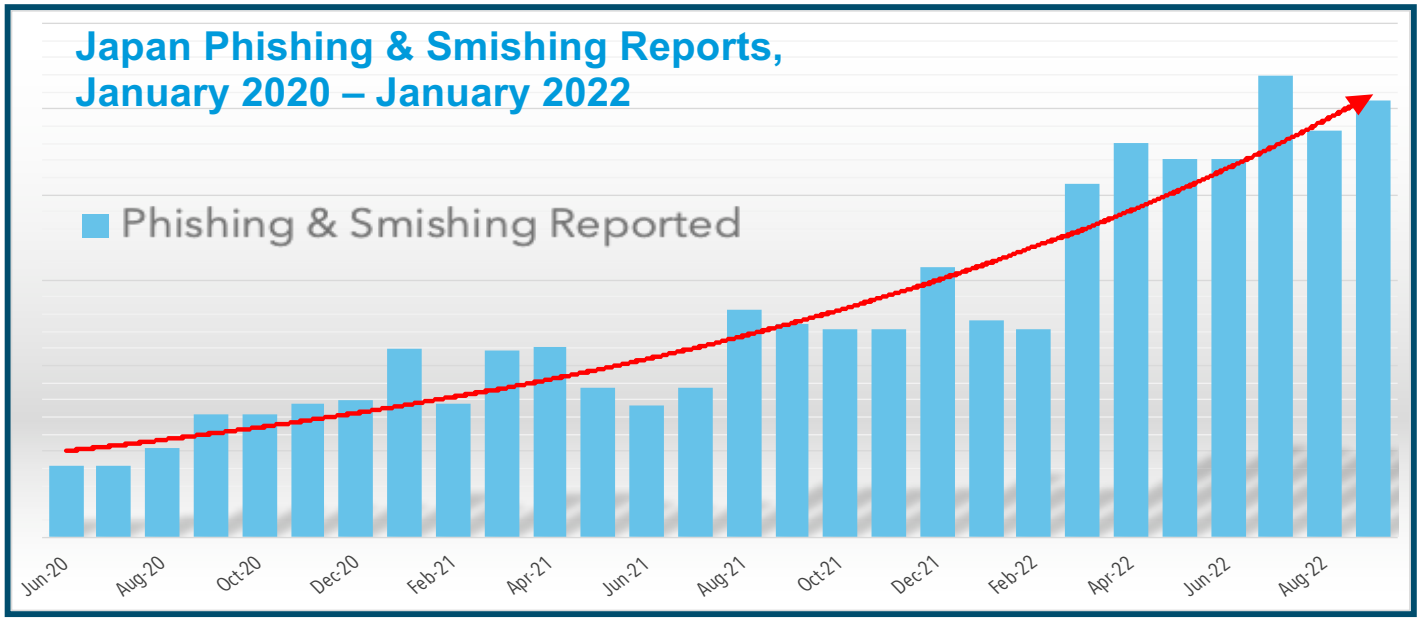

proofpoint
CLOUDMARK
A PROOFPOINT COMPANY
Mobile Abuse Evolution
November 2022
Michael Blum, Mobile Product Manager

Agenda

- Mobile Accuracy Challenges
  - Chasing URLs
  - Obfuscation Tactics
- Mobile Accuracy Tactics
- Business Messaging

