feedzai GASA Global Anti-Scam Alliance

Introducing the Scam Footprint

Definition. Responsibility. Measurement. Reduction.

Abstract

The goal of this consultation paper is to propose a cross-sector action plan for preventing scams

- Robert Harris, Jorij Abraham
Jan 2024

Contents

1. Introduction

1.1 Why this Discussion Paper?

Scams have become a global epidemic. Consumers worldwide lose more than $50 billion every year as a result. The social and emotional trauma cannot be measured. In many countries, scams are the most reported type of crime with 50% in Singapore and 41% in the UK just two examples from countries that have some of the most effective tracking in place.

Actual losses are far higher, as only an estimated 7% of all scams are ever reported. There is little incentive to report as a mere 0.05% of all cybercriminals are caught, and new technologies like Deep Fakes and ChatGPT are making it increasingly harder for consumers and law enforcement to identify deceit.

Governments and security companies have traditionally focused on fighting “Organized Cybercrime” that targets corporations and national infrastructure. However, this ignores the fact that online scams are harming consumers and diminishing their trust in the global digital economy which now represents 15.5% of global GDP. This is unacceptable, and more needs to be done to protect consumers worldwide.

At the 3rd Global Anti-Scam Summit in November 2022, **1,300** (virtual and physical) **participants** collectively formulated Ten Recommendations to Turn the Tide on Scams to enhance consumer protection against global scams. One of these **recommendations** is to **Make Service Providers More Responsible for Scam Enablement**. This paper provides a forum for all industry participants to share what they are doing in support of this recommendation, progress to date and where assistance from others is needed to protect consumers.

Consumers worldwide lose more than $50 billion every year as a result.

1.2 Why this Discussion Paper?

“A scam is a fraudulent scheme or deceptive practice, usually aimed at obtaining money, personal information, or valuables from individuals or organizations through dishonest means.”[1]

1.3 Make Service Providers More Responsible

Scammers use the Internet the same way as legitimate companies and carefully devise their ‘customer’ journeys from the outset. They plan their operation, cast their nets to get customers, hook their victims, land the money and rinse and repeat the process to continuously adapt and improve their scams.

As the scam journey illustrated in the figure below shows, criminals rely on a number of industry participants: registries/registrars, hosting companies, SSL providers, social media, telecom operators, search engines, banks and other payment providers.

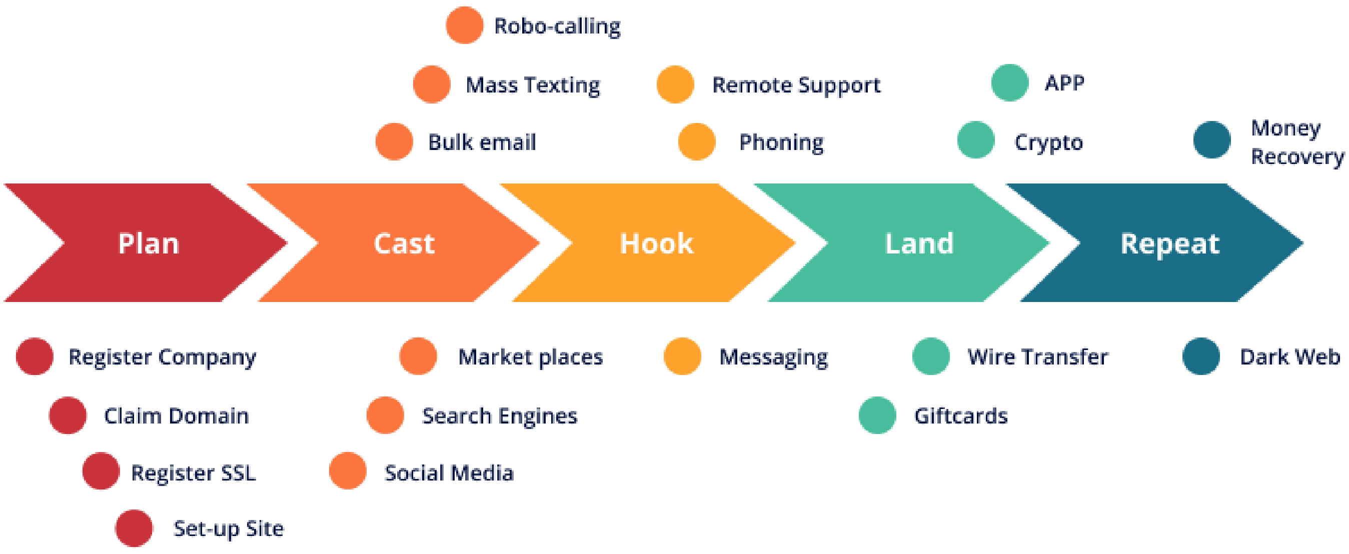


Figure 1: The Scam Journey - the steps a scammer may take to steal from consumers

[1] Further reading on the definition of a scam can be found in the book by Mark Button and Cassandra Cross “Cyber frauds, scams, and their victims” see: https://www.researchgate.net/publication/318041537_Cyber_Frauds_Scams_and_their_Victims

In several countries, new legislation is being considered to make banks liable for scams as they, in many unfortunate cases, affect the transfer of money from a victim to the scammer. While this is a positive development for consumers, the finger pointing for the massive rise in scams currently seems to be primarily directed at the banking sector alone.

Banks, while an important step, are only a small part of the “Scam Footprint”. Scammers need to be identified and combatted at each stage and not only at the final stage. There are several reasons for this:

→ **Alternative payment methods:** Banks are only one kind of payment alternative next to credit cards, PayPal, cryptocurrency, gift cards and other new payment methods on the rise. Scammers will just move to the weakest link.

→ **Banks cannot be all seeing:** As new technologies become available, and scammers become more professional it is unrealistic to expect banks to identify and stop all attacks unaided.

→ **Increase the scammers costs:** Scams can never be stopped completely. However, the cost to scam can be increased, making it a less attractive trade. This can only be done if all service providers raise the bar to counter misuse of their platforms.

It’s time to end the finger-pointing. Every company involved in the Scam Footprint needs to take responsibility for their own involvement.

2. Taking Responsibility: Scam Net Zero Across the Scam Footprint

2.1 The Concept

The first step in every improvement is to measure where you are. Based on the measurements, ideas for improvement can be defined, implemented and evaluated. It is proposed to introduce a self-governing model whereby each organization independently assesses their Scam Footprint.

A voluntary code to allow organizations to demonstrate how they are protecting consumers. It will also incentivize a more rigorous approach by all to gather information from victims to better measure the problem.

2.2 A Voluntary Approach is More Effective than New Regulations

A Voluntary Approach is More Effective than New Regulations

2.2.1 Regulation = Minimal Effort

Regulations often lead to a culture of minimum compliance, blame-shifting, and non-collaboration. This is where the beauty of the voluntary fraud-neutral model comes in.

