Data breaches, identity theft, and online fraud... all the trends are heading in the wrong direction
THE ACCOUNT RESET PATTERN

Forgot Password

Current password
Don't know your password?
New password
Confirm new password
Change Password

Nulla
Incididunt
CLEARINGHOUSE AND ALERTS

• Protect personal privacy / data limitation
• Protect brand of event publishers
• Aggregation of signal recipients
• Standard trust framework
• Aggregation of event publishers
• Lightweight identity alerts
• Real time distribution
• NSTIC development grant
HISTORY

• OIX UK Govt Shared Signals Whitepaper, Sept ’13
• Google Shared Signals Presentation, Oct ‘13
  • October Internet Identity Workshop
• UK IDAP Shared Signals Discovery Project, Sept ‘14
• NSTIC Shared Signals Project, Oct ‘14
• OIDF RISC WG, Jan ‘15
• UK Verify Identity Providers, Nov ‘15
  • Phase II DigID, Post Office, Barclays, GBG, Experian
USE CASE CREATION

• What are actual / emerging issues
• Can an IDP generate an event
• What info could be provided about the event
• Can an IDP utilize the signal
• What information would they need to process the signal
• How could we minimize the data exchange
REGISTRATION VELOCITY

User

Process as show in Flow 1 until...

Requests alternative/additional proofing

Quits attempt

“IdP ‘A’”

Sends Registration Velocity Alert

“IdP ‘B’”

Broadcasts Registration Velocity Alert

“Signal Manager”

Showing only one IdP for simplicity. In practice the alert is sent to all IdPs to prevent fraud across the entire network.

Alerted by Signal
recognises cross-IdP repeat registration attempt; raises burden of proof

Requests alternative/additional proofing

User cannot progress attempt
Fraud is prevented

“IdP ‘B’”

“Signal Manager”
ATO / GHOST IDENTITIES
UK COMMERCIAL HIGH ASSURANCE

• “Registration Velocity” & “Account Takeover”
• Infrastructure deployed
• API integration
• Test signals exchanged
• End-to-end Event Publication and Signal Reception
• Phase II includes other IDPs
• OIX report: http://bit.ly/1t5IUUY
FINDINGS / RECOMMENDATIONS

• Sharing signals successfully addresses threats difficult to address otherwise
• Encrypt rather than hash payloads
• Registration velocity has other variations
• Ghost identity class of threats have other potential triggers
WHERE TO NEXT…

- Strong interest in a follow on project
- Observers have indicated desire to move to active participant status
- At least one use case has already been proposed
EU Cooperation – Identity Signals
OIDF RISC WG
Sharing online identity signals
phil@shield.com uses the same password at all of his sites. 60% of the population does too.