Regional Phishing & Smishing Combined Trends: Japan

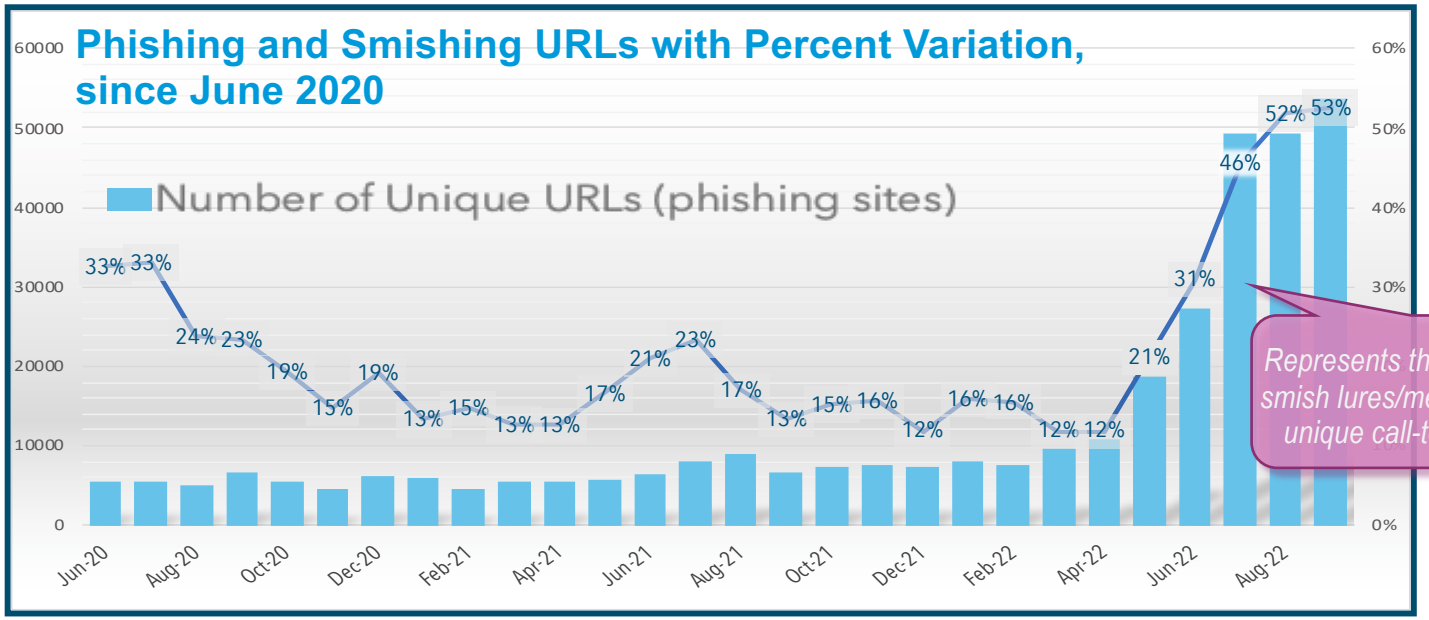


- Data from Council of Anti-Phishing Japan
- Consistent increase of abuse across both Email and Mobile

Source: Council of Anti-Phishing Japan
https://www.antiphishing.jp/report/monthly/202210.html

proofpoint.

