



---

# The Shared Signals Model

**Distribution of Significant Account Events for  
improving integrity and decreasing fraud in online  
transactions**

**A White Paper**

**THE OPEN IDENTITY EXCHANGE**

By Andrew Nash, Conform Inc

## Executive Summary

Fraudulent takeover of Consumer accounts and subsequent misuse is a significant problem that occurs daily at Identity Providers. Consumer information is destroyed, reputations are damaged and the users of these systems often incur financial losses. The financial impacts on these Account Managers of detecting and remediating these problems are huge, and the losses incurred by Service Providers that rely on them may be significant. Accounts fraudulently created or taken over by adversaries are then used to launch attacks on other Identity Providers or Service Providers.

The Shared Signals model describes a new collaborative system that enables intelligence sharing between Account Managers (e.g. Identity Providers) to reduce the impact of fraud and account theft on Identity Providers and consumers. Intelligence sharing is limited to **event evaluation** and **information signaling** at an **account management level** and does not require insight into user level transactions. The model defines a system that supports fast detection and signaling of simple and cascading Identity threats and utilizes policy-based controls, event transformations and criteria-based alerting to meet the varying needs of particular Identity Providers.

While the immediate value of Shared Signaling is described here in the context of online Identity Providers, the model translates to any system of Account Managers, and could be utilized directly by mobile operators.

Operational identity systems are constantly a target of attacks and constant changes. Account takeovers, fraudulent creation or use of accounts and identifiers and a growing and changing set of attack vectors and schemes all increase the cost of operating the system for Account Managers and create loss and pain for consumers.

Identity Providers and other Account Managers receive timely information from a richer collection of sources in the Shared Signals model. The high costs of recovering from account takeover events and reestablishing correct ownership of accounts is reduced by better leveraging information sources.

The deployment of a Shared Signaling model allow Identity Providers to provide a new level of protection to their user base and reduce the operational costs for detecting and recovering from fraudulent activity. These protections include early detection of orchestrated fraudulent activity, reduction in the impact of identity theft, risk evaluation inputs for IDP decision-making and creation of additional tools for Cyber Security evaluation and operation.

At a technical level a Signal Manager receives event notifications and applies policy controls, transformations and evaluations on the event stream and shares resultant signals. At a business level, a Signal Manager establishes a trusted information exchange model that allows competitors to share account and event information assured that such submissions will pose no competitive threat.

Shared Signaling is an informative mechanism. **The Signal Manager does not dictate actions that should be taken by Account Managers, but rather provides a source of business and operational intelligence that can be evaluated by Account Managers as part of their risk evaluation processes.**

The approach described here does not require sharing personally identifying information. The information shared is limited to the account identifiers already owned by the Account Manager and contextual information associated with the events that trigger a signal. As appropriate, double blind mechanisms may be used to provide additional information hiding for account identifiers.

Implementations of this model may employ different technical and policy mechanisms to address the specific requirements of a particular jurisdiction for legal, compliance, policy and privacy needs. Proof of concept testing provided by programs such as the UK IDAP Alpha program need to identify particular architectural and jurisdictional issues.

## Table of Contents

Executive Summary .....	1
Foreword .....	2
Account Take Over and Subversion .....	3
The Shared Signals Model - Overview .....	3
Operating an Identity Infrastructure .....	4
Mugged in London, Paris, Detroit ... ..	4
Cascading Identity Attacks .....	5
Limitations of Single Account Managers .....	5
The Account Web.....	6
A Risk Based Approach.....	6
Existing Shared Signals Models .....	6
US Financial Services.....	6
Mobile Operators .....	7
Shared Signaling Benefits .....	7
The Signal Manager - Principles of Operation.....	8
Use Cases .....	8
Account Take Over (ATO) .....	8
Password Change .....	9
Account Roll-over/Reuse .....	9
Registration Account Linkage.....	9
Recent Account Creation.....	9
Events and Signals.....	9
Events .....	9
Signal Types .....	10
Status Requests .....	10
Policy Controls.....	11
Policy Types .....	11
Global and Local Policies.....	11
Privacy Implications.....	11
Implications for Cyber Security .....	12
Recommendations.....	13
For Further Consideration.....	13
Mobile Information Sharing and Signaling....	13
Consumer Engagement Models .....	13
Terminology .....	13
Account Manager .....	13
Account Identifier .....	14
Identity Provider.....	14
Account Ecosystem .....	14
Service Provider .....	14
Originating Account Manager .....	14
Destination Account Manager.....	14
Consumer .....	14

## Foreword

The Internet is transformational. Yet as the Internet was developed in kinder times, and its core protocols didn't take security into account. While individual islands of innovation, such as **identity providers** or **account managers** have imposed somewhat adequate levels of security, the security and the safety of the ecosystem itself have never been consciously managed.