2.2.2 From “Must Do” to “USP”

The Carbon Footprint used to be something for “nerds”. Now being “green” is a unique selling point.

Fraud neutrality operates on the principle of incentivizing companies to take up the mantle of responsibility rather than duress. Much like carbon neutrality, it’s a self-funded initiative that doesn’t create costs for society or governments.

Mirroring the adoption of the carbon net zero model, companies would claim a fraud-neutral status by taking more fraud out of the system than they allow into it. This would be verified by Fraud-net-zero accreditation agencies.

Companies can then promote their fraud-neutral status to their customers, investors, and stakeholders, creating a powerful brand reputation built on trust and safety. In essence, it changes the narrative from reactive denial to proactive verification.

The fraud net zero approach turns a societal issue into a brand strength.

The Carbon Footprint used to be something for “nerds”. Now being “green” is a unique selling point.

2.3 Scam Offsets: The Fraud Neutral Credit

In the future, the fraud neutral model could even allow companies to gain fraud-neutral credits, similar to carbon offsets. Organizations would measure the amount of fraud they have eliminated from the Scam Footprint and would receive offset credits for that. If a company has a bigger Scam footprint, they could invest in scam offset credits by donating to fraud-fighting initiatives. Fraud offsets foster an environment where corporate actions directly contribute to societal safety.

2.4 The Fraud Net Zero Model Creates More Informed Consumers

Consumer involvement is also pivotal to this approach. Currently only an estimated 7% of all scams are reported, to a large extent because the consumer believes that reporting a scam does not solve anything.

Consumers need to share when they were scammed and provide the details of their experiences. By reporting fraudulent attempts, consumers assist companies in identifying and shutting down scams at the earliest possible stage, creating a robust feedback loop that enhances fraud prevention.

7%

of all scams are reported, to a large extent because the consumer believes that reporting a scam does not solve anything.

Fraud offsets foster an environment where corporate actions directly contribute to societal safety.

3. Measuring the Scam Footprint

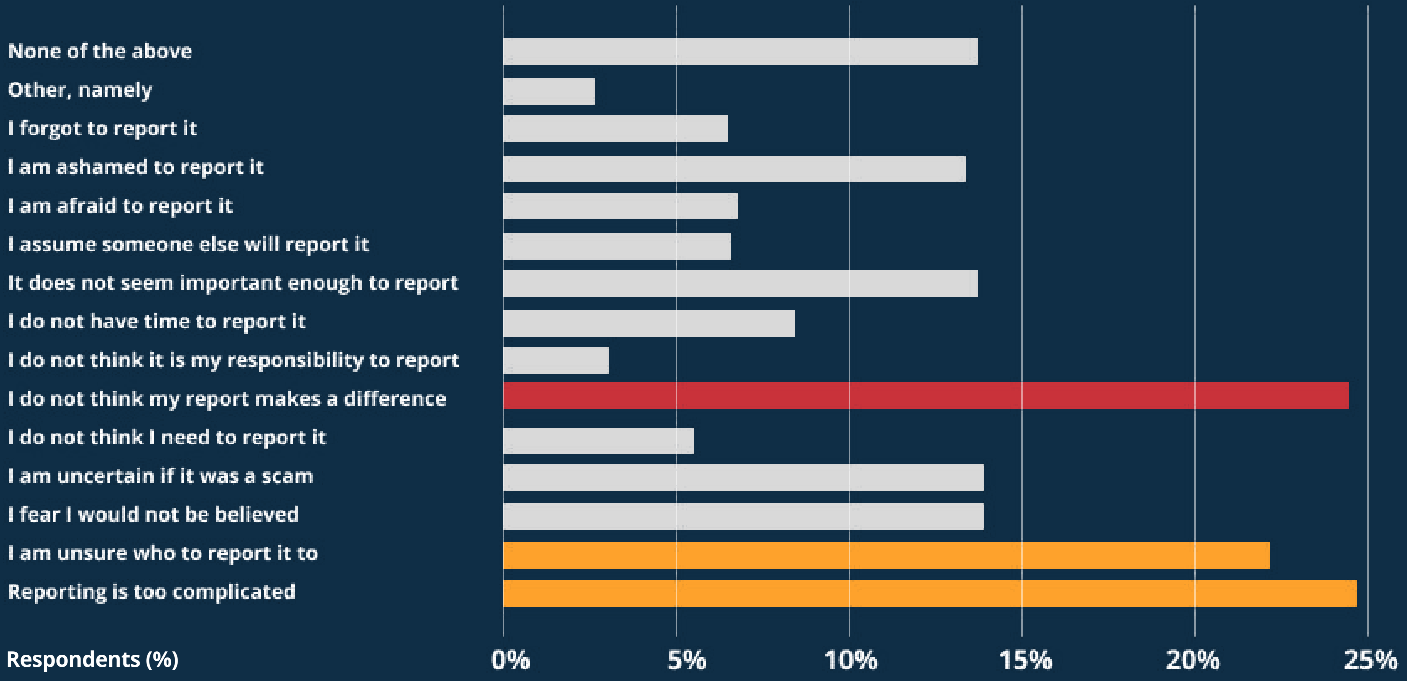
3.1 How Scams are Measured Today

Several organizations are already reporting on scams. Here are just a few:

- Australia National Anti-Scam Center – Scamwatch collects reports.
- Anti-Phishing Working Group (APWG) collects phishing reports.
- FBI Internet Crime Complaint Center (IC3) collects complaints.
- CIFAS: collects fraud intelligence.
- Spamhaus collects spam.
- ScamAdviser: collects scam domains.
- US Better Business Bureau: collects consumer complaints.
- UK Finance: collects fraud losses and measures consumer reimbursement.
- USA Federal Trade Commission: collects fraud reports.

The problem is clearly that measuring scams is made more difficult by each country, industry, and even organization having its own definitions and way to measure scams. Comparison across industries, let alone countries, is nearly impossible. The challenge is made greater by the reluctance of victims to report scams in the first place. See the chart below highlighting some of the reasons for this.

24% of participants believe reporting a scam would not make a difference



Other key reasons for not reporting are that reporting is perceived as too complicated (24%) and uncertainty where the scam should be reported (22%).

So, do we attempt to get a global standard that covers all industry sectors across the scam footprint (see 3.2) or do we take a phased approach by agreeing a standard within a particular country or industry sector (see 3.3)?

Even within a single institution there are sometimes challenges to standardized reporting as each country may need to comply with different regulatory requirements.

