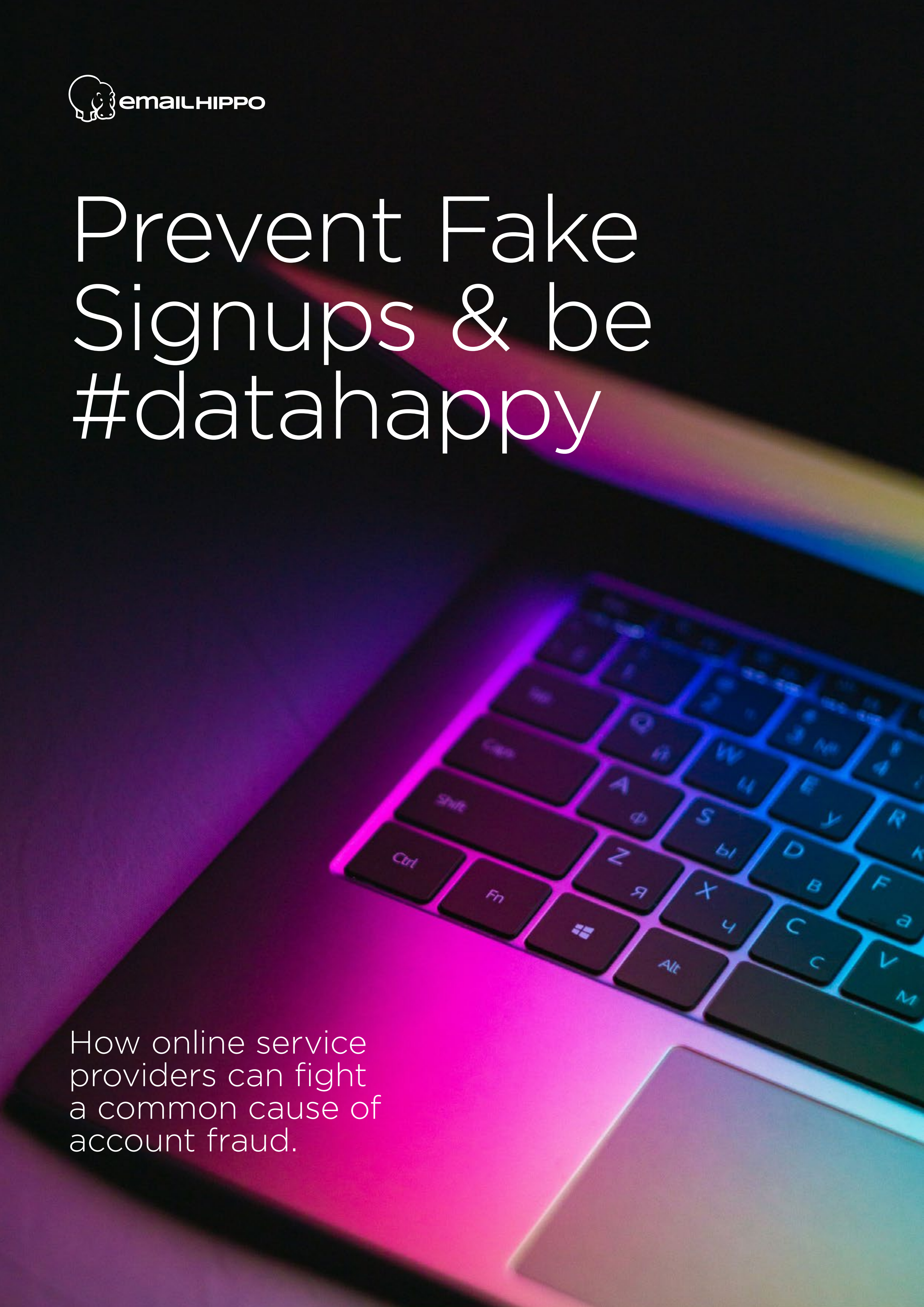
emailHIPPO

Prevent Fake Signups & be #datahappy



How online service providers can fight a common cause of account fraud.