This white paper describes an approach that enables substantially improved ecosystem safety without compromising control, and without dangerous levels of data sharing that could compromise users' privacy.

This white paper recommends coordination between account managers as they develop their operating policies. The suggestion is for an ecosystem level coordination of the policies utilized by various account managers served by a **single signal manager**.

There are analogies in today's commercial ecosystem. Credit card networks impose unified rules on all their merchants, acquirers and issuers; these rules are designed to ensure the secure operation of the ecosystem. It would be an unfortunate failure to act if similar care isn't taken with account manager operating policies.

The importance of a similar coordination between the public and private sectors seems especially important in the UK's Identity and Assurance Programme. Critical to the IDAP deployment is the required interdependence of government and commercial suppliers and even identity providers.

From a cyber security perspective, the UK IDAP and US FCCX systems and others will be the target of fraud and other malicious attacks on deployment. It is therefore incumbent upon both government and commercial suppliers to use all appropriate tools, such as the shared signals manager, to mitigate risk and contain costs associated with fraud.

Don Thibeau  
President, Open Identity Exchange

## Account Take Over and Subversion

Every Identity Provider or Internet Account Manager faces daily operational challenges of account take overs, subversion and the cost and pain of restoring access to the rightful owners of accounts.

Mat Honan, a well-known journalist, documented his experiences in losing control of multiple Internet accounts in the August 2012 edition of Wired Magazine. <sup>[WM12]</sup> The series of cascading account takeovers utilized by fraudsters in this case are a classic example of the relationships between accounts held at multiple Account Managers and how a takeover of one account may progressively expose all the linked accounts.

Mr. Honan's Google, Twitter, Amazon and Apple accounts were all successively attacked. Each Account Manager in turn was subverted using trusted linkages from the previously attacked account. The goal of the attacker appears to have been to exploit Mr. Honan's Twitter account as a commenting platform, but in addition his Google account was deleted, and information was erased from his iPhone, iPad and MacBook including all images of his new daughter and many professional documents.

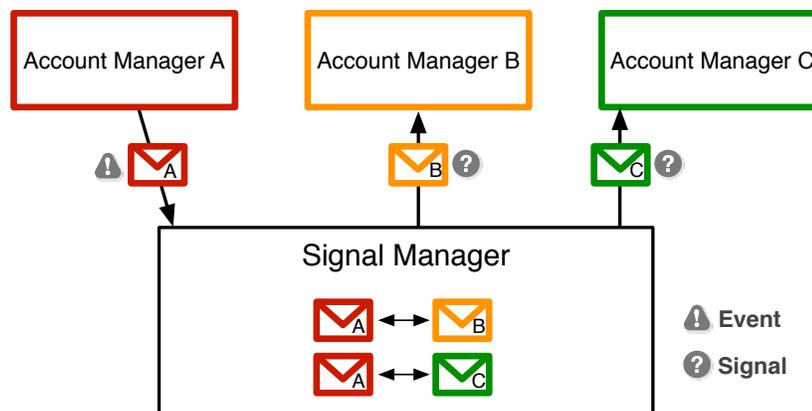
Mr. Honan's experience is not unique. The same issues affect millions of Internet Consumers every year. The impacts may not be as spectacular, but whether it is the minor inconvenience of spam email or major fraud and loss of reputation and funds the problems are endemic.

## The Shared Signals Model - Overview

The term Account Manger is used here in place of the usual designation of Identity Provider as expectations on the functionality of an Identity Provider vary dramatically by jurisdiction. Account Manager in this context does not need to carry the connotation of Identification or Validation of identities as the model works without knowledge of "real identities" In addition; the model may also be applied to other contexts such as the Account Managers utilized by mobile operators.

Account Managers are the principal entities described in this model, although Service Providers that rely on the Identifiers and capabilities of an Account Manager may in some implementations be considered beneficiaries or even participants in the model.

