Asymmetric Federations

#RSAC





- Trusted communication path subversion
- Registration velocity @ high assurance IDPs
- Breach implications for downstream online identities
- Revocation of credentials in Identity Federations
- Ghost Identities
- Password resets
- Account recycling
- ... (20+ and counting at the moment)



Google

twitter



conform

facebook

Aol.

LinkedIn



Windows Live

NRI

# Addressing Fundamental Issues



#RSAC



- Lightweight identity alerts
- Real time distribution
- Authoritative events vs scored evaluations
- Independent of credit card fraud alerts
- Share signals before fraud occurs
- Protect personal privacy
- Protect brand reputation

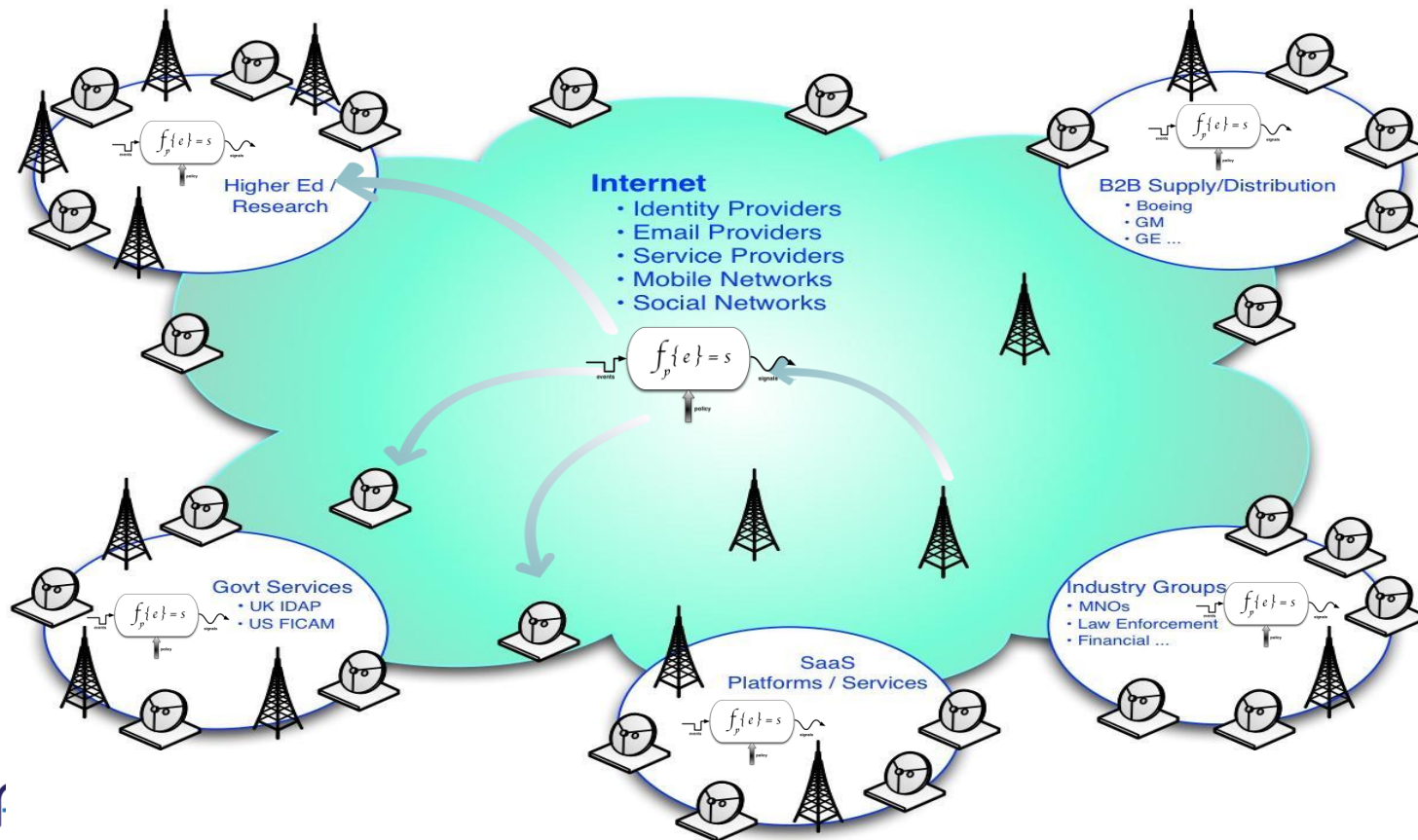


Clearinghouse  
that alerts enterprises  
when their customers  
are exposed at other  
companies / verticals