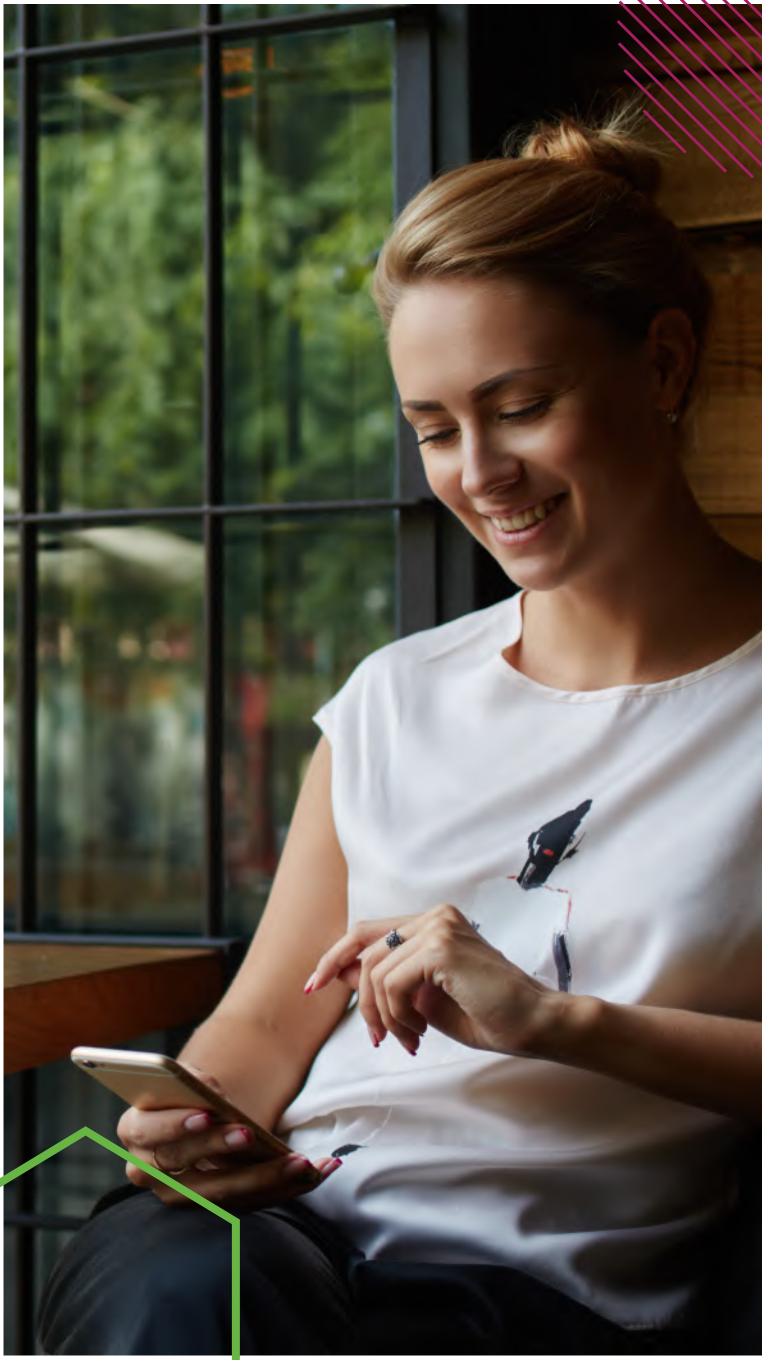
3.2 Option 1: Measuring Across the Scam Footprint by Service Abuse reported by Customer Complaints

The proposal is not to just measure fraud and scams specifically but instead measure abuse of services offered by the company. The reason for this is an operational one. Separating scams from other kinds of crime such as identity theft or phishing is difficult to do. To operationalize the measuring of the Scam Footprint we therefore propose using the term: Service Abuse.

Service Abuse is the misuse of services offered by a company with malicious intent, harming businesses and/or consumers (not necessarily the company itself).

Abuse differs by industry. In the world of Internet Service Providers (registries, registrars, hosters) abuse is often defined as the use of their services to spread malware, botnets and CSAM or execute phishing, pharming, spam, etcetera.

In the Social Media market Service Abuse is the use of the platform to spread hate speech, scams and spam, while in the Financial Services industry abuse can be defined as activities of money laundering, scams, identity theft, etcetera.



The kinds of abuse differ by industry. To make comparison across industries possible, abuse is defined as the number of complaints from external sources received by a company that their services are being misused.

Each company receives external communication, and these can in general be divided into general questions, questions/complaints about the company's services by a client or complaints about misuse of the company's services. The latter is Service Abuse.

Service Abuse is the Number of Complaints received from External Sources about Misuse of Services provided by the Company.

3.2.1 Measurement Rules

A few rules are set to measure Service Abuse in the same way across industries:

→ Reporting abuse has to be made easy: At a minimum with a link in the footer of the website, e.g., “Report Abuse”, linking to a form. Preferably reporters can also send an email directly to abuse@<company.domain>.

→ Each report counts as the same abuse reported by 10 different individuals, counts as 10 reports. Only the same abuse, reported by the same person, does not add to the total.

As with the Carbon Footprint, the idea is that an organization measures its own Scam Footprint, that is independently validated by an external accountant, agency or industry association.

3.2.2 Benchmarking Service Abuse

To compare the level of Service Abuse across companies in the same industry the following Key Performance Indicators (KPIs) are proposed:

- Abuse Level = Number of Abuse Reports / Number of Assets
- Abuse Resolution = Abuse Reports Resolved / Number of Abuse Reports
- The definition of Number of Assets differs per industry. A few suggestions:
- Social Media: number of active accounts (active = used in last 3 months)
- Registries/Registrars: number of domains managed.
- Hosters: number of active client accounts (accounts which pay a monthly fee)
- Banks: number of active bank accounts (active = used in last 3 months)

The definition of Abuse Reports Accepted & Resolved is the number of cases where the abuse reported has been blocked, stopped or removed annually. In short, the abuse is no longer present.

3.3 Option 2: Measuring Across a Single Sector Using A Standard Taxonomy for Fraud Reporting and Data/Intelligence Sharing – The Euro Banking Association (EBA)

3.3.1 Understanding what makes the victim take the bait: The EBA Fraud Taxonomy helps protect consumers against payment fraud

Money travels fast and fraudsters operate in real time. Fraud prevention and detection tools not only have to be fast but should also be able to follow fraud across borders and allow relevant parties to join forces in fighting it. To support collaborative efforts in this area, the Euro Banking Association (EBA), a practitioners' body for banks and other service providers supporting a pan-European vision for payments, created the EBA Fraud Taxonomy, a common pan-European vocabulary for fraud categorization.

The taxonomy was developed by fraud experts from banks across Europe. The aim is to equip fraud experts with one set of terminology and a uniform pan-European approach to categorizing fraud cases. A common taxonomy is seen as a key prerequisite for sharing fraud intelligence or data among payment service providers for fraud prevention and detection purposes. Since no such pan-European vocabulary and approach existed, fraud experts from 15 European countries set out to develop these under the umbrella of the EBA.

15

European countries set out to develop these under the umbrella of the EBA.