The Shared Signals Model utilizes a Signal Manager to act as a clearinghouse between Account Managers. The Signal Manager receives event streams from Account Managers, applies various policy-based transformations and utilizes triggers conditions to distribute Signals to Account Managers.



Interdependent accounts between Account Managers are the norm. All Account Managers depend on other Account Managers in order to provide a secondary channel for communication with Consumers or activities such as account recovery processing. In general these secondary channels are implemented via email but may include social network messaging services or SMS communications.

While useful for operational interactions, these linked channels form trusted communication paths that are frequently exploited by attackers to gain access to the next account manager or service provider. IDPs do not have any alerting scheme that would allow knowledge of suspect or compromised channels to be shared.

Identity Providers in the UK Government Identity Assurance Program (IDAP) and the US Federal Cloud Credential Exchange (FCCX) system are particular examples of Account Managers that would benefit from the Shared Signals model. In the IDAP scheme, IDPs are responsible for validation, verification, creation, authentication, management and protection of the accounts that support the digital identifier utilized by Government Service Providers. Commercial Service Providers may utilize other implementations of the IDAP system.

Examples of other Account Managers might include Mobile Operators providing a different identifier that takes the form of a mobile phone number or International Mobile Equipment Identity (IMEI).<sup>1</sup> Similar account linkages exist within the mobile operator infrastructure, and progressively are being employed Identity Providers for notification mechanisms.

## Operating an Identity Infrastructure

Any operational Identity Infrastructure supporting authentication and identification is destined to become the target of fraudsters. Single Sign On and Federated Identity systems that utilize an underlying Identity Infrastructure provide many values, but tend to magnify corresponding cyber security and identity theft risks. Subversion of a trusted identifier places all services that rely on it at risk.

The trust attached to those identifiers can be turned against the identity ecosystem if fraudsters are able to gain control of the underlying accounts. It is vital that as the identity ecosystem grows that there be a means of detecting suspect events and sharing intelligence. Doing so enhances the protection of consumers and mitigates the risk to Account Managers and Service Providers. Likewise, an identity ecosystem that does not support a way to detect fraud across the ecosystem creates new vulnerabilities for Consumers, Account Managers and Service Providers alike.

### Mugged in London, Paris, Detroit ...

Everyone has seen occasions where a friend or associate has had an account taken over. Innumerable examples exist of the various outcomes. Common cases include requests for money claiming they have been mugged in some major city and need emergency financial support or generation of spam advocating miracle drugs that will address every medical condition imaginable. The victims will often have all account information such as address books deleted in order to delay the opportunity to notify others that the account has been subverted and misused. Service Providers linked to these accounts may be the target of frauds utilizing trusted account information to purchase goods and services or expose them using trusted communication paths for account operations including password resets.

---

<sup>1</sup> While it is enticing to consider the extension of account identifier support to mobile providers, experience has tended to show that existing business practices, regulation and other compliance issues mean that the sharing of information between the online identity context and mobile context is difficult to achieve. This is the subject of the Further Considerations section in this paper.

## Cascading Identity Attacks

Identity and other fraud attacks are seldom limited to a single Account Manager alone.

A compromised account and the corresponding identifier are often utilized to directly exploit a Service Provider that relies on an Account Manager for identities. However, the compromise at the original Account Manager may be only the first link in a series of cascading steps, where additional accounts are compromised at other Account Managers until an ultimate service is exposed to the attacker.

Frequently Twitter, Facebook and other social network accounts are the targets of spammers or fraudsters looking to use a wider array of services for spamming or theft.

If signaling of alerts between Account Managers had been available, it is possible that in cases such as the one where Mat Honan was the victim, the downstream account takeovers could have been prevented or at least limited. Fraudsters frequently exploit the secondary communication channels utilized by an Account Manager for normal operational support. It is common for an attacker to pretend to be an account owner engaging in an account recovery process. Distinguishing between a genuine account owner in distress, who is trying to recover access to an account, and an attacker pretending the same, requires careful evaluation of all available indicators.

## Limitations of Single Account Managers

Identity systems are notoriously difficult to maintain. Identifying information goes stale; bad information is introduced inadvertently or with malicious intent; passwords change; identifiers may be reallocated; accounts may be misused, or the confidence level associated with them may need to change over time.