Introduction

Anyone who runs a business online is at risk of fraudulent activity, from smaller-scale instances like friendly-fire (fraudsters attempting to 'try their luck' and get your products or services for free) to much larger cases like cyberbot attacks and data breaches.

According to *gov.uk, around 20% of UK businesses have been victim of at least one cyber crime in the past year, with increased risks for larger companies. The most common attacks being phishing scams.

Even so-called 'friendly fraud' can have a negative impact on your business. **40% of people who commit friendly fraud by charging back for goods and services they have purchased online say they would do it again within 60 days, signalling financial implications for online businesses.

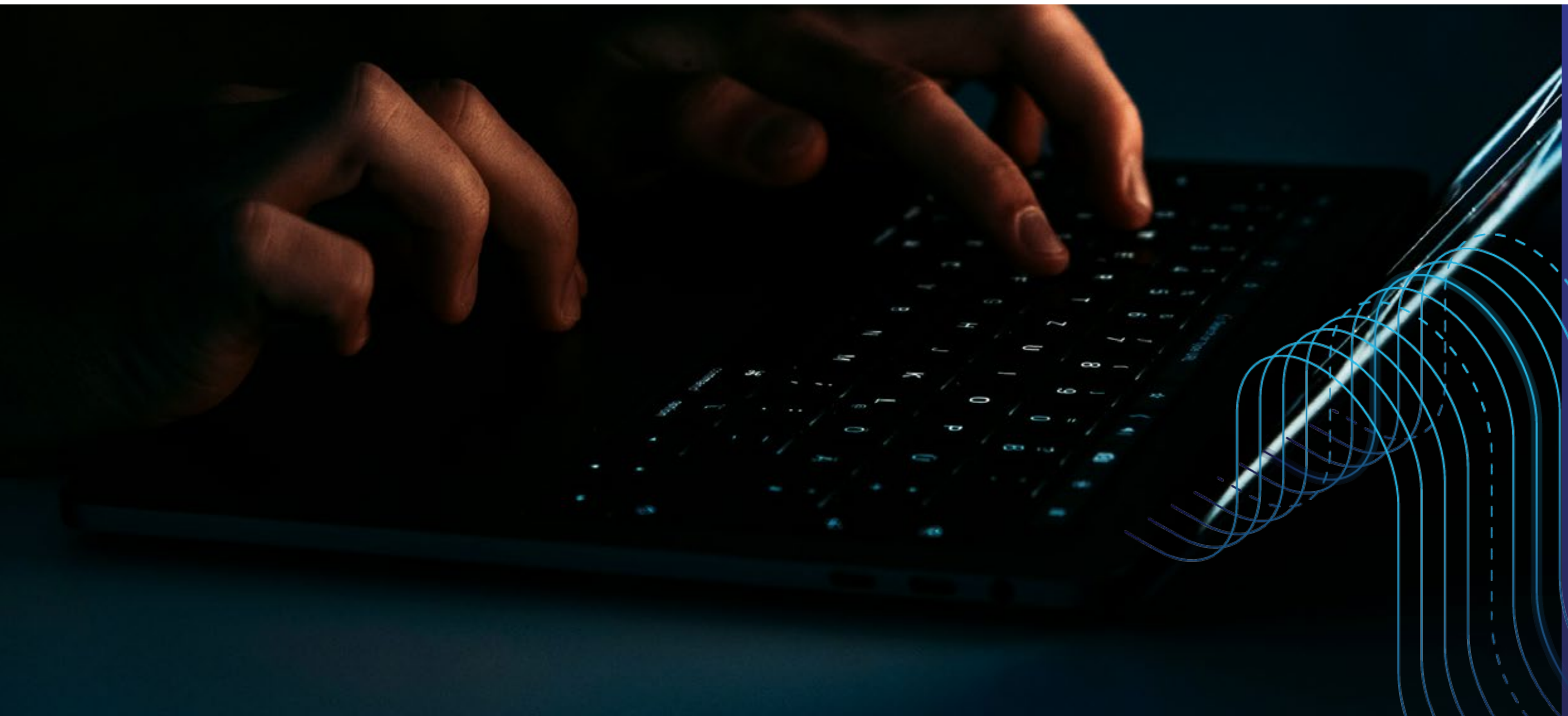
One of the most common tactics used by fraudsters is account fraud: the use of fake or stolen information to pose as a legitimate user of an online product or service. Over *£1.17 billion in the UK alone was stolen through unauthorised and authorised fraud in 2024!