3.3.2 A standardized approach for fraud classification is essential for more cooperation in the fight against payment fraud

The EBA Fraud Taxonomy provides a simplified and straightforward framework to capture and categorize fraud scenarios related to all kinds of payments, including card transactions. It offers a standardized way to identify who initiated the payment transaction affected by the fraud, how the fraudster first contacted the victim and what trick the fraudster used to get hold of the victim's money or credentials. At the same time, so-called labels or tags allow fraud experts to add further details on a fraudulent event, as they deem fit, for example to align with internal reporting requirements. This ensures ease of use, maximum flexibility and a smooth transition from any legacy taxonomy to this pan-European taxonomy.

The EBA Fraud Taxonomy also leverages existing fraud-combatting vocabulary by relying on definitions from authoritative and publicly available sources, wherever possible.

To highlight how the EBA Fraud Taxonomy works in practice, let's look at a fraud scenario that has gained in popularity across Europe due to the ongoing energy crisis and which experts have labeled as the firewood or wood pellet scam:

Who? How? What? What else?

From fraud case to fraud type

Who?

Initiator of payment transaction: **customer**

How?

Method: **Fake merchant**

"Fake merchant websites offering non-existing goods... to make the victim initiate a payment transaction."

Fraud case description

Consumer orders firewood or pellets online, pays upfront but never receives the wood/pellets

What else?

Label/tag: **Goods not received**

Potential dedicated label 'defined by a PSP: Firewood / wood pellet scam

What?

High-level classification:
"I am a seller/buyer"
Modus: **Online shopping fraud**
"Shopping and auction fraud involves fraudulent shopping scams that rely on the anonymity of the internet."

Source: National Fraud & Cyber Crime Reporting Centre in UK 'Online shopping fraud'

Delineating the who, how, what, what else elements allows us to describe any fraudulent event in a very brief and precise manner. It also empowers the users of the taxonomy to speed up the tracking of fraudulent transactions and capture more granular data required to develop effective countermeasures. The standardized approach to fraud classification provided with the taxonomy also ensures that any fraud trend intelligence and data is both accurate and easy to compare.

As a result, the taxonomy is increasingly recognized as a key enabler for more cooperation in the fight against payment fraud across the European payments ecosystem. Early adopters unanimously confirm that the taxonomy is an important asset for their journey towards sharing intelligence or data for fraud prevention and detection purposes.

The EBA Fraud Taxonomy is available via the EBA website.

3.3.3 Developing better ways to educate and alert consumers across industries

A unique feature of the taxonomy – or a "revolutionary approach", as one pilot adopter observed – is that it separates the contact methods used by fraudsters from the actual tricks they apply. In addition, the taxonomy describes key strategies and emotional triggers deployed by fraudsters with a view to making the victim take the bait, i.e. engage with the fraudster in the first place. This has allowed institutions that have already implemented the taxonomy to develop effective fraud prevention campaigns for their customers.

The taxonomy could also support other industries to pinpoint where action is needed and support their efforts to educate consumers about the prevalent methods applied by fraudsters to contact them and the tricks they play to get hold of their money or credentials

3.3.4 Clarifying the regulatory requirements applicable to the sharing of fraud intelligence

Today, the sharing of intelligence and data for fraud combatting purposes among PSPs is still hampered by diverging regulations and regulatory interpretation related to data privacy and, most importantly, banking secrecy – but emerging regulation, such as the Instant Payments Regulation or the Payment Services Regulation, will change this. These future regulations are expected to pave the way for a wide range of new cooperative initiatives, such as the sharing of elements related to mule accounts, which will take fraud-fighting efforts in Europe to a new level. To be able to reap these benefits, fraud experts should get ready – aligning their vocabulary with the help of the EBA Fraud Taxonomy is one big milestone on that journey.

4. Moving from Measurement to Reduction

Whichever approach is adopted, measurement makes it possible to identify opportunities to prevent consumer abuse and create a continuous cycle of improvement. It facilitates benchmarking with peers to identify where action is needed and where the company is doing better than the market average.

Of course, measurement is only a first step. Many other improvements need to be made to combat scams. A few ideas:

4.1 Set Industry standards

Define which abuse levels are acceptable within the Industry and where action becomes mandatory or penalties are set if abuse levels increase above the norm.

4.2 Standardize reporting

And associated metadata of the abuse across the Scam Footprint to allow real time exchange of data.

4.3 Automate counter abuse measures

Agree upon automated actions to be taken on the abuse if proper proof of abuse is provided. This allows an abuse identified at any stage to be automatically communicated to other stakeholders, who can take down websites, freeze accounts, or block messages in real time.

4.4 Develop scam prevention strategies

Each sector would devise comprehensive scam prevention strategies that include technology, processes, and collaborations. These strategies should focus on proactive measures to detect and prevent fraud, as well as mitigation plans to minimize the impact when it occurs.

4.5 Implement scam detection technologies

Sectors would invest in advanced scam detection technologies, such as artificial intelligence, machine learning, and data analytics. These technologies would enable the identification of fraudulent activities, patterns, and anomalies across their respective platforms.

4.6 Share best practices and collaboration

Sectors would collaborate and share best practices to enhance scam prevention efforts. This could involve regular meetings, workshops, and information sharing platforms to exchange knowledge, insights, and emerging trends. Additionally, collaborations with law enforcement agencies and regulatory bodies would strengthen the overall response to fraud.

4.7 Establish reporting and accountability mechanisms

Sectors would implement reporting mechanisms for scam incidents and establish accountability measures. This includes transparent reporting, implementing clear procedures for reporting incidents, and holding accountable individuals or organizations responsible for enabling or facilitating fraudulent activities.

4.8 Customer education and awareness

Each sector would devise comprehensive scam prevention strategies that include technology, processes, and collaborations. These strategies should focus on proactive measures to detect and prevent fraud, as well as mitigation plans to minimize the impact when it occurs.

4.9 Regulatory support and standards

Governments and regulatory bodies would play a crucial role in supporting scam prevention efforts across sectors. They would establish regulatory frameworks, guidelines, and standards to ensure consistent and effective prevention strategies. Regular audits and assessments would help monitor compliance and identify areas for improvement.

4.10 Continuous improvement and adaptation

Similar to the net-zero challenge model, scam prevention efforts would need to be continuously improved and adapted to address evolving techniques and emerging risks. Regular evaluations, feedback loops, and technological advancements would help refine strategies and stay ahead of fraudsters.

In short, only with standardized measurement can we start to turn the tide on scams.

5. Next Steps towards Fraud Net Zero

To build towards global adoption of taking responsibility for the scam footprint the following steps need to be taken:

5.1 Involve Industry Associations

The involvement of ICANN (registries, registrars), the banking industry, the hosting community, telcos and social media is essential to fine tune the Footprint per sector.

5.2 Set-up a Scam Footprint Organization

Supporting industry bodies and key stakeholders should establish an independent organization or use an existing one to manage the Scam Footprint. Its key tasks would be to protect the standards set, promote the use of the Scam Footprint amongst industry associations and key players and annually report on the program and progress towards a Fraud Net Zero infrastructure.