Operational identity ecosystems are difficult to understand, interpret and protect when viewed or controlled from any single vantage point. Individual identity providers and relying parties have limited insight into account usage and identification throughout the ecosystem. A gestalt perspective, derived from multiple view points based on sharing signals about account use and misuse, creates a much more powerful set of insights. Each Account Manager contributing information from its own unique perspective helps build a more reliable perspective on fraudulent activity for the whole ecosystem.

An identity ecosystem<sup>2</sup> as a whole benefits from good information sharing about the operation of the accounts that underlie the system. While such information is appropriately recognized as the property of an Account Manager, sharing such information enhances open ecosystems resilience and effectiveness. Analysis of aggregated signals and behavior, provides protection for individuals, increases the security and trust of the ecosystem as a whole and the commercial interests of participating IDPs.

Sharing account intelligence adds a significant tool to address Cyber Security risks and ensure that government web sites have access to timely information that will combat fraud and provide additional protection for citizens and national security interests.

*If a means of protection exists within an Identity System that citizens are required to use, and that protection is financially viable, then it is incumbent on all participants to use all such protections to ensure the safety of those citizens.*

---

<sup>2</sup> An identity ecosystem may variously consist of some collection or subset of consumers, identity providers, identity validators and verifiers, relying parties, attribute brokers and other entities.

## The Account Web

The interconnected nature of consumer accounts managed and maintained at Account Managers and Service Providers is an attribute of the operational nature of any identity system.

If suspicious activity needs to be reported or queried, alternate channels must be utilized to avoid notifying an attacker that the account usage is under suspicion. If access to the account has been lost, evidence of ownership must be presented to regain control without using the account. If a password needs to be reset, alternate communications channels may be utilized in the reset process.

This interconnected web of accounts provides mechanisms that allow other Account Managers linked to the consumer to be notified or signaled that they should be aware of some developing problem.

Account linkages are implicit in the communication between consumer identities. Abnormal usage patterns in those communications mechanisms may be a signal that someone other than the legitimate owner is using the associated accounts.

For example, an email service provider may see significant amounts of spam traffic arrive from an external email user. That may be the earliest signal that could be returned to the Account Manager for the external email user that the account may have been taken over.

## A Risk Based Approach

Shared signaling is an informative mechanism. It does not dictate actions that should be taken by any specific Account Manager.

Different evaluation criteria and operational models may be utilized by each Account Manager to assure the continued protection of the consumer accounts it manages. Today most Account Managers employ some form of risk analysis, including a reporting and response structure designed to handle large-scale identity collections.

Shared Signals contributes to the ongoing risk evaluation criteria employed at an Account Manager.

Policies set by Account Managers may be used to establish trigger conditions, and various transformations of event streams at the Signal Manager before a signal is distributed. However, decisions about actions that should be taken in response to a signal delivery are the responsibility of the Account Manager.

## Existing Shared Signals Models

A few examples of commercial intelligence sharing agreements that are analogous to the Shared Signals model exist already. These systems vary in the “real time” nature and support for policy driven notification. In most cases the information shared is restricted by defined membership agreements.

Two examples are provided here as to frame some of the considerations for these systems.

### US Financial Services

<sup>[FSISAC]</sup>On July 15, 1996, the President of the United States signed executive order 13010 creating the President’s Commission on Critical Infrastructure Protection (PCCIP). This commission was created to bring together the public and private sector to assess infrastructure vulnerabilities and develop assurance strategies for the future. The PCCIP identified the Banking and Finance Sector as one of eight critical infrastructures that require review and assurance strategies.

The Financial Services Information Sharing & Analysis Center (FS-ISAC) provides for authenticated and, when appropriate, anonymous and confidential input from its membership. It also shares and disseminates information associated with physical and cyber incidents, threats, vulnerabilities, and resolutions or solutions associated with the sector's critical infrastructures and technologies.

The FS-ISAC operates under the following principles:

- **Submission Anonymity:** Faith that submissions will pose no competitive threat and will be without attribution to the originating member if the submission is submitted anonymously.
- **Authenticated Sharing of Information:** The FS-ISAC structure will allow certain information, such as events, incidents, threats, vulnerabilities, resolutions and solutions, to be shared in an authenticated, anonymous and private manner. Recipients of alerts are confident information is from an authorized and vetted source.
- **Industry Owned and Operated:** Assurance that the database and input is owned by the Members
- **No Freedom of Information Act (FOIA) Access Control** of the portal by the private sector ensures that the FS-ISAC database is not subject to Freedom of Information Act requests from the press or others that are not members of the FS-ISAC.