No matter how big or small the scale, account fraud doesn't discriminate and is notoriously difficult to get on top of. If your business falls victim to account fraud, you risk facing credit card chargebacks and large-scale data breaches, resulting in substantial fines and potential damage to your reputation.

> Anyone who runs a business online is at risk of fraudulent activity.

Dealing with online fraud is a huge task for all businesses providing a product or service online. In this e-book, we'll tell you why it's important to reduce your business' exposure to fraud at the very first point of contact, how to prevent fake sign-ups and why email address intelligence is one of the most effective ways to do so.

** Source: Cyber security breaches survey 2025*
*** Source: https://chargebacks911.com/cyber-shoplifting/*
**** Source: UK Finance*



Account Fraud

Why Is Account Fraud a Problem for Online Service Providers?

Account fraud occurs when a fraudster uses a fake or stolen account to pose as a legitimate user of a system, then abuses the capabilities this gives to them.

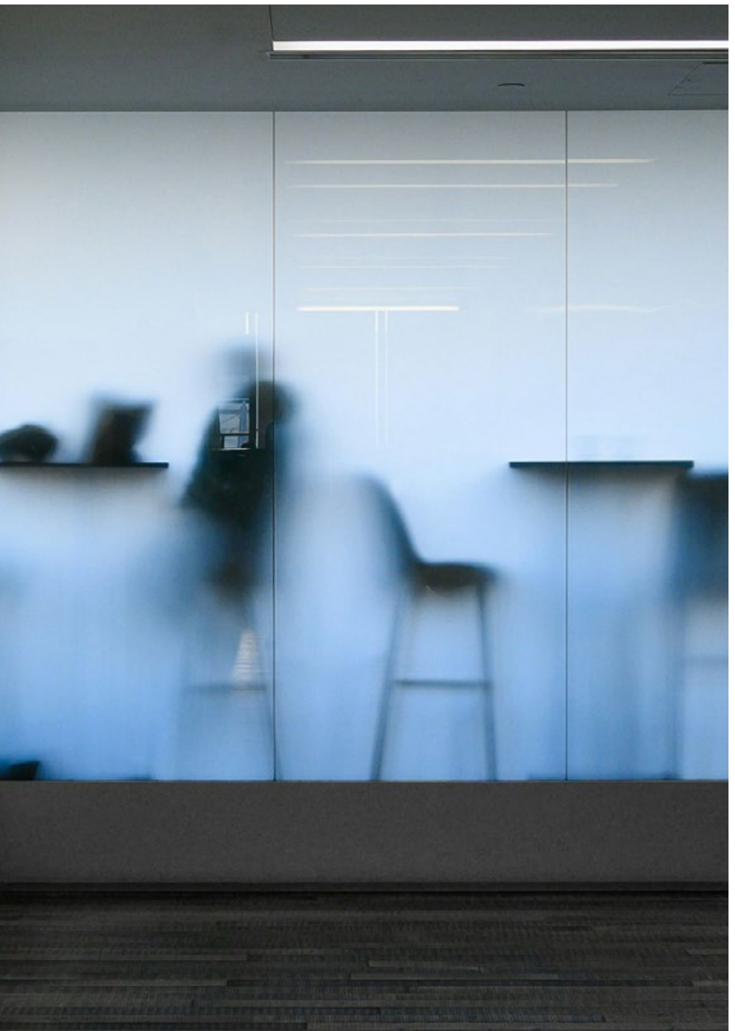
Suspicious sign-ups to your website can be a warning sign for account fraud and ultimately lead to financial losses, damage to your reputation as well as legal issues.

> “”
> £1.17 billion
> in the UK alone was stolen through unauthorised and authorised fraud in 2024.

Account Fraud

Who is Most at Risk?