# Network Development

#RSAC





# **Commercial High Assurance Identity Provider Case Study**

- When you're using digital services, you need to be sure that your privacy is being protected and your data is secure.
- Government departments providing services online need to know it's you.
- GOV.UK Verify uses certified companies to check it's you.





# UK Verify Federated Identity



#RSAC



# UK Verify Service Providers



#RSAC

Email  
Provider

Interpol

Mobile  
Network  
Operator

Authoritative  
Identity  
Provider

Document  
Checking  
Service

Payment  
Service  
Provider

Credit  
Reference  
Agency

- email account takeover
- tampered documents
- false debit/credit cards
- SIM swap
- KBA/KBV leakage

Network Operator Identity Provider Checking Service Service Provider Network Operator Identity Provider

Document Checking Service Payment Service Provider Credit Reference Agency Email Provider Interpol Payment Service Provider Credit Reference Agency Email Provider

Email Provider Interpol Mobile Network Operator Authoritative Identity Provider Document Checking Service Email Provider Interpol

Mobile Network Operator Authoritative Identity Provider Document Checking Service Payment Service Provider Credit Reference Agency Mobile Network Operator Authoritative Identity Provider Document Checking Service

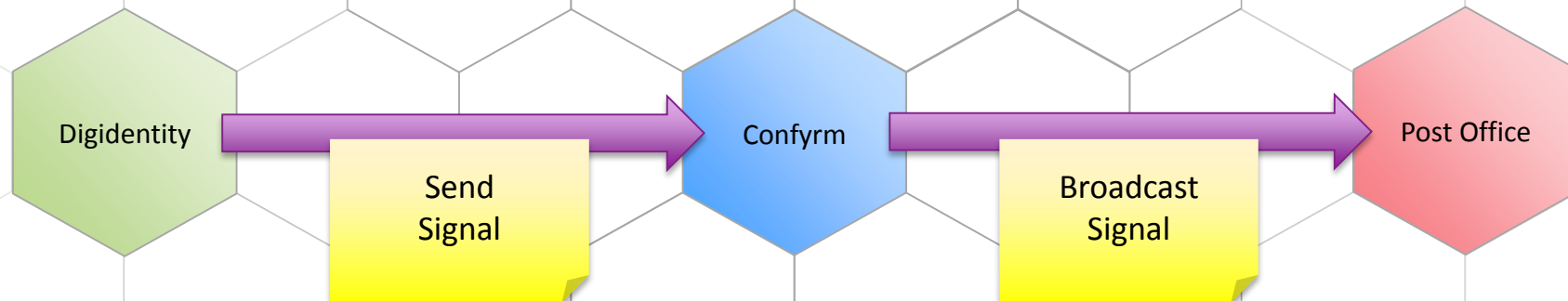
Authoritative Identity Provider Email Provider

conform digidentity RSA Conference 2016

# UK Verify IDP Pilot



#RSAC



# Pilot Progress



- Infrastructure deployed
- API integration complete
- Test signals exchanged
- End-to-end Event Publication and Signal Reception completed
- Digidentity and UK Post sharing events
- Phase II includes other IDPs

# “Apply” Slide



#RSAC

- Be aware that assumed communication paths and trust dependencies are becoming exposures
- Simple event sharing (password resets, account recycling) are a source of really useful early problems
- The Good Housekeeping award requires identity alert handling
- Operation of identity federations is no longer about trusted introductions, it is about trusted operations