## Mobile Operators

<sup>[GSMA]</sup>The GSM Association (GSMA) maintains a unique system known as the IMEI Database (IMEI DB), which is a global central database containing basic information on serial number (IMEI) ranges of millions of mobile devices (e.g. mobile phones, laptop data cards, etc.) that are in use across the world's mobile networks.

The GSMA provides access to the IMEI DB and its data to GSMA member mobile networks operators across the world, and to qualified industry parties (i.e. manufacturers of device management products and regulatory authorities). IMEI's listed in this database correspond to subverted accounts in the Shared Signaling model.

The IMEI DB also supports a black list of IMEIs that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use. This is known as the Central Equipment Identify Register (CEIR), the IMEI DB acts as a central system for network operators to share their individual black lists so that devices denied service (blacklisted) by one network will not work on other networks even if the SIM card in the device is changed.

Network operators that deploy Equipment Identity Registers (EIR) in their networks use them to keep their own lists of black listed devices. Operators' EIRs can connect to the GSMA IMEI DB to share their latest lists of blacklisted devices with other operators. The IMEI DB takes the black lists from the various operators around the world that are connected to system and it compiles the data into one global black list.

## Shared Signaling Benefits

The Shared Signaling model provides significant value to all participants in an Account Management ecosystem.

Consumers benefit when early detection and collaboration between Account Managers reduces the impact of account takeovers and other associated misuse of their identities and accounts. Limiting downstream account attacks, fraudulent use of services, damage to reputation, credit risk and impact on friends and associates in within a social networks are only a few of the benefits that accrue to consumers.

Identity Providers and other Account Managers receive timely information from a richer collection of sources in the Shared Signals model. The high costs of recovering account takeover bursts and the painful process of reestablishing correct ownership of accounts is aided by better information sources. The challenges of discerning between account

recovery requests by the real account owner and an attacker may be simplified if awareness of activity within the identity ecosystem can be utilized.

Service Providers operate with a higher level of confidence that the identities they are relying on have a significantly lower potential to be subverted through the lifetime of the identifier usage.

Enterprises and Government derive Cyber Security benefits when fraudsters and attackers are exposed early and the scope of misuse of identifiers is limited.

## The Signal Manager - Principles of Operation

The Signal Manager is the critical technical and business entity that establishes a trusted information exchange model that allows competitors to share account information assured that:

- Submissions will pose no competitive threat
- No attribution will be made to an Originating Account Manager when anonymous submission is required
- Account Identifiers within the name space of the originating will not be shared unless explicitly requested and agreed to
- Policy controls will support configuration of appropriate Signal delivery
- Signals will be delivered in a timely fashion

Signals that are delivered to a Destination Account Manager will not identify the Originating Account Manager or the Account Identifier that was included in the original Event stream. Mechanisms to facilitate the privacy preserving aspects of a given implementation will vary by Account Manager ecosystem architectures but may include double blind mechanisms to provide additional safeguards on identifier usage.

All event streams, policy application, transformations will be logged and audited to ensure correct operation of the Signal Manager.

## Use Cases

Examples of some of the more common use cases facing an Identity Provider or Service Provider.

### Account Take Over (ATO)

One of the most common events at any large-scale consumer Identity Provider is take over of an account by an attacker. Depending on the type of Identity Provider, unauthorized access to accounts will expose address books; allow misuse of trusted communication paths; facilitate assumption of trusted relationship status with other consumers; and provide additional identifiers with which to launch wider down stream attacks at other Account Managers or Service Providers.

Typical impacts on the consumer include financial loss, destruction of personal data such as email, photographs and address books, damage to reputation based on activities in social and business networks, loss of productivity and the pain of coping with the loss of trust and reestablishing ownership of the account and later recovery actions.

Detection of ATOs will often be triggered by internal risk evaluation processes at the Account Manager but may be the result of the consumer reporting an event or external recognition of associated events such as spam generation or malware propagation by the account.

The earliest possible signaling of an ATO allows much faster discovery of similar issues at associated Account Managers and limitation of many of the issues described above.

## Password Change

Password change events are a regular and often normal occurrence. The password change event may be benign, such as the result of password update policies, or it may be in response to inimical activity such as recovery from an account take over.