5.3 Finalize Measurement Standards

Per industry the measurement standards must be defined and communicated.

5.4 Assign Neutral Auditors

To support organizations in each industry in measuring their Scam Footprint, independent auditors like PwC, EY, KPMG, etc. have to be involved, trained and guided.

5.5 Launch the Scam Footprint

Not all sectors will be able to introduce the Scam Footprint at the same time. The financial sector seems the furthest ahead and would be a logical first industry to launch the methodology. Other sectors can follow as soon as standard measurement criteria have been set.

5.6 Publish The Annual Scam Footprint

The goal of this annual publication is to report on the progress towards a Fraud Net Zero society by publishing industry wide data and highlighting best practices.

6. The Scam Footprint Sector by Sector

As part of this consultation and aligned with the Fraud Net Zero concept, we are seeking contributions from individual organizations to state how they are addressing the problem of protecting consumers. Specifically:

1. Measuring the scam footprint.
2. What is already being done to prevent scams.
3. Future plans to protect consumers.
4. Help that is needed from other sectors.

The contributions will be collated and included in the next version of this paper. Alternatively, please feel free to submit questions or comments on this paper here: https://www.gasa.org/contact

Below are the views of the presenters invited to speak at the Scam Footprint workshop held at the annual GASA Summit in Lisbon on 18th October 2023.

6.1 Playing Devil's Advocate – How Online Platforms Benefit from Fraudsters, an Academic Perspective – Jack Whittaker

6.1.1 Introduction

The growth of online platforms and technology in the past twenty years has created numerous opportunities for fraudsters. They now initiate fraud on e-commerce and dating platforms rather than in the physical world. In addition, we have also seen the creation of a whole new marketplace of 'fraud-as-a-service' products, such as the opportunity to bulk-buy fake reviews on e-commerce platforms or on-demand bank (mule) accounts used in laundering the stolen funds of victims exploited on social media websites.

This raises the question:
"Should we care that technology is used in the perpetration of fraud?"

On the one hand, proponents of the instrumentalism perspective of technology argue that no, we shouldn't care. Technology under this perspective is viewed as being neither good nor evil and it should not be regulated. The implication being that technology does not have a role to play in determining fraud liability.

On the other hand, technology can be viewed through the lens of extension theory which argues that it extends human capabilities by providing new opportunities beyond what was possible. Therefore, regulation and measurement are necessary because technology amplifies the modern fraudster's capabilities.

Extension theory can also be useful in explaining the growth in fraud victimization on online platforms. Marshall McLuhan, in his influential book 'Understanding Media', argues that technology can also result in 'amputations' of various kinds. In the context of 'cyberspace', users arguably sacrifice their mental faculties like concentration or memory in favor of convenience, speed, and new interactions inside the digital environment. This can increase the chance of fraud since consumers rely on trust in the sellers rather than inspecting products physically.

Additionally, many online platforms lack 'know your customer' (KYC) processes, often to attract as many users as possible, especially when operating a freemium business model. In the case of many online dating platforms, for example, one can merely sign up for a free account without any formal checking procedures.

Additionally, one can argue that platforms can benefit from fraudsters operating on them in three ways:

1

To inflate user figures. For example, after the Ashley Madison data breach in 2015, it was discovered that nearly every female profile was either fake or dormant and was retained solely to lure men onto the platform.

2

To generate income. A key component of the online fraud economy is that fraudsters need to spend money to make money.

An example of this is how many fraudulent e-commerce websites reinvest their previous victim's stolen funds into search engine advertising campaigns as a means of attracting traffic to their website.

3

To decrease cost. It is simply easier and cheaper for platforms to ignore instances of fraud by not training a well-resourced abuse department.

In summary, there is a historical relationship between technology and fraud, two opposing viewpoints argue whether technology is or is not capable of harm, and lastly, that platforms can in fact benefit from fraudsters operating on them parasitically. In the longer term, a suggestion is that 'know your customer' verifications should be a mandated part of any online platform's business model. It is simply not enough for platforms to play whack-a-mole with fraudsters by taking down some fraudulent content only for it to appear again later.

6.2. An eCommerce Perspective – Amazon

6.2.1 Introduction

Amazon is committed to being the Earth's most customer-centric company. So, if these scams are happening to customers, Amazon cares. Scammers, apart from communicating through various channels, are monetizing through them making everyone susceptible to it. The new digital age is driving the rise of a new generation of victims.

Additionally, many online platforms lack 'know your customer' (KYC) processes, often to attract as many users as possible, especially when operating a freemium business model. In the case of many online dating platforms, for example, one can merely sign up for a free account without any formal checking procedures.

6.2.2 Scam Measurement

There is a challenge regarding nomenclature, language shifts, and taxonomy that makes it difficult from the outset for anyone cross-industry approach to defining the scam footprint. A universally adopted taxonomy would help classify scams and enable concerted action. Every day there's a new scam popping up and there are many different monetization techniques, which makes it complex.

6.2.3 What is Already Being Done

Behind the scenes, over 15,000 people worldwide work to protect Amazon from fraud and abuse. Some of the enforcement actions pursued are working with law enforcement to do criminal referrals, takedowns, business disruption actions, and cease and desist orders.

Last year, Amazon shut down over 20 000 phishing websites, 10 000 phone numbers, and referred over 100 bad actors worldwide.

Amazon stands against impersonation scams. The idea of just picking a trusted name, finding a convincing way to capture someone who bites, and then exploit them until the money runs out. Over 50% of scams are some form of impersonation, and our work is trying to prevent it. We try to prevent scams in three ways:

1. By going after the bad actors.
2. By employing techniques to ensure customers know that it's the genuine Amazon they are dealing with such as authenticated communication.
3. Educating consumers that knowledge of scamming techniques is important.

However, we can't enforce our way out of this challenge, so we have different solutions in our store to help customers know if communication is authentic.

One of them is through our message center. Customers can go there and check all communication from Amazon or check their order history. Another way is through email verification, if you see an Amazon logo accompanied by amazon.com on the e-mail address, you can feel confident of its authenticity.

We work closely with different partners, including an information campaign in the US with the Better Business Bureau. We were proactive in our communication to spread valuable information regarding scams and communicating with customers through emails to flag some of the tips and trends we're finding.

6.2.4 Future Plans

We are now working with organizations in varying capacities. In some ways, it's part of a broader network of scam fighters like the Global Anti Scam Alliance or working on developing tools and resources to address shared concerns and opportunities regarding consumer pain points, like the Better Business Bureau. Amazon will continue to develop a Victim Support toolkit that's very comprehensive.