Account fraud affects all online service providers, but certain industries face greater risk due to the nature of their onboarding flows, incentives, and user behaviours.



Understanding these high-risk sectors can help shape a stronger fraud prevention strategy.

eCommerce
High traffic and incentives like discounts or free trials make eCommerce platforms prime targets. Fraudsters use fake accounts to exploit offers or conduct payment fraud.

Fintech & Crypto
The financial value of accounts and quick access to funds attract sophisticated attempts, often involving synthetic identities and bot-driven sign-ups.

SaaS Platforms
Freemium models, trials, and usage-based billing can be exploited by fraudsters who cycle through fake accounts to avoid paying or test attack vectors.

Online Education & Training
Platforms offering credentials or gated content are targeted by users attempting to gain access without valid enrolment.

Gaming & Social Platforms
Bots and fake profiles are used to manipulate engagement metrics, distribute spam, or abuse community features.

“”

We identify Your Unique Risks

By identifying the unique risks in your sector, you can tailor defences like email verification, identity checks, and fraud scoring to your business model.

Fake Sign-ups

Fake sign-ups are commonly perpetrated with the help of disposable email addresses.

Any business that collects data from their website, for example through a form, runs the risk of gathering fake information from spambots, fraudsters or people who don't want to give away their real details.

This can be problematic for online service providers because it potentially means allowing bad actors to access apps and services where they can make financial transactions, interact with other users, or even look for security loopholes they can exploit.

Fake sign-ups can harm your business in several ways:

1. Leads to the possibility of online service being abused
2. Increases the risk of fraudulent transactions
3. Increases the risk of security breach
4. Heightens the risk of credit card chargebacks

Many online service providers face challenges around the volume of sign-ups. If their service, product or app is very popular, it becomes more difficult to stay on top of risks within their data, making it even more important to spot fake sign-ups at the earliest opportunity.

The good news is, fake sign-ups can be combated!

1. Using detection and prevention tools to spot fake sign-ups
2. Using ReCAPTCHA-enabled signup forms, which require anyone signing up to your service to prove that they are human and not a spam bot
3. Performing identity checks that require proof that someone is who they say they are before allowing them to use the service
4. Exporting your lists and checking through them manually - many fake sign-ups are easy to spot because they share a common characteristic such as an alphanumeric string or domains that contain the same word
5. Enable email verification. Require users to verify their email addresses after signing up. This ensures that the email address provided is valid and actively used.

Disposable Email Addresses

Disposable email addresses (DEA'S) are email addresses that only last for a short period of time before disappearing. they allow fraudsters to make transactions and then cover their tracks afterwards.