Any associated Account Manager or Service Provider that has a session established based on the earlier password usage (or any shared secret) should cause a session reset of some form to ensure that subsequent activities or transactions are occurring with the consent of the consumer. In cases where session resets are required by a given trust framework or service agreement, the Signal Manager provides a scalable distribution point to support such notifications.

## Account Roll-over/Reuse

Identifier reuse is a common practice among some of the largest Identity Providers and Account Managers on the Internet. At very large scale, flat name spaces such as those implemented by email providers and social networks result in unwieldy, unfriendly and nearly unusable identifier names. To maximize the use of “good identifiers” some Account Managers will allow a previously used identifier that is no longer “active” to be recycled and reissued to a different consumer.

This can present a major problem to associated Account Managers or Service Providers that rely on the identifier for communication or recovery mechanisms. The identifier in use may at any time, without warning represent a different user. This mechanism has actively been utilized by fraudsters to attack associated Account Managers.

Account Managers that allow identifier reuse could signal the change in state or ownership of an identifier, allowing associated Account Managers and Service Providers the opportunity to take some form of remedial action.

## Registration Account Linkage

A common fraud pattern is for an attacker to obtain an existing identifier, often via an Account Take Over, and then use it as the basis for establishing a new account at a Service Provider. Allowing queries on the known status or current signal stream of an associated account at registration time would provide a useful check that may circumvent downstream fraudulent activity.

## Recent Account Creation

A close variant on the previous case is where a new identity is created at an Identity Provider expressly for the purposes of using it during the registration process at another Account Manager or Service Provider. Signals showing the “recency” of account creation would help limit establishment of interconnected networks of fraudulent identifiers.

## Events and Signals

Various types of information may be sourced or delivered in the context of a shared signals model. Information is variously categorized as Events, Signals and Status Requests.

### Events

Events are defined as a set of source activities or occurrences at an Account Manager or other entity in the identity ecosystem. They may be derived by internal systems or be externally observed.

Events corresponding to the use cases described above may initially include:

- Account Take Over
- Password Change
- Account Reuse
- Account Linkage
- New Account Creation

Events are delivered to the Signal Manager where policy controls and transformations may be applied to generate particular Signals.

## Signal Types

Signals are notifications that are generated by the Signal Manager and passed to Account Managers or Service Providers. Some set of events or other activities, triggers, thresholds and historical context may be processed in conjunction with various policies to generate a signal. Signals may be specifically targeted, multicast or broadcast to recipients also based on policy controls. The information delivered as part of a Signal may also be controlled by policy to allow finer grain control on information based on trust levels, privacy requirements or data hiding.

Mechanisms for delivery of signals will generally be asynchronous or timed and delivered to a nominated listener. Triggers for Signal distribution will generally be the result of event activity within the ecosystem or based on evaluation at the Signal Manager.

Signal types corresponding to the use cases described above may initially include:

- Associated Account Impacted by Account Take Over
- Password Change may Impact Existing Sessions
- Associated Account Identifier Recycled
- Associated Account Status
- Associated Account Creation

Specific signal types may be defined for particular operating contexts to support the additional signal needs or available event streams for particular classes of Account Managers.

Additionally, to ensure correct operation of the signaling system itself and to allow for notification of a restoration of a normal operating state for accounts, an All Clear signal must be triggered by the Account Manager that originated events such as Account Take Over. It is generally expected that such signals will be indicative rather than directive, but this may be modified by specific implementations and Global Policy agreements for the Account Manager Ecosystem.

## Status Requests

Some information available may be best utilized within the process flows of an Account Manager or Service Provider. In those cases provision is made to allow a request for information on the status or signal stream associated with an identifier to be queried.

Status requests are may result in a synchronous response but may also have appropriate asynchronous delivery requirements depending on where pertinent information needs to be sourced from and whether a notification time period is nominated.

## Policy Controls

Policy controls for the operation of Shared Signals are required to support the Principles of Operation described above including support of individual Consumer privacy, establishment of business trust, terms of service delivery, information sharing agreements and tunable signal delivery.

### Policy Types

Where possible, it is desirable to establish most policy principles at an ecosystem level utilizing a model similar to those described by the OIX Trust Framework. This would allow a common set of expectations to be established and agreement on responsibilities and behavior for the various participants. Issues including limitations on information sharing, ombudsman processes, common event and signal types and a range of other topics.