6.2.5 Help that is Needed from Other Sectors

There are, also, a number of challenges that Amazon would like to see addressed, namely:

- **Timely alerts** - we've launched the Scam Trends Alert System, but these need to be communicated faster.
- **Victim Support** - It's not just money or your ID. It's the emotional impact of these crimes that needs to be supported.
- **Reporting** - we rely on self-reported data. More data-sharing would help.
- **An increase in ease of information** - between setting standards of the taxonomy, and the type of data, between industries, organizations, and jurisdictions.
- **Work with others** - establish and share best practices of communication with consumers.

Taking the guesswork out of it for consumers leaves no room for questioning as to whether a communication is authentic. And we would love to work with other organizations who want to set those standards moving forward.

6.3 A Social Media Perspective – Meta and DNS Research Federation

6.3.1 Introduction

Meta Inc., as one of the largest social media, chat, and application providers, faces a large number of scams. Criminals use our brand to attract the public and the platform to manipulate unwitting users into dangerous traps. Meta has provided seed funding for the establishment of the Domain Name Research Federation (DNRF), a UK not-for-profit research company that addresses the impact of the domain name system on cybersecurity, policy, and technical standards.

Improving the cybersecurity of domain names and other unique identifiers is a key part of tackling scam abuse. Research in this area shows that victims use 'selective scrutiny' as they are bombarded with a plethora of information contained in websites, emails, and text messages to decide whether the content is good or bad. Unwitting users who are scammed typically follow the false signals of reassurances presented in fake domains or the misuse of popular brands.

6.3.2 Scam Measurement

There is no single, universally agreed definition or form of measurement for domain name-based scams. An effective response to it implies extending cooperation beyond the domain name industry to include content and hosting providers, DNS routing, and email providers.

6.3.3 What is Already Being Done

DNRF is working with stakeholders across the sector to close the governance gaps and foster inter-sectoral cooperation to reduce scams. It maintains many domain and URL-based blacklists for network operators and public safety officials to address any sort of abuse. This platform holds unique data sources and continues adding more feeds, providing normalized data through API and web services. By making data available, working with others to highlight divergent approaches in definitions and measurement, and publishing quantitative, evidence-based studies, the DNRF is contributing to scam measurement.

DNRF is working with numerous partners including Meta, GASA, and the Motion Picture Association at Oxford University, as well as government departments. Project-based funding has been obtained from the Internet Society Foundation. Our research is supported by distinguished advisors. Relevant measurement projects include:

- → DAP.LIVE - data sharing platform, comprising 70+ data feeds
- → Consumer research on scam volumes and its impact on the emotional side;
- → Habits of excellence: why are EU ccTLD abuse rates so low?
- → Development of open source tools to measure DNS resolver capability will help to identify adoption rates of security protocols such as DNSSEC and DMARC
- → Blog series by Alex Deacon on the intersection between scams, cybersecurity, and brand protection
- → RPKI uptake in the ARIN region;
- → Web3 disruption and governance gaps in alternative naming systems

6.3.4 Future Plans

Future plans include but are not limited to:

→ A better understanding of NIS2 and modeling cost-effective ways of identity verification mechanisms such as electronic identification (eID) and know your customer (KYC)

→ Researching ways to reward domain name registrars for improving the quality of WHOIS data, and improve the timeliness of disclosure to public safety and brand protection through better electronic services.

→ Providing quicker access to WHOIS data through electronic tools.

→ Closing governance gaps within the DNS, hosting, sub-domain provider, and proxy ecosystems.

6.3.4 Help that is Needed from Other Sectors

We are seeking donations from organizations and individuals, and those willing to share data, for all the projects above, through:

→ Research projects

→ Donations

→ Partnerships

→ Sponsoring events

→ Using DNRF DAP to research scams and abuse.

6.4 A Government Perspective – UK Home Office

6.4.1 Introduction

On 3 May 2023, the UK Government published the UK Fraud Strategy, which sets out 52 actions which capture the UK's whole-of-system response to tackling fraud across 3 pillars:

1. Pursue fraudsters, disrupting their activities and bringing them to justice more often and quicker.
2. Block frauds at source by dramatically reducing the number of fraud and scam communications that get through to the public.
3. Empower the British people to recognize, avoid and report frauds and equip them to deal easily and appropriately with frauds that do get through.

In this Strategy, the UK government noted that criminal techniques are becoming ever more sophisticated, making it close to impossible for consumers to routinely and confidently detect fraudulent communications across online and telecommunications platforms. The Strategy therefore puts great emphasis on public-private partnerships. Additionally, the Fraud Strategy sets out legislative and regulatory measures to structure industry incentives to prevent fraud and disrupt enablers of fraud.

> *UK government noted that criminal techniques are becoming ever more sophisticated*

6.4.2 Scam Measurement

The UK uses the world-leading Crime Survey of England and Wales (CSEW) to measure crime prevalence in society, including the scale and volume of fraud. Additionally, the UK Home Office has made an estimate of the cost of consumer fraud in Annex 3 of the Fraud Strategy.

However, due to the diverse nature of the counter-fraud sector, the inherent nature of fraud as a crime of deception and the rapid hydra-like adaptation by threat actors, it remains difficult to effectively detect impact of specific counter-fraud measures. Sometimes it is not easy to make an accurate analysis since there are multiple variables that cannot simply be added together.

> *...the UK Home Office has made an estimate of the cost of consumer fraud in Annex 3 of the Fraud Strategy.*

6.5 A Bank Perspective – Dutch Banking Association

6.5.1 Introduction

Banks are clearly heavily involved in various activities, with a large impact on prevention, awareness, and the implementation of technical measures. In the Netherlands, three factors have contributed to the banks' success:

1. A campaign launched last year.
2. A specific technical measure.
3. Partnerships.

6.5.2 Scam Measurement

See below.

6.5.3 What is Already Being Done

The campaign was named 'Scamming'. It was based on our research which showed that, despite consumers being aware of scams and the dimension of the problem, they don't think becoming a victim is a possibility, and that's the biggest challenge regarding prevention campaigns. So, we chose a different tactic - to write a storyline from the perspective of the scammer in order to help consumers understand how it works. It has proven to be effective since if people know how it is done, they can recognize and prevent it.

The second technical measure was successfully implemented in Dutch banks. It consisted of setting low transaction limits, with ranges between $2,000 to $ 5,000. However, they allow consumers to increase, temporarily, these limits for larger purchases, but with a four-hour waiting period.

This delay has been proven to be effective in thwarting scammers, as it disrupts criminal attempts to rush victims into transferring money. This practice helps consumers reconsider whether transactions are legitimate, or not. Additionally, those who want to have a higher limit, such as $10,000, will face an increased waiting period.

$10K

those who want to have a higher limit, (...) will face an increased waiting period.

The third measure we have introduced is a public-private partnership called the integrated approach. All companies, and private partners within the scam chain are welcome to participate, but also consumer organizations and tech companies.

One of the most important tracks for banks is intervention. What is being done is writing a criminal journey to follow all the different steps a criminal takes.

Starting with bank employee impersonation scams and then, talk with all the partners in the scam chain about what intervention can be done.

