White Paper

Disposable emails in fraudulent activities

Unveiling the threat

Ana Bargo, Dilip Singh
Equifax D&A

May 27, 2025

Abstract

In the ever-evolving landscape of online interactions, the use of disposable emails has emerged as a tool for both consumers seeking privacy and fraudsters seeking anonymity.

This white paper explores the concept of disposable emails — delving into their nature, the motivations behind their usage, the potential risks they pose, and the role of advanced models in identifying and mitigating their impact on fraud.

Introduction

The digital era has ushered in unprecedented convenience in communication and commerce. However, it has also given rise to new challenges, with fraudulent activities disappearing in the world of legitimate activities.

One such tool is the disposable email, an innovation that serves both legitimate users and malicious actors. This paper aims to discuss the complexity of disposable emails, offering insights into their use, misuse, and the role advanced models play in mitigating associated risks.

What are disposable emails?

Disposable emails are temporary, one-time-use email addresses created with the primary purpose of facilitating short-term interactions. These email addresses are typically discarded after a single use or a brief period, making them appealing for users seeking to keep their online presence private.

Types of disposable email addresses:

Throwaway: These email addresses can last between 10 minutes and a few days. For a small amount of time, the emails work as expected, but then all emails sent to that address are deemed non-deliverable.

Throwaway emails can be either created by a random program, or utilize temporary or unsafe domains.

Alias: These email addresses look like a traditional email address but have an add-on; for example - email handle "+alias" @domain.com.

Alias emails can be made by adding special characters and a label to an existing email address.

Forwarding: An email service from a different domain from the user's private email address that forwards emails to another account.

Forwarding services require constant monitoring and changing from users, as different services are discovered and blocked.

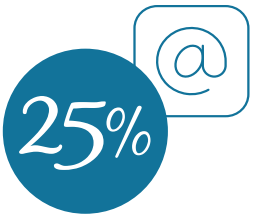
Emails are already considered slightly risky to authenticate because they are free to create, which means it is relatively easy for anyone to open a new email account that they never plan on using.

Additionally, businesses that rely on email verification methods could face difficulties verifying user authenticity. This fact leaves businesses open to a lot of potential liability if we don't put a stop to them.

Why consumers want to use disposable emails

Both businesses and individuals alike use disposable email addresses. Businesses use disposable emails, oftentimes in the format of "noreply@domain.com" or something similar, to send out marketing or order status information.

One survey states that 25% of consumers have opted out of brand emails because of the impersonal nature of the use of disposable emails.



of consumers have opted out of brand emails because of the impersonal nature of the use of disposable emails.

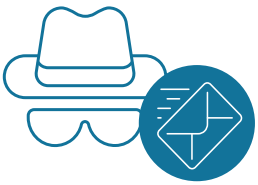
Legitimate consumers often resort to disposable emails to safeguard their privacy in various online activities. From signing up for newsletters without revealing personal email addresses to accessing limited-time promotions, the desire for increased anonymity drives individuals to employ disposable emails for day-to-day online engagements. Since most consumers have more than one email address, it is easy to provide an alternative email when they are unsure whether they would like to fully engage with a business.

There are other reasons why consumers do not want to share their personal emails. Specifically speaking, people who do not wish to receive multiple, repeated marketing emails. Additionally, consumers also would like to know what companies are doing with their information - they want to get to know the companies first before sharing their private emails with them.

Why disposable emails are detrimental to businesses

While the legitimate use of disposable emails is understandable, their darker side lies in their exploitation by malicious actors. Fraudsters capitalize on these temporary addresses to engage in deceitful practices such as identity theft, phishing, and fraudulent transactions.

The transitory and dynamic nature of disposable emails makes it challenging for traditional security measures to trace and counteract these illicit activities effectively. Businesses could be liable for fraudulent transactions — such as account takeovers — due to fake accounts.



Scammers and cybercriminals can use disposable email services to create fake identities or register on websites with malicious intent.

Scammers and cybercriminals can use disposable email services to create fake identities or register on websites with malicious intent. They can exploit this anonymity to engage in activities such as online fraud, phishing, or identity theft. Plus, these services can be vulnerable to security breaches. Since these services often lack robust security measurements, unauthorized access to temporary email accounts is possible. This can lead to the exposure of sensitive information and compromise user privacy.