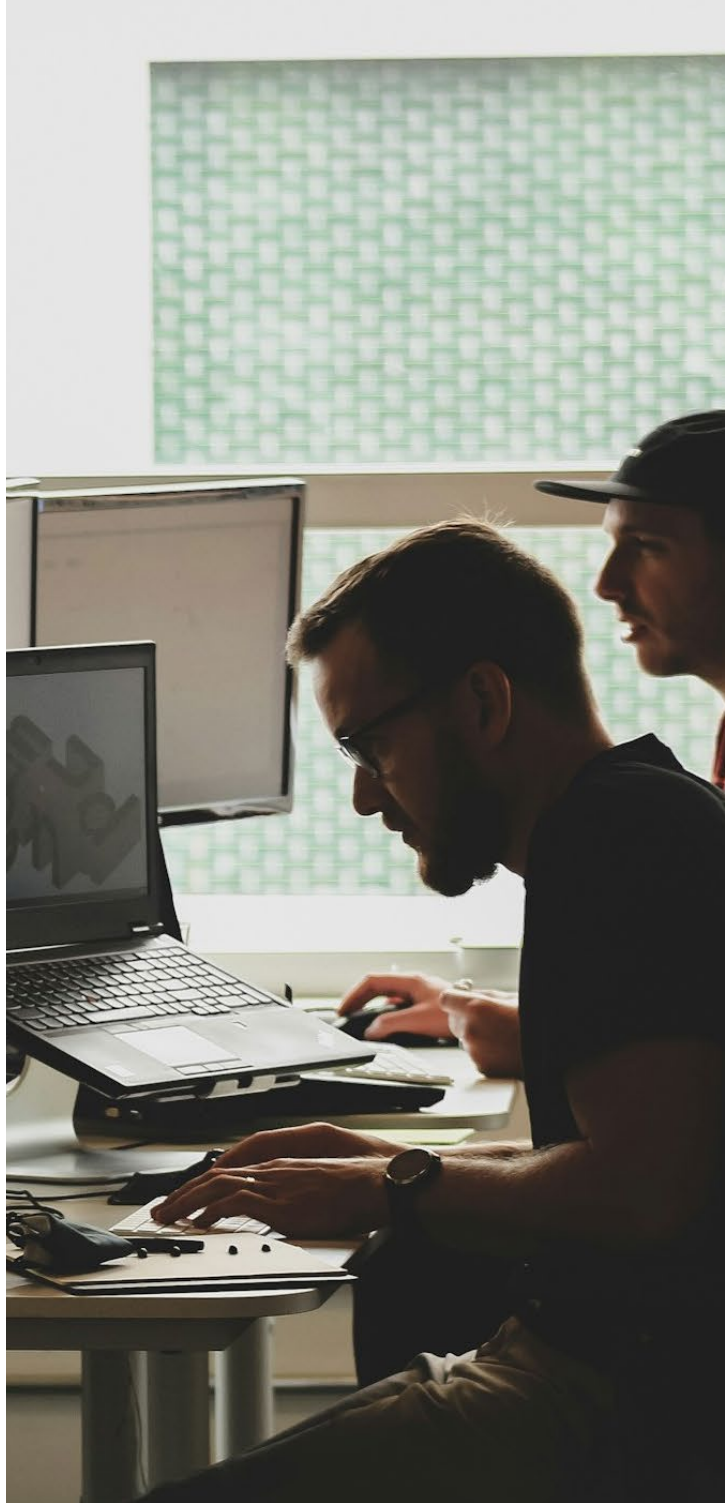
Disposable email addresses pose a risk to your business and can devalue your data if they reach your database. 2025 not only saw a notable increase in DEA's, but the introduction of hyper disposable email addresses. These are faster, more deceptive email addresses that are harder to spot... and they have an even shorter life span! With this in mind, how can businesses be expected to know which email addresses are disposable?

How email address intelligence is an effective way to stop fake sign ups

An email address acts like a digital fingerprint and reveals data about the person using it. It's also normally one of the first items of information captured about a person when they interact with an app or online service for the first time. For this reason, email verification can be used as the first line of defence against account fraud: helping companies spot warning signs of fraud from the moment the fraudster steps in the door.

In addition to prompting genuine users to edit errors in their email addresses, this can help reduce exposure to fraud and prevent harmful attacks.

Email address intelligence allows your business to build its own blocklists and rules by figuring out sign-up patterns and email addresses connected to fraudulent activity.



The key benefit of email verification intelligence is that it checks email addresses at sign-up, before a transaction takes place...

This gives your business more control over who you engage with and saves you time and money by reducing the risk of chargebacks.

Using ASSESS for detecting email fraud

Our fraud prevention tool, ASSESS, puts sign-up data and email address intelligence at the centre of fraud detection.

Key features

The ASSESS Trust Score
Tis is an aggregated score that shows the result of checking multiple elements within an email address, IP and username data. It helps your business to respond automatically to block fraud.

New disposable email address checks
This is led by our leading disposable email address detection system.

Advanced gibberish detection
This identifies email addresses that are potentially linked with fraud or spam bots. The enhanced service has been developed to reduce the need to manually review sign-ups.

Plus-address scoring
With this feature, you can deal with the growing use of multiple email addresses related to one primary account. Our plus-address scoring grades email addresses to qualify user intent.

ASSESS delivers a scalable account screening solution at the very first point of contact, reducing manual reviews and allowing you to automate preventative action.

How does ASSESS work?

Through a simple API, ASSESS enables online service providers to check every sign up coming into your system. Dark web links, spam history, temporary email addresses, mail provider quality, and many more 'tells' all set the scene for fraud and ASSESS can detect all of these.