Some bilateral agreements could be reached that would allow more business information to be shared between some Account Managers that had higher levels of business trust. For example, it is expected that the normal mode of operation would hide the origin of specific source events in order to protect business reputations. It is possible, however, that two closely allied account managers might be comfortable sharing more contextual information with each other that would further improve reaction time.

Technical and business policies are needed between each Account Manager or Service Provider and the Signal Manager. For example, a particular Account Manager may wish to throttle signal arrival rates or batch notifications for performance or business processing reasons. Sensitivity thresholds on reporting particular signal types or determining an alert level may also be useful.

### Global and Local Policies

The fundamental expectation is that for Account Managers, signals produced by the Signal Manager are informative rather than directive. Most signals will be processed as part of a risk based evaluation process and individual Account Managers may have different criteria for how and when to make decisions affecting the accounts they manage.

There are some notable possibilities for “global” policy expectations. All Account Managers should recognize and evaluate the “All Clear” signal triggered by an Account Manager that originated an event such as “Account Take Over”. It is possible that other Account Managers may wish to do additional evaluation before taking specific action. While particular implementations may choose to make such Global policy handling more or less proscriptive, in order for the system to allow correction of errors the signals must at least be generated, received and evaluated.

Global policies will vary by jurisdiction and need to account for privacy and legal constraints. Semantic mappings and transformations of incoming events to outgoing signals are a policy consideration at a Signal Manager. In addition, architectural choices made by Account Managers may require particular policy based transformations at the Signal Manager such as hiding identifiers for directed identity purposes utilizing hashing or mapping. These requirements are not universal and should be specified in the trust framework agreement governing participation in a particular Shared Signaling implementation.

## Privacy Implications

Privacy is a principal concern in a model such as Shared Signaling. Although the nature of the information that is being shared is primarily operational, provision must be made to allow review and response on behalf of individual consumers particularly to provide an Ombudsman Channel to ensure information is corrected.

Exact definitions of Personally Identifying Information (PII), allowable use for fraud detection and prevention, consumer permission and other issues in this area are specific to particular jurisdictions. The trust framework defined for any given implementation of Shared Signals must necessarily consider these topics in detail. This section describes some approaches and questions, but does not assume that the principals are universal or necessarily applicable in all implementations.

The fundamental information that is shared is restricted to an account identifier rather than real world identifying information such as “real names”, physical address etc. The goal is to signal information about accounts, not people.

There is a grey area when account identifiers have been selected by the consumer to correspond to a real name. However, the identifier associated with an event reported by an Account Manager (such as an ATO) is not included in the signal that is propagated by the Signal Manager. Even so, it is a requirement that all participants treat all account identifiers as sensitive information.

The analogue to the Shared Signals model that may be most appropriate is that of fraud notification between banks. In those systems it is generally recognized that information shared with the consumer must be restricted lest fraudsters be alerted to a current investigation or remediation activity.

In the use cases envisaged it is the Account Manager that owns the account and event information shared. It is business knowledge derived from the operations of specific Account Managers.

However, where possible, it is desirable that a consumer notification service be established that would allow individuals to be notified where practicable of signals that have been issued associated with them. The inclusion of such a service may be a policy consideration for the Account Ecosystem as a whole or may be left to a particular Account Manager to decide how and when to include consumer notification and engagement in the process.

In support of a model that allows correction of false positive events, three elements are required:

1. An **Online Ombudsman Process** needs to be established to ensure consumers can identify problems with Account Manager events and corresponding signals generated and have a means to seek correction
2. A **Redress Signal** must be supported in order to allow reset notification to all Account Managers and Service Providers that a signal was incorrectly generated
3. All Account Managers and Service Providers must handle an **All Clear Signal**. This signal should serve as an indication that the Signal Manager has information indicating that normal usage of a Consumer’s identifiers should continue from this point. It should be noted that risk engines at individual Account Managers and Service Providers will consider this as an indication as they do with all other signals.

## Implications for Cyber Security

Attack vectors for many Cyber Security events depend on the fraudulent assumption of trusted identities by an attacker or the creation of ephemeral identities for the purposes of launching some form of orchestrated series of events.

We have been severely hampered by the lack of timely notification of events such as account take over, suspicious activity or even basic information about the recency and velocity of account creation and use.

