How to Reduce Fraud and Prevent Abuse: Anti-Fraud tools and Registration Flows for Registrars

Introduction

While improving reactive processes to DNS Abuse is important and the focus of much of the work of the DNSAI, ultimately the DNSAI and industry needs an approach that helps prevent abuse from happening in the first place. But preventing abuse from occurring requires acting on potentially malicious domain names, which can bring its own challenges, including lost customers and false positives.

This document aims to demonstrate the opportunities for retail[1] domain registrars to prevent abusive registrations while reducing potential impacts to registrants and anti-abuse teams. There are three key components to this work:

- Understanding the overlap in DNS Abuse and payment fraud;
- Leveraging existing tools; and
- Optimizing registration processes

Below we put these together.

Reduce Fraud, Reduce DNS Abuse

For most retail registrars, domain registration is a volume-driven, low-touch business, requiring the automated processing of thousands of credit card transactions a day. A domain registrar with half a million names under management[2] would likely be averaging around 1,400 renewal and new registration transactions a day, or 42,000 a month.[3]

Malicious actors, the people registering domain names explicitly to conduct phishing and other forms of DNS Abuse, do not generally do so using their own identity and payment methods. The most common form of payment for these activities is to use stolen credit card numbers.

[1] Wholesale registrars may consider what attributes could be passed from their downstream partners
[2] Registrars with over 500,000 names represent a majority of the domain registration market
[3] Assumes that domains are evenly distributed throughout the year, and that new registrations + renewals keep the Registrar stable.

Sometimes a charge to a stolen credit card goes unnoticed by the card holder. But frequently, the cardholder will dispute the charge.

Credit card chargebacks, where a cardholder disputes a charge with their bank and the bank reverses the charge due to fraud that occurred at the merchant, are deeply problematic for registrars in this context. Not only is the registrar losing revenue and potentially paying the registry for the cost of the domain (depending on the timing of the delete and the registrar's Add Grace Period status) but also puts their ability to process payment transactions at risk. Being terminated by their payment processor for too many credit card chargebacks, primarily because of fraudulent transactions involving stolen credit cards, is an existential risk for many registrars.

Consequently, the vast majority of retail registrars already have some form of anti-fraud processes in place and, conveniently for our purposes, by leveraging these tools we can reduce malicious domain registrations, fraud, and chargebacks.

Registration Flow

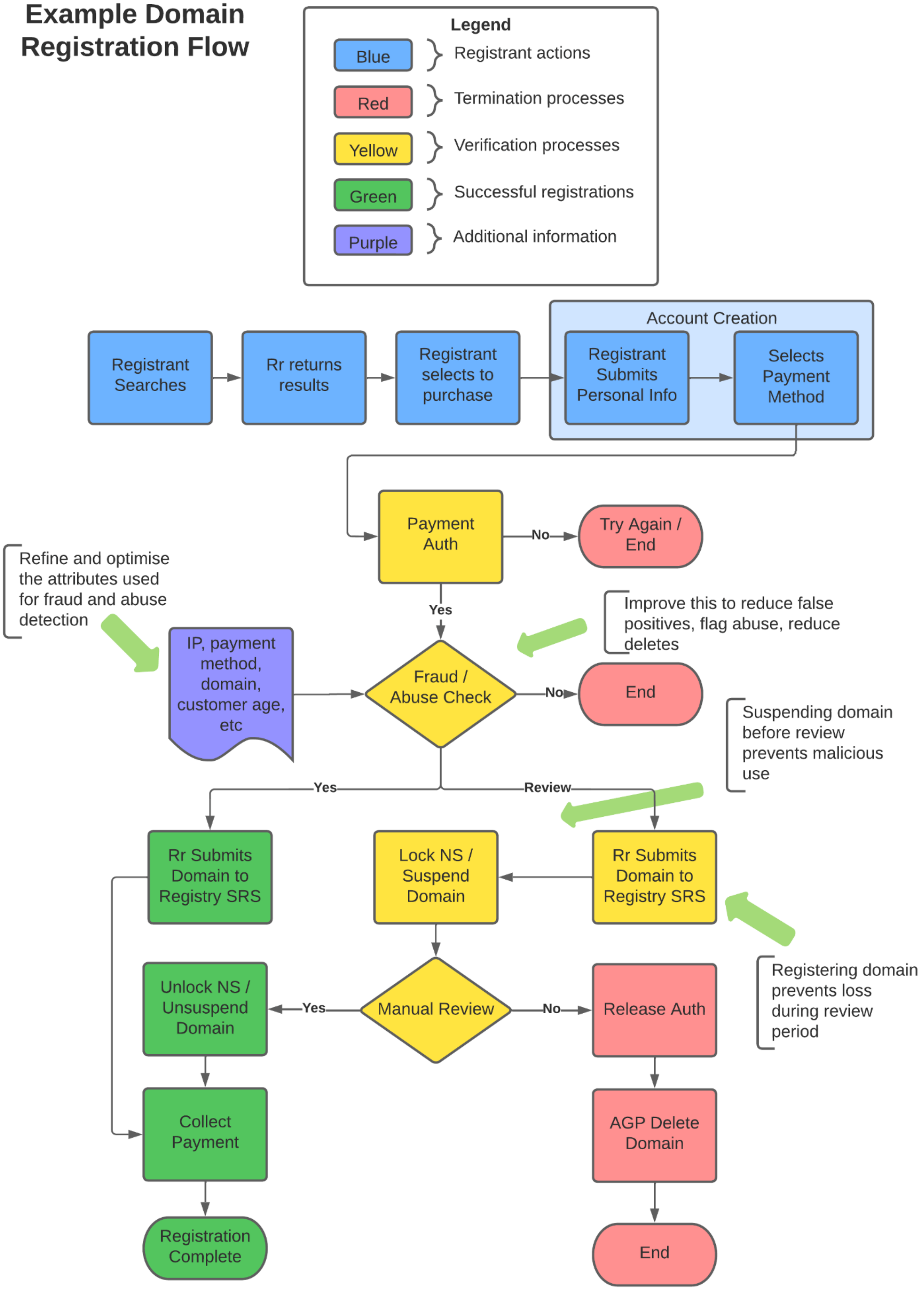
Below is a simplified domain registration process for a retail domain registrar.

