TCPA settlements in the crosshairs of typosquatters

Posted on February 20, 2020

The Telephone Consumer Protection Act of 1991 (TCPA), Public Law 102-243., as also explained on its Wikipedia page, "restricts telephone solicitations (i.e., telemarketing & BPO) and the use of automated telephone equipment. The TCPA limits the use of automatic dialing systems, artificial or pre-recorded voice messages, SMS text messages, and fax machines."

Naturally, it has generated a number of court cases, which frequently result in calls for settlement claims. Victims can submit their claim online, either directly, or with the help of a number of lawyers and their companies specializing in helping with such cases. The related web pages attract a lot of visitors, and many of them type in the URL of the case manually - a very attractive situation to do some typosquatting… leaving a footprint of TCPA settlements in the records of WhoisXML API's Typosquatting Data Feed.

Most frequently, this goes about collecting some advertisement money. The recipe is as simple as that. Create some domain names which are misspelled versions of the legitimate site. Add pages containing links to searches with popular topics you see as possibly attractive for visitors ending up here. Some of the links can even point to other pages within the group of your domains. Finally, monetize the whole stuff by adding a pay-per-click service.

Before checking how to find a plethora of such actions by using the files from the Typosquatting Data Feed, let us first assess to what extent such typosquatting activities can be considered as harmful.

Making money with pay per click is a great opportunity for bloggers and web page operators to obtain financial support for their activity. The Internet is a medium which provides a great opportunity for talented content creators to efficiently reach their audience. Writing a good blog takes a lot of time and effort; a lot of great content could never appear without the pay per click money support for their creators.

Creating a page without a real contribution, just to collect money upon unwanted mistyping of URLs is a very unethical misuse of this system. The pay per click model is definitely not fit for this type of money collection.

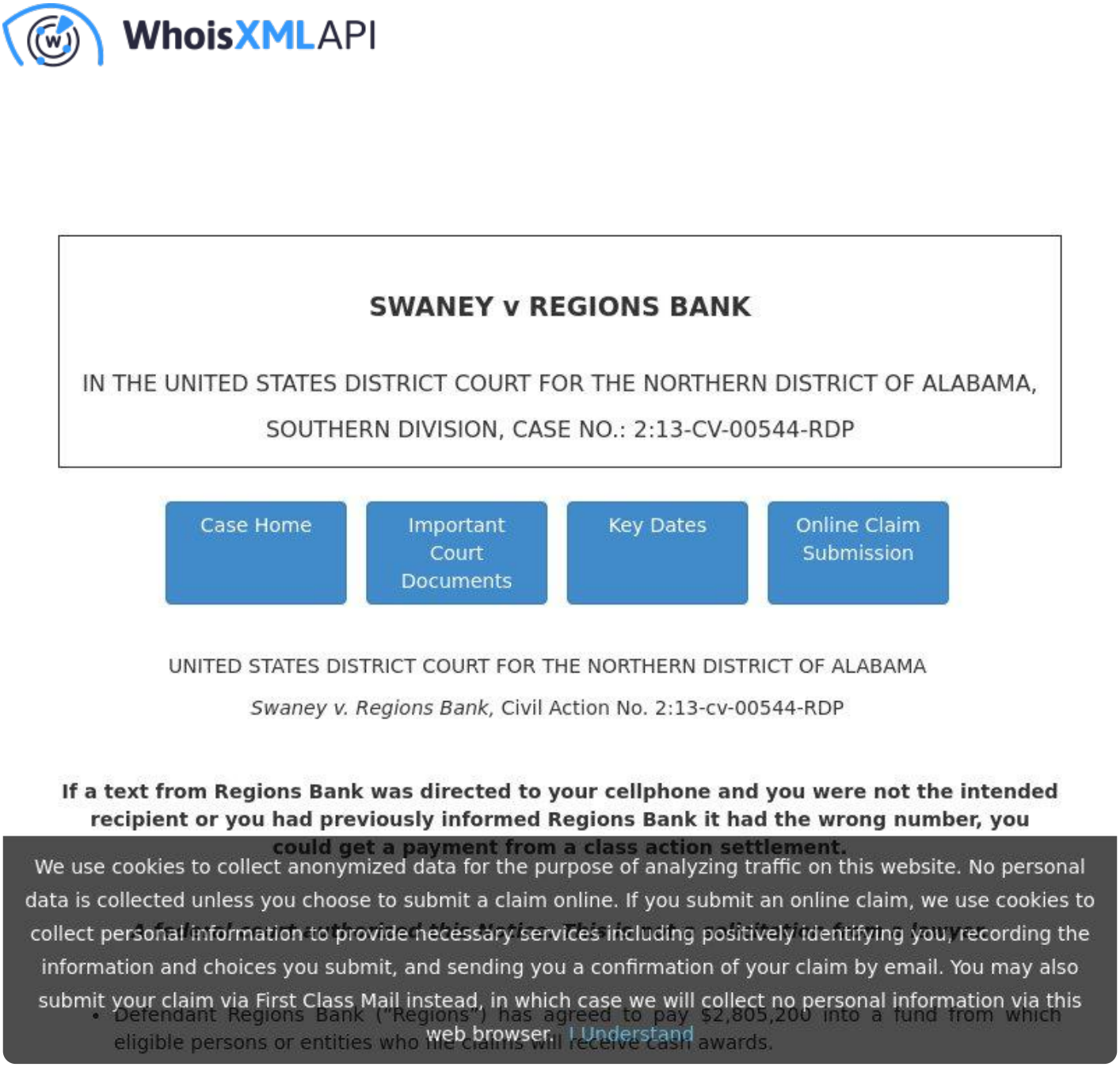
In addition, typosquatting is also harmful in the sense that the less trained users to whom a webpage appears in their browser as a trusted source of information, like a TCPA settlement site, can be completely misdirected. Instead of finding a page to file their rightful claim for a breach settlement, they may end up on a page collecting links leading to completely different pages.