Sophistication: URL Rotation is Increasing

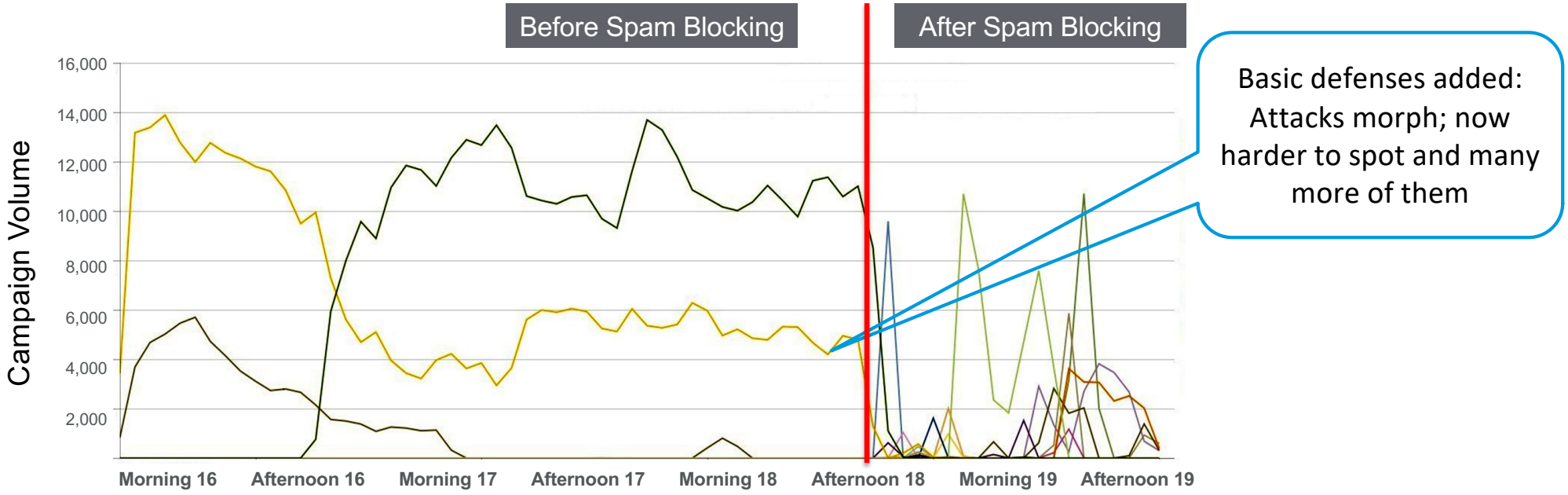


- URL Rotation on the rise: Unique URLs in attacks increasing
- Consistent with other regions as attackers change tactics, more difficult for traditional systems to detect *campaigns*

Source: Council of Anti-Phishing Japan
https://www.antiphishing.jp/report/monthly/202210.html

proofpoint.

Basic blocking tactics



Rudimentary Concepts In Defense

Seemingly Low Complexity / Few Attack Variations Easy to block with:

- URL blocks
- Number Blocklists
- Simple Volumetrics Limiting

New Attacks - Difficult To Defend

Rapidly mutating attacks

- More sending numbers
- Random/Obfuscated content
- Rotating URLs

proofpoint.

Obfuscation via Homoglyphs

Content	MD5
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	cef216367b00556002ebec6b0506d62b
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	B45ffb99292c8b0322e3bfb6b511cea8
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	E93930dfaebbd97de6223e4f48eb43e6
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	Cde986d7ec8c265c28f7dbc4c8c1f260
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	316ec752879e96a7fde8fefdc1b4401e
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	B7b457e9df87cc8987e15234e12b9d37
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	0776f26681a5ef28583d2b9540f4b1b7
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	751dc1f08aa731c7c79d11bdbd1cc465

Obfuscation via Homoglyphs

Content	MD5
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	cef216367b00556002ebec6b0506d62b
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	B45ffb99292c8b0322e3bfb6b511cea8
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	E93930dfaebbd97de6223e4f48eb43e6
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	Cde986d7ec8c265c28f7dbc4c8c1f260
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	316ec752879e96a7fde8fefdc1b4401e
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	B7b457e9df87cc8987e15234e12b9d37
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	0776f26681a5ef28583d2b9540f4b1b7
В ДЕЯ CONCEPT CLUB цены продолжают таять! Скидки до 70%! Спешите!!!	751dc1f08aa731c7c79d11bdbd1cc465

http://unicode.org/cldr/utility/confusables.jsp

proofpoint.

Highly Mutating Messages

Jeniffer,Apply This Daily and Observe Your Bags Under Eyes and Lines And Wrinkles Fade AwayVisit EraseWrinklesX.us to learn moretxt 4 to quit

Nasem,Apply This Once A Day and Watch Your Bags Under Eyes and Old Wrinkles Fade AwayGo to FreeWrinkleFaceX.us to read moreRply 9 to unsub

Tamra,Apply This Every Day and Observe Your Eye Bags and Wrinkles DisappearGo to FreeWrinkleFaceX.us to learn moretxt 2 to unsub

Elaina,Apply Like This Once A Day and Look At Your Eye Bags and Old Wrinkles Fade AwayGo to WrinklesEraserX.us to learn moretxt 2 to quit

Christine,Apply Like This Daily and Look At Your Eye Bags and Wrinkles EvaporateGo to WrinklesEraserX.us to learn moreRply 4 to unsub

Tracy,Apply Like This Daily and Look At Your Puffyness and Old Wrinkles EvaporateSee EraseWrinklesX.us for infoRply 7 to unsub

Joy,Apply This Every Day and Look At Your Eye Bags and Lines And Wrinkles Fade AwayGo to EraseWrinklesX.us to learn moreRply 7 to end