- In blue are the customer led registration processes
- In yellow are the processes that are used to reduce abuse and fraud
- In red are the processes that end a transaction
- In green are the processes to complete a registration
- In purple are the data that one feeds into an anti-fraud process

This document is primarily concerned with two components of this process:

- The fraud and abuse check, including what data is passed into it
- The process for reviewing potentially malicious registrations

Example Domain Registration Flow


Legend
Blue
Registrant actions
Red
Termination processes
Yellow
Verification processes
Green
Successful registrations
Purple
Additional information
Account Creation
Registrant Searches
Rr returns results
Registrant selects to purchase
Registrant Submits Personal Info
Selects Payment Method
Payment Auth
No
Try Again / End
Yes
Refine and optimise the attributes used for fraud and abuse detection
IP, payment method, domain, customer age, etc
Fraud / Abuse Check
No
End
Improve this to reduce false positives, flag abuse, reduce deletes
Suspending domain before review prevents malicious use
Yes
Review
Rr Submits Domain to Registry SRS
Lock NS / Suspend Domain
Rr Submits Domain to Registry SRS
Registering domain prevents loss during review period
Unlock NS / Unsuspend Domain
Yes
Manual Review
No
Release Auth
Collect Payment
AGP Delete Domain
Registration Complete
End

Fraud Tools

There are many payment processing services in the market today, most of them offer some form of anti-fraud service, sometimes for a per-transaction fee. These features are more sophisticated than the basic CVV checks that all credit card transactions must pass. A few of the larger ones are:

- Radar, from Stripe
- Risk Manager, from Square
- Merchant Fraud Protection, from Braintree
- Fraud Protection Services, from Paypal Payments
- Fraud protection, from GlobalPayments
- RevenueProtect from Ayden

Most of these services operate in a similar fashion: the merchant provides them with attributes of the transaction and they return a score that indicates a likelihood of fraud. These scores result in three potential outcomes:

- The transaction is approved
- The transaction is denied
- The transaction is flagged for manual review

In a perfect system, all malicious registrations and fraudulent transactions would be denied and everything else would be approved. In the real world, merchants are in a constant process of responding to risks and balancing and tuning systems to reduce manual review, prevent unhappy customers, and reduce fraud. In the rest of this section, we explore what data elements a registrar should consider adding to their anti-fraud processes to improve detection. In the following section, we detail best practices related to manual review.

In general, reducing fraud is going to also reduce malicious domain registrations, as they frequently go together. However, by leveraging these fraud tools to deliberately also catch malicious registrations, we can increase the detection of both.

This is done by providing the fraud detection services with additional information, not only about the customer and the transaction, but also about the domain itself. Typical anti-fraud attributes passed to fraud detection systems include:

- Customer details
    - Geography

  - Account age
  - Number of previous transactions
  - Number of declined transactions
  - Frequency of recent transactions
  - IP address
  - IP address geography
  - Previous IP address(es)
  - Previous IP address geography
  - Is it a renewal transaction
- Transaction details
  - Amount
  - Amount of discount applied
  - Payment type
  - Payment geography

Depending on the features of the payment processor, the processor can either incorporate additional data points into a machine learning model, or the registrar can build their own rule sets and weights. For example, the Registrar may wish to create a rule where the inclusion of a frequent phishing term would increase the likelihood of fraud.