6.5.4 Future Plans

Partners in the model have the flexibility to select and implement different interventions. Furthermore, partnerships with an advisor for the Electronic Crimes Task Force, known as ECTF, involving the police, banks, public prosecutors, and workers engage in both research and exchanging models.

6.5.5 Help that is Needed from Other Sectors

In the Netherlands, authoritative data is required and for it to be effective in fighting fraud, legislation is needed as it enables the sharing of data, that is where the government can help as well as Europe as a whole.

6.6 A Bank Perspective – Grupo Santander

6.6.1 Introduction

At Santander, having a customer-centric mindset along with a defined business strategy is key to success. Protecting its systems, information and clients is a top priority for the Group and a crucial component of the Santander's goal to 'help people and businesses prosper'.

6.6.2 Scam Measurement

To better understand nuances between different fraud and scams, establishing a clear taxonomy is fundamental to understand the threat landscape.

6.6.3 What is Already Being Done

Something that has been proven to be effective is a combination of bringing together awareness and technology. This approach relies on having a strong transaction and monitoring capacity based on machine learning, AI, and behavioral biometrics. This intelligence is used by our business and service channels to help support customers. For example, Santander UK introduces specific questions in digital journeys to help customers take an informed decision during critical purchases or transfers.

6.6.4 Future Plans

Santander has a program in place to combat fraudulent activities. New technologies are making it possible to disrupt scams and fraud campaigns at critical points so that they are not successful. Also, investing more in intelligence can help identify the malicious activity and act quickly against them.

6.6.5 Help that is Needed from Other Sectors

Building and enhancing our intelligence and information-sharing relationships, within the industry and with the public sector, is crucial. By joining forces and creating concrete channels for information-sharing and tactical collaboration, we can make a decisive shift in the fight against cybercrime.

6.7 A Remote Access Software Perspective – AnyDesk

6.7.1 Introduction

Anydesk is remote access software commonly used by genuine IT teams. It is regarded as an attack vector for fraud because it is directly installed on a victim's computer and is also used by scam centers globally.

6.7.2 Scam Measurement

As an experiment, we held an event named 'Scammer Payback' where the whole office was turned into an anti-scam call center aiming to farm information from the scammers. From that action, money mule addresses and accounts were caught and saved over $200,000 for victims.

This approach is unique because Anydesk is sometimes restricted by law to what data it can access from our customer installations.

$200K

money mule addresses and accounts were caught and saved over $200,000 for victims.

6.7.3 What is Already Being Done

Some progress has been made, however, without breaking any law. For example, whenever a mule account is detected, some banks in the United States shut it down within minutes, meaning that the scammer does not have time to liberate the funds and therefore make it possible to reimburse victims.

Communication is key as is a fast response. In the past, Anydesk was used because privacy was protected and this hindered the detection of frauds and scams. To overcome this, a collaboration with some private scam interceptors has played a big role. During two weeks, more than 2000 scammers were blocked from using Anydesk software. This is not just an inconvenience for scammers. They not only have to find alternative mechanisms but also cause concerns in their minds, making them believe someone is coming for them and thereby preventing a possible return.

6.7.4 Future Plans

An ongoing action is shutting down Text Now, a provider frequently used by scammers. Anydesk collaborated with a representative from the platform to accomplish this goal.

The focus of scambaiting has shifted from mere pranks to a more impactful approach. After engaging with scammers, the caller gathers information to report and eventually shuts down their operations. By leveraging this process, creating a communications platform that enables protection for the customers and ensures scammers face justice is a must. That way not only is harm being prevented but also creates a stance in safeguarding individuals from falling into these schemes.

> *That way not only is harm being prevented but also creates a stance in safeguarding individuals from falling into these schemes.*

Whenever a scam interceptor reports a victim, for example, it allows Anydesk to access the network and shut down multiple scams in progress. Nowadays, there are many techniques that make it a tough challenge to understand the authenticity of certain calls. For example, today some scammers even pretend to be victims, accusing the genuine victims of being a scammer in order to obtain information. It is important to work with individuals as much as associations since they have valuable pieces of information that are helpful.

Knowing this, a natural question that must be asked is: "When is the right time to intervene in a scam?" The best answer might be mid-scam because it's not only about following the money trail but also about saving people from being scammed and ensuring that the criminals are facing the consequences of their actions.

6.7.5 Help that is Needed from Other Sectors

One thing companies can do to help this cause is to share data within a single platform where anyone can access and communicate effectively because it's the only way to put an end to this fight.

6.8 A DNS Perspective – DNS Abuse Institute

6.8.1 Introduction

The DNS Abuse Institute ("the Institute") focuses on initiatives to help reduce domain name server (DNS) abuse by fostering collaboration, creating best practices, and developing open, industry-shared solutions provided at no cost. DNS Abuse is defined as malware, botnets, phishing, pharming, and spam when used as a delivery mechanism. The Institute was created in 2021 by the Public Interest Registry, the registry operator for the .ORG top-level domain, in furtherance of its non-profit mission.

6.8.2 Scam Measurement

To the extent that phishing and malware overlap with scams that involve a domain name, some scams are measured through the Institute's measurement initiative: DNSAI Compass ("Compass"). Compass was launched to increase the quality of information about the prevalence and persistence of DNS Abuse within the domain registration industry. Compass seeks to measure DNS Abuse in a robust and transparent way, and to use that information to drive abuse reduction activities. Compass measures the number of unique domain names used for phishing and malware distribution, whether the harm has been mitigated, and the speed of mitigation. It also indicates whether the domain name was registered for the purpose of phishing or malware (malicious) or has been compromised (a benign domain name that has been compromised at the website, hosting, or DNS level). See our website for interactive charts, monthly reports, and a full methodology:
https://dnsabuseinstitute.org/dnsai-compass/

6.8.3 What is Already Being Done

To improve reporting and mitigation of harm, the Institute runs NetBeacon (https://netbeacon.org/), a free centralized abuse reporting service that automatically routes reports of phishing, malware, botnets, and spam to the relevant registrar. NetBeacon aims is to improve the quality of reports that registrars receive by making sure they are evidenced and standardized, while simultaneously making reporting easier and simpler for people who encounter DNS abuse to report it. NetBeacon was launched in June 2022 and is free to use.

6.8.4 Future Plans

The Institute will continue to pursue its mission to reduce DNS Abuse through education, collaboration, and innovation. We welcome feedback as we continue to optimize and improve our existing initiatives.

NetBeacon aims is to improve the quality of reports that registrars receive (...)

6.8.5 Help that is Needed from Other Sectors

Reports of abuse online: If you encounter scams and have evidence, please submit reports of malware, botnets, phishing, pharming, and spam to NetBeacon: https://netbeacon.org/

Feedback: If you would like to learn more about how much is the prevalence and persistence of phishing and malware, please see our Compass reports and provide us with feedback. https://dnsabuseinstitute.org/dnsai-compass/ or contact us at: Info@dnsabuseinstitute.org

6.9 A Telco Perspective

Unfortunately, we have yet to receive a contribution from a telecom provider. These organizations are seen to play a critical role in the scam footprint and we therefore would sincerely welcome a contribution from either a national or multinational provider.