Shared Account Signals establishes a critical alerting structure that supports timely recognition and interception of Cyber Security attacks that utilize consumer identifiers. This has enormous potential to reduce threats to global cyberspace infrastructure in addition to reduction in loss and damage to individual consumers.

## Recommendations

Shared Signals is a simple concept that has enormous potential power. Much of the opportunity lies in facilitating trusted exchanges of information between competitors – **no single Account Manager could be trusted by all other Account Managers to establish such a clearinghouse**. Furthermore, the participation by account managers in multiple ecosystems requires that Account Manager intelligence sharing operate across all ecosystems.

These two requirements motivate establishment of a new third party service that is trusted to protect the interest of all participants, independent of the ecosystems supported.

While the fundamental concepts and technology required to support a Shared Signaling Model are not complex, the operational agreements and policy constraints that create a fair and valuable service for Consumers, Account Managers and Service Providers need further investigation and prototyping.

It is recommended that prototype deployment should be undertaken to validate the claims and expectations that have been raised here.

## For Further Consideration

### Mobile Information Sharing and Signaling

Information sharing between Account Managers is not restricted to email addresses or other online communication methods. Mobile phone numbers in conjunction with SMS notifications or customer contact methods form a valuable set of adjunct signal types and information. Experience has shown that even with all good will, that sharing such information outside of mobile carriers (often even within them) is very difficult. Various businesses, compliance legislative and other valid reasons including operational constraints may be the reason for these issues.

Despite this, it is highly desirable that mechanisms and models that facilitate sharing of information between Identity Providers and Mobile Operators be considered and trialed.

### Consumer Engagement Models

The principles and operation of supporting infrastructure such as an Ombudsman Channel and the consumer engagement model need more consideration. In general it is assumed that any particular implementation of a Shared Signals system will make specific choices depending on the needs, context and operating principles of the Account Managers participating in the system.

There may be merit in allowing consumers more direct engagement mechanisms both to report a subverted account or to receive notification of inimical activity on an account. Legal, compliance and privacy constraints that support or prevent such engagement vary dramatically by jurisdiction.

The viability of consumer engagement for various use cases and the establishment of an Ombudsman Channel are topics that need more focused attention in the descriptions of specific implementations of Shared Signaling.

## Terminology

For the purposes of this white paper, the following definitions of terms are provided. Terms described here generally fit with broad Internet and Identity System usage but are intended to address the more narrow confines of the use cases and context discussed in this paper.

### Account Manager

An Account Manager is the operational entity that owns and manages Consumer accounts. In many cases this may be represented by an Identity Provider, but is not limited to that case. In general, all Identity Providers are Account Managers, but not all Account Managers are Identity Providers.

### Account Identifier

The digital identifier provided by an Account Manager and utilized by another Account Manager or Service Provider. In this context, the Account Identifier is not directly tied to a “real world” identifier of an individual person.

### Identity Provider

An Identity Manager for the purposes of this model is a special case of an Account Manager that may to some degree validate and assert the association between the account and identifier that is managed and an individual person.

### Account Ecosystem

For the purposes of this paper, the Account Ecosystem is comprised of a set of Account Managers, some or all of which may originate events and receive signals, and optionally a set of Service Providers that may receive signals.

### Service Provider

Any online service that may be accessed by utilizing a Consumer Identity, whether for personal, business or government reasons. Examples might include mobile applications, web applications, and email or search services.

### Originating Account Manager

The Account Manager that delivers an Event stream to the Signal Manager

### Destination Account Manager

One or more Account Managers that receive a Signal from the Account Manager either as an asynchronous notification based on activity within the Account Ecosystem, or in response to an explicit request for information about an account.

### Consumer

Consumer here is used in its most general sense to connote “a consumer of online services” generally delivered over Internet protocols. In this sense, the term may include more specific classes of consumers including Citizens, Employees, Customers and Service Users.

---

<sup>[FSISAC]</sup> This section is directly drawn from the description of the FS-ISAC system operating rules located at: [https://www.fsisac.com/sites/default/files/FS-ISAC\\_OperatingRules\\_2012.pdf](https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2012.pdf)

<sup>[GSMA]</sup> This section is directly drawn from the description of the GSMA IMEI Database system located at: <http://www.gsma.com/technicalprojects/fraud-security/imei-database>