Jolene,Apply This Every Day and Observe Your Bags Under Eyes and Wrinkles DisappearGo to FreeFromWrinklesX.us for infotxt 2 to quit

Sherry,Apply Like This Once A Day and Look At Your Bags Under Eyes and Lines And Wrinkles DisappearGo to WrinklesEraserX.us for infoRply 2 to cancel

Tracy,Apply This Every Day and Observe Your Under Eye Bags and Lines And Wrinkles DisappearVisit AntiAgingFormulaX.us for infoRply 5 to cancel

Catherine m,Apply This Every Day and Look At Your Under Eye Bags and Old Wrinkles DisappearVisit WrinklesEraserX.us to see howRply 1 to end

Miriam,Apply Like This Every Day and Watch Your Bags Under Eyes and Wrinkles Fade AwayVisit WrinklesEraserX.us to learn moretxt 2 to unsub

Joy,Apply This Daily and Observe Your Under Eye Bags and Old Wrinkles EvaporateGo to AntiAgingFormulaX.us to read moretxt 6 to end

https://en.wikipedia.org/wiki/File:Whac-a-mole_-_Tokyo_-_Jan_7_2020.webm#file

proofpoint.

Effects of Smishing

Smishing impacts everyone in the Mobile Value Chain

Consumer Impact

- Loss of Personal Information
- Financial Loss
  - Japan: 1.13 Billion Yen lost due to online banking fraud according to Stastia
  - Australia: A$3.1 million in losses directly related to SMS message scams (Australian Consumer & Competition Commission)
  - US: Greater than $86 million loss from smishing alone, circa 2020 (US Federal Trade Commission)

Mobile Network Operator Impact

- Brand erosion and decreased consumer trust due to consumer vulnerability
- Large volume smishing and malware attacks cause direct impact on MNO operations/expenses
- Increased customer support calls and complaints plus follow up with device sanitation causes financial loss

Enterprise/Corporate Impact

- Brand erosion due to impersonation attacks and consumer misidentification of bona fide corporate communications
- In Septermber, 76 different brands were abused in Japan††
- Top 10 brands abused in Japan represent 82% of attacks. Top 3: Amazon, Apple, and DoCoMo are prominent

†† Council of Anti-Phishing Japan
https://www.antiphishing.jp/report/monthly/202109.html

proofpoint.

Mobile Abuse Tactics

proofpoint.

Fingerprinting

- Fingerprints represent ***indicators*** of message content
  - URLs
  - Content Strings
  - Phone Numbers (in the message body)
  - ...
- Fingerprints can also represent metadata ***indicators*** of a message
  - Types of character sets contained within a message
  - The presence of a URL in a message
  - Indications of obfuscation within content
  - …
- Fingerprinting is ***powerful and easily extensible***
  - Fingerprinting engines can easily be enhanced to generate new types of fingerprints ***without requiring code changes and new software deployments***
  - Advanced preprocessing and normalization capabilities

proofpoint.

Fingerprinting Engines

- Fingerprinting Engines target different types of content
  - Preprocessing / ”Normalization”
  - URLs: TLDs, Multi-level domains, URIs
  - String / Word Patterns
  - Images
  - Binary / Executable Content

- Adaptable Fingerprinting engines that can be adjusted to fingerprint in new ways
  - Adjustable match patterns
  - Embedded lua / scriptable engine

proofpoint.

“Indicator” Fingerprint: Example

- The following message:

[◌ア◌マ◌ゾ◌ン]プライム会◌費のお支払い方◌法に問◌題があります: https://amazon-reset.com

- May generate the following fingerprints:
  - **Indicator Fingerprints**:
    - a=aksifue51sx:22 Indicates that the message contains Unicode Katakana/Kanjii characters
    - a=ksjfuka2fkah:22 Indicates that the message contains Unicode Arabic characters
    - a=9dsfksd9w2:22 Indicates that the message contains Unicode zero-width characters
    - a=ksifn8skahs:10 Indicates that the message contains a URL
  - **Content Fingerprints**
    - a=9sdfnadafka:8 A unique fingerprint representing the URL amazon-reset.com
    - a=jasnasd8faa:9 A fingerprint representing a hash of the body content string

proofpoint.