7. Conclusion and Next Steps

7.1 Summary

The digital landscape is continuously evolving, bringing with it the increasing complexity of online scams. Authored with the collective insights of industry experts, this whitepaper sheds light on the multifaceted nature of online scams and underscores the urgent need for a unified approach to tackling this global challenge.

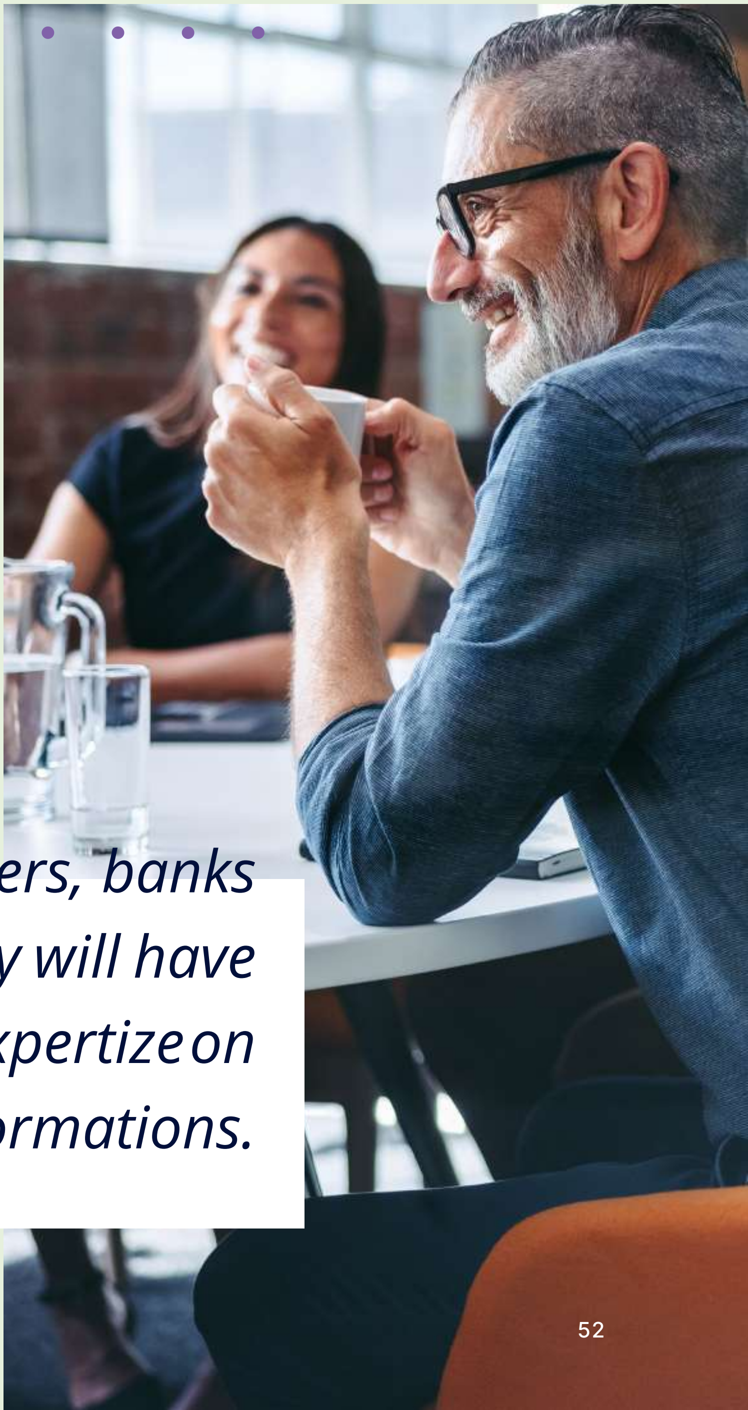
The responsibility of mitigating the impact of scams extends beyond individual entities to encompass a collective effort across various sectors. Service providers, especially in the banking and financial sectors, are positioned at the forefront of this battle, holding a pivotal role in safeguarding consumer trust and financial security. It is imperative that these institutions not only recognize their part in the scam ecosystem but also actively engage in strategies to diminish their scam footprint.

Measuring the scam footprint is critical to understanding and combating online fraud. This whitepaper introduces the innovative concept of Scam Net Zero, advocating for a voluntary, proactive stance that encourages organizations to self-assess and minimize their involvement in scams. This approach mirrors the successful models used in environmental sustainability and is poised to transform how businesses view and tackle the issue of online scams.

The insights gathered from diverse sectors, including e-commerce platforms like Amazon, social media giants like Meta, governmental bodies, and various banking institutions, reveal a common thread: the necessity for collaborative efforts. This unity not only fosters shared knowledge and strategies, it amplifies the effectiveness of scam prevention measures.

In conclusion, our journey through this whitepaper leads us to a compelling call to action: for organizations to step forward and actively participate in shaping a scam-resistant digital world. This involves continuous adaptation, rigorous measurement, and a shared commitment to innovation in scam prevention strategies. By doing so, we protect our individual interests and contribute significantly to the integrity and trustworthiness of the global digital economy.

As we move forward, it is our collective responsibility to embrace these challenges and opportunities, working synergistically towards a future where the digital landscape is thriving and secure for all its participants.



Working with the right partners, banks can have confidence that they will have experience, knowledge, and expertize on their side during their transformations.

7.2 Proposed actions

1

Get input from any national regulator on what is being done to provide the framework for cross-industry collaboration on defining and addressing the scam footprint for the benefit of consumers.

2

Seek input from a telecoms provider on the role telco plays in the scam footprint and how they are helping to protect consumers.

3

All social media, dating, and other such platforms to implement a basic Know Your Customer (KYC) program in order to reduce their scam footprint and liability share.

4

A universally adopted taxonomy would help classify scams and enable concerted action.

All industries to consider the EBA's fraud taxonomy and comment on its applicability for their sector.

5

More effective mechanisms for building consumer trust by reducing uncertainty and ensuring there is no room for questioning as to whether a communication is authentic.

6

Banks to consider, as per Dutch banks, a simple technical measure to set low transaction limits, with ranges between $2,000 to $5,000. Consumers can also temporarily increase these limits for larger purchases but with a four-hour delay.

7

Does this Scam Footprint initiative need funding and if so, who should fund it.

8

Hold a follow-up session on the scam footprint in Q1 2024.

7.3 Get Involved!

Anyone is welcome to comment on the ideas shared in this paper. Alternatively, we are happy to add contributions from any organization that is helping to address the scam problem.

Contributions or comments, for inclusion in the next version of this paper, can be submitted here: https://www.gasa.org/contact

feedzai.com info@feedzai.com sales@feedzai.com