Why use Email Verification?

Email verification is cost-effective, easy to integrate and extremely powerful in keeping your data secure. Systems can immediately take action against potential account fraud by analysing email addresses as they are entered and checking results against a specific set of rules, rather than running your lists manually.

This means that ASSESS can check every address entered into your system within milliseconds and takes location points associated with IP address and mail server into consideration. It also cross-checks for known geographical fraud 'hot spots' and provides a Trust Score to give you an instant view of how confident you can be about accepting sign-ups from new accounts.

In fact, our award-winning Trust Score has enabled us to reduce instances of fraud by more than 90% since 2016, despite an overall increase in CNP fraud of 24% each year in the same period in the UK.

What You Need to Know

Compliance in 2025...

Fraud prevention must work hand-in-hand with data protection and regulatory compliance.

In 2025, businesses need to stay ahead of evolving privacy frameworks while protecting their systems from misuse.

Key regulations to consider:

GDPR & ePrivacy Regulation (EU)
Personal data must be collected with clear purpose, transparency, and user consent. Email verification tools must operate within these boundaries.

UK GDPR & Data Protection Act (2018)
When using automated tools like ASSESS, organisations must demonstrate "legitimate interest" as a lawful basis for processing personal data related to fraud prevention.

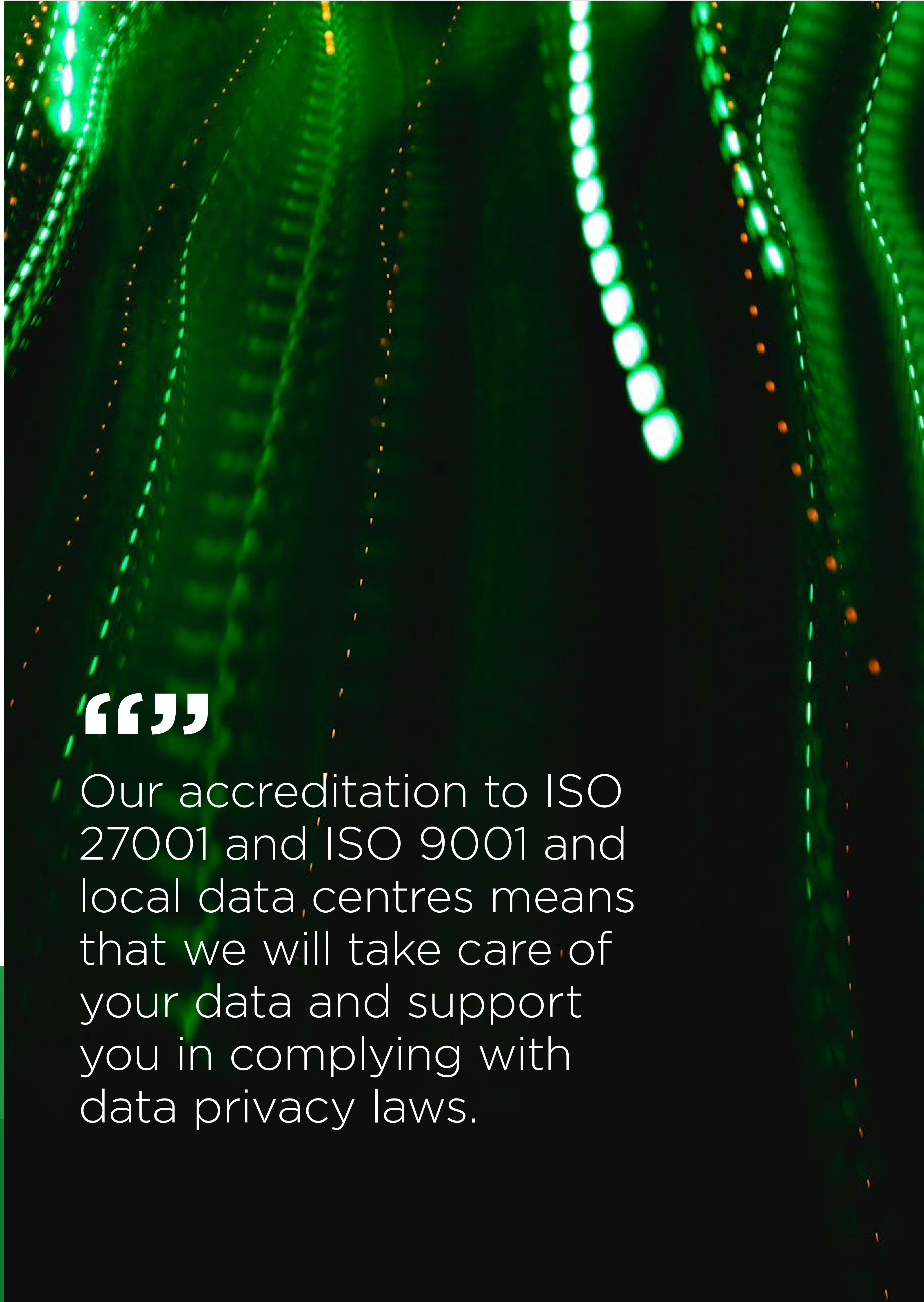
ISO 27001 & ISO 9001 Certification
These global standards signal robust information security and quality management. Email Hippo holds both accreditations to support customer trust and compliance.