Normalization

- Content Normalization Engine
  - Preprocessing engine that executes on content before fingerprints
  - Applies multiple transforms to messages/content
  - Can easily and dynamically be updated to apply new transforms based on changing conditions and scammer tactics
  - New instructions distributed by use of a remote update mechanism

- Example Transforms
  - "Visit www.ama***zo***n-r***e******s******e***t.com"

  ➔ "Visit www.amazon-reset.com"
  - "Please verify your password by calling 1-456-CIT-BANK"

  ➔ "Please verify your password by calling 1-456-248-2265"

proofpoint.

Intelligent Policy

Using “Signal” fingerprints can be used:

a=aksifue51sx:22
a=ksjfuka2fkah:22
a=9dsfksd9w2:22
a=ksifn8skahs:10

contains_unicode_katakana
contains_unicode_arabic
contains_unicode_zerowidth
contains_url

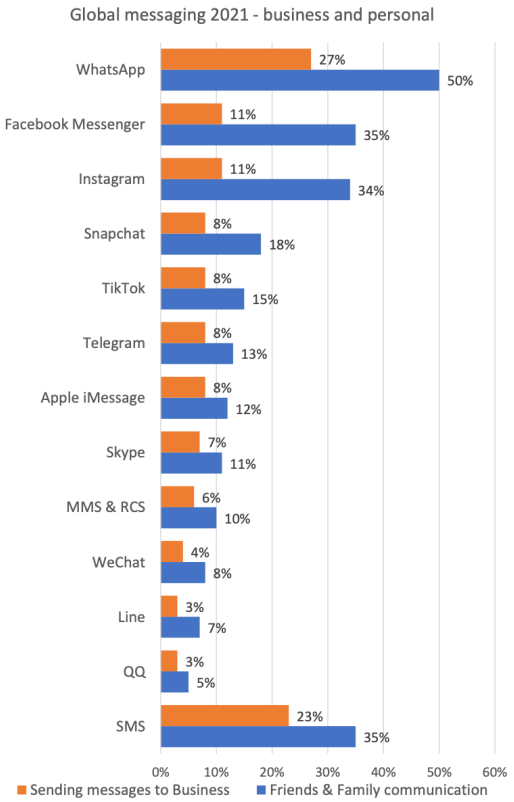
BLOCK based on combination of intelligent indicators

proofpoint.

Business Messaging

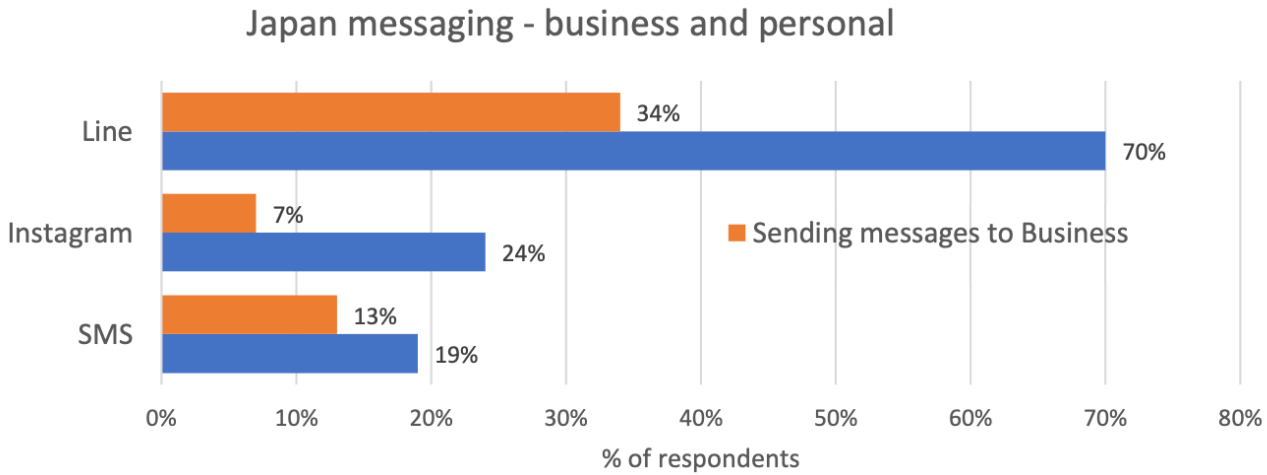
proofpoint.