Let us see a recent example of how such a situation works in real life, along with an illustration of how the domains related to this kind of scams appear in the Typosquatting Data Feed. In fact, the data feed is capable of detecting a typosquatting action without being aware of its existence in advance. For instance, via a simple text search in the feed data for "tcpa" in the data set of December 24, 2019, we find the following group of 8 domains:

1. tcpasettlmentregionsbank.com
2. tcpasettementregionsbank.com
3. tcpassettlementregionsbank.com
4. tcpsettlementregionsbank.com
5. tcpasettlementregionbank.com
6. wwwtcpasettlementregionsbank.com
7. tcpasettlementregionsbank.com
8. tcpasetlementregionsbank.com

In order to be present in the dataset, these domains had to be added on the same day (i.e, December 24, 2019) to the domain name system as new, and their names also had to be similar to each other.

Now, what could be the reason for such bulk registrations by potential typosquatters? A quick google search for "TCPA settlement regionsbank" will quickly help find the background of the story at https://www.tcpasettlementregionsbank.com/, allegedly, the page of this settlement, which looks like this:



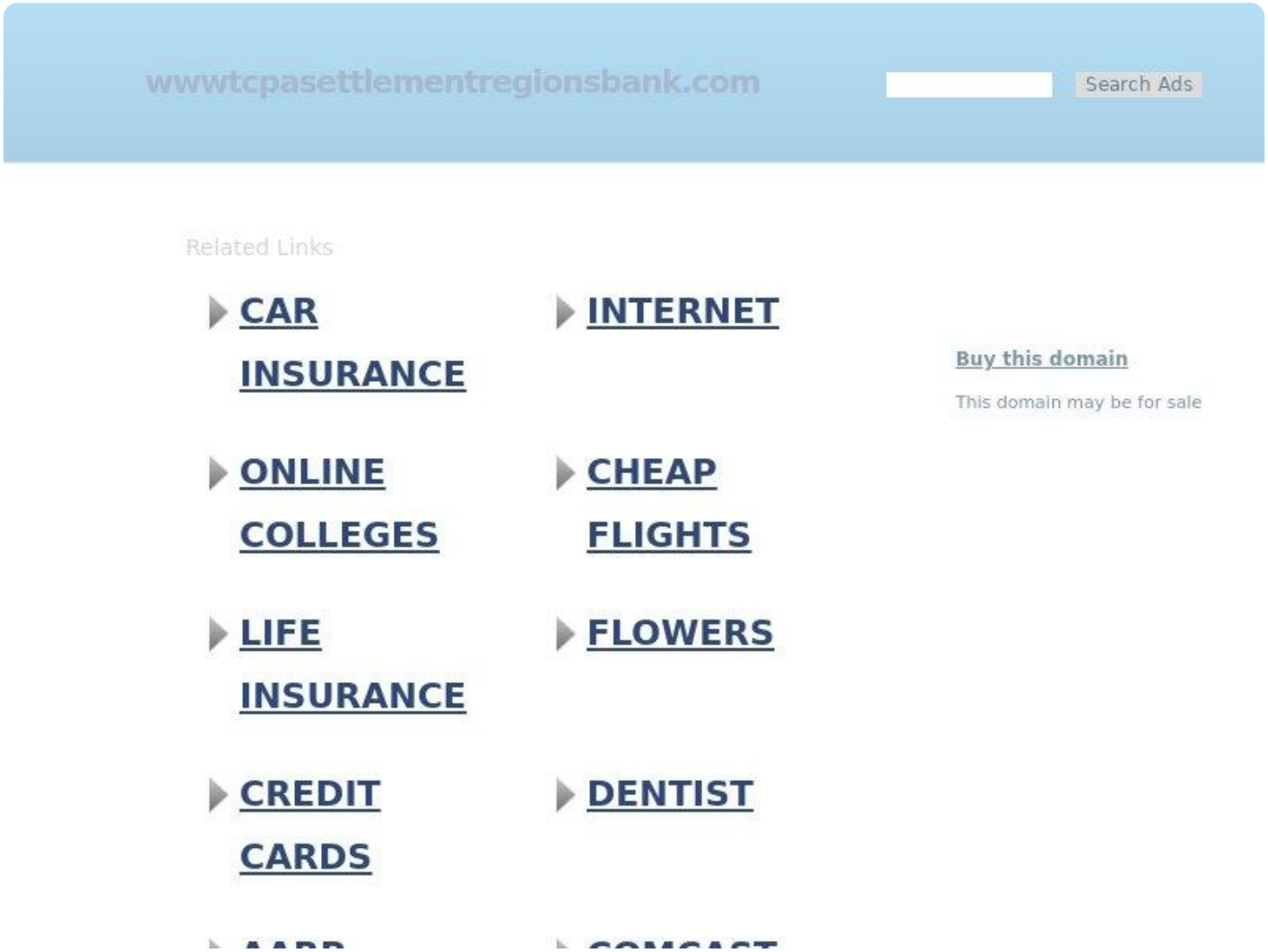
The case is referred to on the page as the "Swaney v. Regions Bank, Civil Action No. 2:13-cv-00544-RDP", at the United States District Court for the Northern District of Alabama. The claims can be submitted from April, 2020, to receive a payment. Interestingly, this page with the information is the 7th registered domain in our group.