Emerging Regulations
Stay prepared for the EU AI Act and growing patchworks of US state privacy laws — especially if your fraud prevention solutions include AI or behavioural scoring.

How Email Hippo supports compliance

1. Hosted in secure, regional data centres.
2. Avoids unnecessary collection of personally identifiable information.
3. Transparent about processing logic, third-party services, and uptime guarantees.

By choosing tools that are built with compliance in mind, businesses can reduce risk without compromising on security.



> “”
> Our accreditation to ISO 27001 and ISO 9001 and local data centres means that we will take care of your data and support you in complying with data privacy laws.

Case Study

Real-World Results

“”

99% Uptime

We guarantee 99.99% service uptime to ensure your system will never be out of action during email address checks, and we provide 24/7 support through real people, a clever bot and a library of online resources

CRM SaaS

A fast-growing CRM software company serving mid-sized businesses worldwide faced a steep increase in fake trial sign-ups, with over 30% of weekly registrations flagged as suspicious. These false accounts drained resources, skewed campaign metrics, and triggered concerns about bot-driven activity.

To solve this, the company implemented Email Hippo's ASSESS API at the point of registration. The integration was seamless and preserved a smooth user experience.

Results after 30 days:

- 60% reduction in disposable and temporary email addresses
- Dramatic drop in false trial accounts using gibberish or spoofed domains
- Marketing teams gained confidence in campaign performance metrics
- Manual list reviews reduced by 80%, saving time and effort

ASSESS now plays a central role in the company's fraud strategy, silently screening each sign-up and enabling the team to focus on engaging real users.

emailHIPPO

About Email Hippo

Email Hippo was established in 2000 as a 'sticky' tool that was popular on an IT advice and affiliate marketing website. Through this tool, we were quickly established as a pioneer in email address validation. There were other services out there, but they were all desktop-based and couldn't be scaled up because mail servers would not trust repeated enquiries from small business networks or dynamic IP addresses. Today, Email Hippo continues to lead the way in email verification solutions, with an app that allows you to 'verify on the fly'.