Ubiquitous Messaging Channel



Globally SMS/MMS is a strong Commercial Channel

After Line, SMS is the main Channel in Japan



proofpoint.

MEF MOBILEECOSYSTEMFORUM.COM

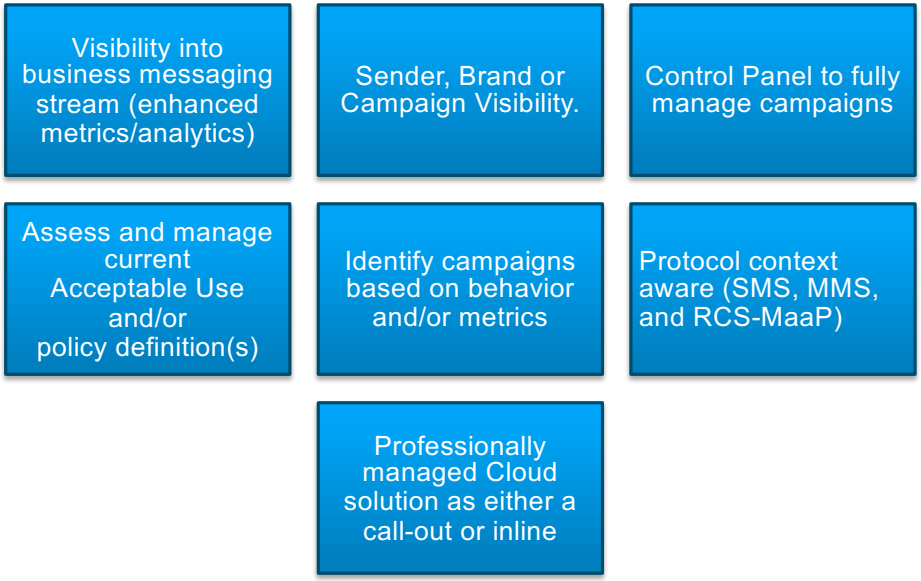
Platform for Business Messaging Management

- Gain insights through advanced visualization and forensics regarding legitimate campaigns, while protecting against abuse targeting subscribers
- Identify A2P content, ensuring it's on the right path, properly rated, and monetized
- Manage and enforce policies to maintain mobile, enterprise, regulatory requirements

Value:

- Accurately price your business messaging according to use (2FA, Advertising, Notifications, First Responder)
- Ensure your customers view your Business Messaging as "wanted" – mitigate abusive sending practices
- Single source of management for your Business Messaging

Solution Functionality



proofpoint.

Solution: Platform for **Mobile Messaging Security**
JIRA: PMMS

Internal Use Only – Sales Enablement

Accurately price your business messaging according to use (2FA, Advertising, Notifications, First Responder)

Ensure your customers view your Business Messaging as “wanted” – mitigate abusive sending practices

Single source of management for your Business Messaging

- Visibility across all A2P vendors regardless of source
- SPAM / Fraud Management
- Continual feedback provided by SRS on current campaigns to detect SPAM, AUP violations, unmanaged STOP requests, etc.
- Single connectivity management point for ALL A2P messages destined for Operator.
  - Creates consistency across all Campaign senders
  - Enforcement options, i.e. blocking/throttling, content audits, MNO AUP Guidelines, CTIA Guidelines, etc
  - Flexible management tools that support 10DLC management objectives

proofpoint.

Solution: Platform for Business Messaging Management

JIRA: PBMM

Single Point of Control for Business Messaging with Policy Management and Enforcement

- Campaign Registry adherence
- Customer Feedback loop via SRS (7726)
- CTIA and AUP enforcement
- SPAM / Fraud Protection
- Extensive Analytic capabilities
- Monitor for stop messages