We suggest adding attributes of the domain names themselves:

- Domain name
- TLD
- Number of dashes
- Does it contain non-ASCII characters
- Does it contain frequent phishing terms or misspellings of these terms, such as: login, support, billing, or gov
- Does it contain frequently exploited brand names or misspelling of such names, like: Apple, Netflix, Google, Facebook, iCloud, etc.
- Does it contain frequently exploited names of financial institutions, like Paypal, CitiBank, HSBC, etc

If the registrar sells primarily within a particular geography it should consider adding additional terms and brand names. For example, a French registrar would add the names of French banks and payment services.

Further, abuse follows current trends and term lists should be updated and adjusted frequently and accordingly. At the time of this publication, there is a general concern with heating costs over winter in Europe and, consequently, there has been an increase in malicious registrations related to heating solutions.

It will require time and testing to optimize the attributes and how they are used but by providing these fraud tools with domain specific attributes, it is possible to reduce fraud and abuse simultaneously. The DNSAI is considering how to collect and share an optimized set of attributes for the industry to use.

Registration Flow & Manual Review

It is straightforward to deal with transactions that are approved or denied by the payment processor, but the transactions that are flagged for review require more work. Below we suggest an architecture for domain registration flow that can limit the harm malicious registrations can do, while minimizing the impact on customers.

For transactions that require a manual review we want to meet three goals:

- Reduce the harm caused by potentially malicious domain registrations
- Reduce the impact on legitimate registrants
- Reduce the impact on fraud and compliance teams

The way these three goals intersect with a manual transaction review is found in how the transactions are processed. In discussions with retail registrars, three different approaches have been shared. These were:

1. A transaction is flagged for manual review and the domain is registered prior to the review.
2. A transaction is flagged for manual review and the domain is not registered until the completion of the review.
3. A transaction is flagged for manual review and the domain is registered prior to the review but suspended until the review is complete.

The process with the least impact to legitimate registrants would be to operate a 24/7 anti-abuse team ensuring that all flagged transactions are reviewed prior to registration. This is unfortunately not an option for all but the largest registrars. A registrar using the first approach above saw increases in abusive registrations on Fridays at 6pm, because malicious registrants knew they would have the weekend to use the domain prior to its likely deletion on Monday. The registrar in the second scenario saw frustrated customers, unable to use their domain immediately, often over a weekend.

While there is substantial diversity in the approach with the domain registration industry. The DNSAI prefers scenario three. By suspending domains flagged for review the registrar ensures the domain is not lost, but can also prevent harm from malicious registrations. Further, by completing the review before collecting payment, the registrar can reduce the volume of fraud-related chargebacks it receives.

The idealized registration flow diagram above follows this example.

Other Tools & Approaches

Some registrars have found success with other methods that may be less generally applicable. One registrar found a substantial amount of their abuse was coming from countries they neither operated or marketed in, and subsequently refused service to customers from those locations.

Other registrars have found that preventing domain registrations from IP addresses associated with cloud computing providers or VPN(s) has reduced the amount of fraud and abuse they see.

Future Work

There are clear places for future work based on the above. First is a service to optimize and share the domain name attributes used in detecting malicious registrations. Ensuring that domain registrars have access to useful and timely information that can be fed into their systems could make a meaningful difference in reducing malicious registrations.

Second is to investigate if there is sufficient value and interest in malicious-detection-as-a-service in order to develop such a service. A simple API, optimized for the purpose of detecting malicious registrations could prevent substantial amounts of harm.

Additionally, we would be remiss if we did not acknowledge that any approach will need to be evolutionary. There is not going to be a single solution that works in perpetuity. Malicious actors are dynamic and will evolve their tactics in attempts to evade both detection and countermeasures.

Summary

Because of the overlap in malicious registrations and payment fraud, it is possible to use transactional anti-fraud tools to prevent DNS Abuse. This is done by providing and optimizing additional information into the fraud detection tools that most registrars will already have in place.

This approach leverages tools already at the disposal of most retail registrars, and has the potential to reduce fraud, abusive registration, and credit card chargebacks.   Additionally, these benefits are compounded by reducing the substantially greater costs of reactive anti-abuse efforts in the future. In short, preventing abuse is a substantially lower cost than mitigating it.

Further, for domains that are flagged for review, it is generally recommended to register and suspend the domain until the review is completed to prevent malicious use, especially between registrar operating hours.