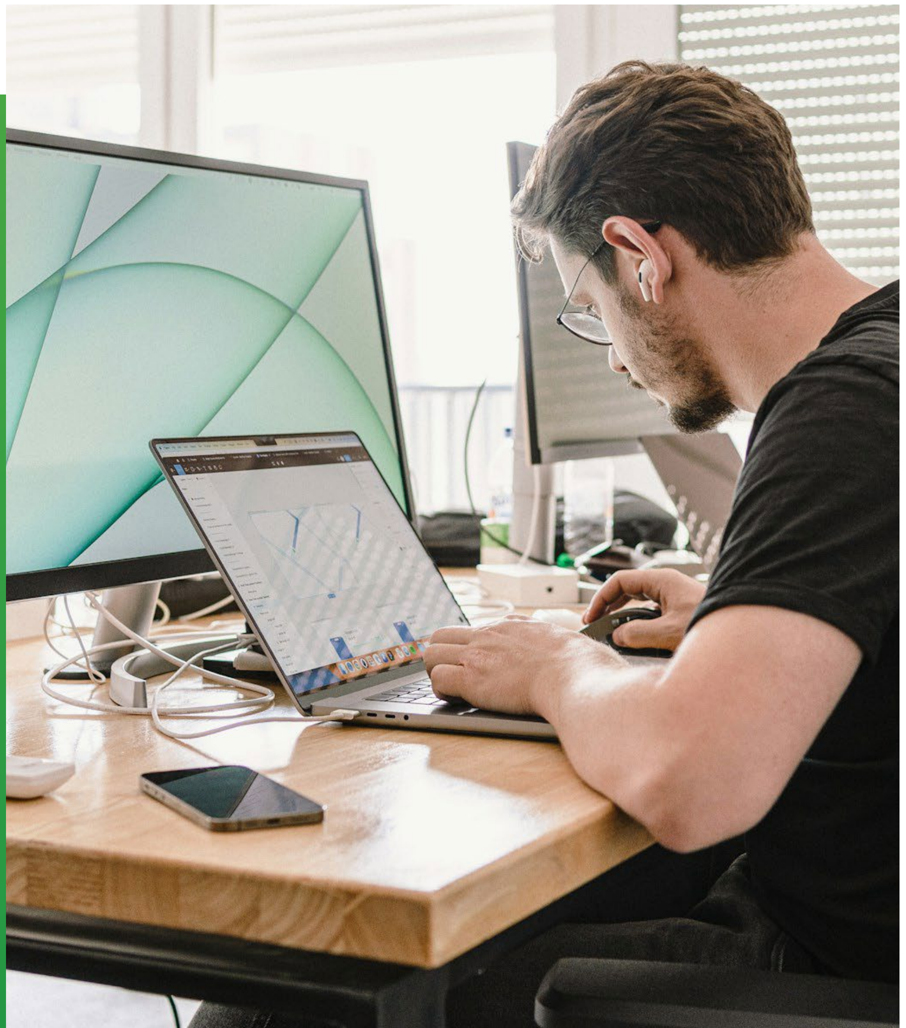
Solving this problem was an attractive challenge for our developers, whose tools were experience, knowledge and email validation software. With this toolkit, they set about engineering a fraud-proof sign-up process.

This fraud-proofing product became our next API, and we launched MORE as a product that combined email verification with additional checks that spotted suspicious sign-ups. Since then, we've added more products for a variety of uses.

Our app allows you to Verify on the Fly!

In 2017, we became the first company in the industry to receive international security accreditation ISO 27001. We have also been awarded a Queen's Award for Enterprise, the UK's most prestigious award for innovation.

> “”
>
> Email Hippo have experienced extraordinary growth over the years.
>
> *However, we were also targeted with 'friendly fraud'.*



Take Advantage of all Email Hippo's Email Verification Tools

We've designed a series of email solutions, tailored for different uses. Try for free to see how Email Hippo works for your business.

No payment details required, and no obligation to sign-up at the end of the trial!

CORE
Our basic email list checking solution that's perfect for all businesses

MORE
An email validation API tool that specifically filters sign-ups, improve data quality and stop disposable email addresses

ASSESS
Prevent fraud at sign-up with our fraud prevention API

INSIGHT
Perfect for service providers with large data sets that require a more powerful email validation API.

You can trust us with your data

We understand that data is valuable, and it can feel like a risk to trust someone else with your information. Rest assured that our accreditation to ISO 27001 and ISO 9001 means we will look after your data and support you in your compliance with data privacy laws.

Our principle is to treat each bit of data we process as if it was the most sensitive data we could ever handle. We invest in our people and work processes, as well as in third party services such as penetration testing and firewalling to ensure we all sleep easy.

We share compliance information, server policies and information about the third-party security services we use so customers can confidently do business with us.