Another way that businesses can be impacted is that having a lot of disposable emails in your lists can lead to emails that are never opened (and later on, never even delivered) — which leaves you with inaccurate analytics and reputational damage. There is also a risk that once the email is disposed of, that user handle can be used by someone else, which could in turn put your business at risk of sharing private information with the wrong person.

In addition, email domains that are unopened or not delivered are often placed on a spam list by email providers. So when you try to reach your customers, your emails are placed in a spam or junk folder. It can really damage your market reach, meaning that you won't see as much return from your marketing efforts. In turn, you may wind up wasting the money you put into the marketing.

Identifying disposable emails through modeling

To combat the misuse of disposable emails, advanced modeling techniques offer a robust solution. Machine learning models — both supervised and unsupervised — trained on extensive datasets can analyze patterns, behaviors, and anomalies associated with disposable email usage. By integrating these models into security protocols, organizations can efficiently identify and block potentially fraudulent activities, enhancing the overall resilience of their digital ecosystems.

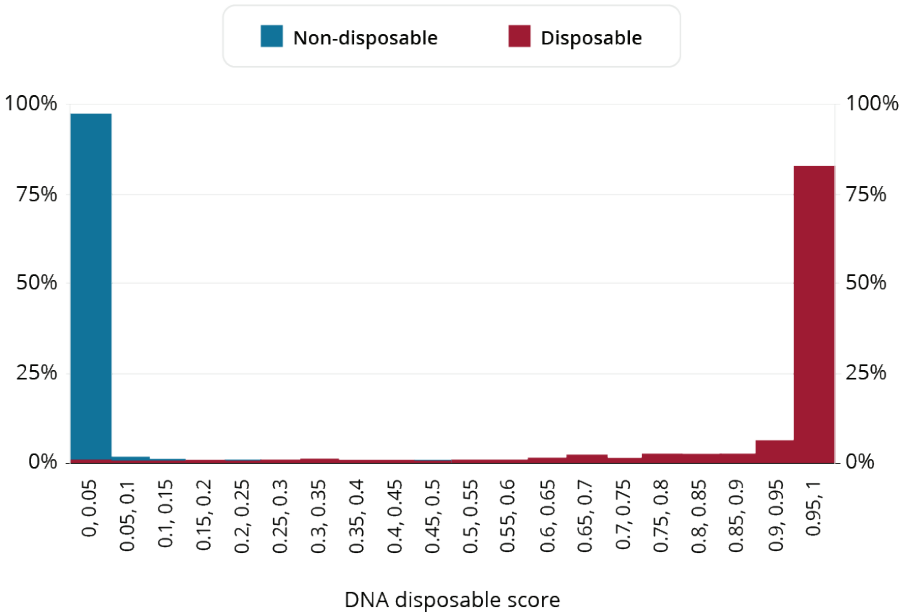
How is Equifax addressing the disposable email issue?

Equifax has created an ML-based model that identifies disposable emails, whether they come from forwarding servers, are throwaways, or are aliases.

Different attributes describing emails were created for the ML model. These attributes explore the distribution of domain characteristics and handler characteristics. The modeling process takes into account the linguistics-based characteristics of the email name and domain, and applies a mix of rules-based and ML algorithms to make the model decisions explainable.

Model results boast superior disposable email identification, intuitive rationale for each email component the model identifies as suspicious, and an in-house approach to identifying new threats.

Figure 1: Disposable email model score vs. Disposable flag



Our commitment to consumer safety and account protection is further bolstered by this novel way to identify incoming threats to consumers.

Conclusion

In the complex web of online interactions, the use of disposable emails introduces a dual challenge: preserving user privacy while thwarting malicious activities. Striking this delicate balance requires a multifaceted approach, with advanced models at the forefront of identifying and mitigating the risks associated with disposable emails. As we navigate the evolving landscape of digital transactions, vigilance, innovation, and collaboration remain essential in safeguarding the integrity of online platforms and protecting users from the shadows of fraudulent endeavors.

Identifying disposable domains can take on many different forms:

- Identifying forwarding domains
- Using REGEX-based functions to identify aliases or other special characters
- Building attributes to identify common patterns in the email handle and domain, and using ML-based methods to predict whether an email is disposable or not