Looking at the WHOIS data of the domain, we find that the registrant's details are hidden; unfortunately, this is in the habit of legitimate registrants these days, too, so one should not draw far-leading conclusions from this. Nevertheless, it was registered at GoDaddy, and the registrant is from the US. The page expires on 2021-12-23, after 2 years, which is standard practice. The web

page it hosts looks legitimate, although there is no information mentioned on it about who exactly is running it. Nevertheless, they list a phone number, so before submitting a claim here, it is a good idea to phone them and ask about it, just to make sure that it is not about phishing, and to find out who will act upon the claims submitted here – especially as there is no street address appearing on that page, just a P.O. box. The sentence "Please do not contact the court, the judge, or the Regions Bank with questions about the settlement or claim process" does not improve our trust in this page either.

But let us assume that, in spite of all the suspicious signs, this page is legitimate, and let us remember the IPs the WHOIS API gives us for this domain: 104.18.62.99 and 104.18.63.99.

Let's now take a good look at the other 7 domains in the group. Taking a screenshot of them with WhoisXML API's Screenshot API to avoid any penetration into our browser or getting our IP address logged by some malicious actor, e.g. wwwtcpasettlementregionsbank.com shows the following page:



All the others look similar to this. And indeed, this is the very design of ad collector pages: a number of links to different topics, but no information about the breach settlement… A look at the page source shows that indeed it uses Google's services to collect ad money.

Looking at the WHOIS data (e.g. the WHOIS API or Domain Research Tools), we see that nearly everything is "redacted for privacy". However, the registrant is from China, and the IP is 103.224.182.242, different from that of the assumedly legitimate domain. The expiry date is 2020-12-24, so it has only been registered for one year. This pretty much suggests that it has nothing to do with the actual settlement. After checking the other 6 suspicious domains, it turns out they all

have the same data as wwwtcpasettlementregionsbank.com, including the country (China), IP, expiry date and name servers.

To summarize our example, we have a slightly suspicious but possibly legitimate page for the case, which, if it is really legitimate, should warn its users of the other pages and fix the issues mentioned here to deserve trust. In addition, we have found 7 more pages apparently making use of this all by ad money collection. And all of these were apparently put into operation on the same day, December 24, 2019, not quite in the spirit of Christmas…

The case also illustrates how the Typosquatting Data Feed can be used, along with other services such as the WHOIS API or the Screenshot API, or the integrated Domain Research Tools for further detecting and investigation. Indeed, notice that we found this purely by using the information in the Typosquatting Data Feed, so in a real-life situation it enables us to be proactive and know about similar cases even before they reach any media attention. It is enough to make a text search e.g. for "tcpa" (or "settlement", or "breach", etc.) in the data files of the feed to find similar threats.

To whom do we recommend this type of investigation? A few examples:

- **Organizations offering pay per click services** can verify their clients and filter out those who do not provide real contents on their pages.
- **Settlement services** can prevent similar attacks against themselves and warn their actual or potential clients to avoid similar traps.
- **Security operation centers** can devote extra attention to domains appearing in their logs as they can be potential actors or victims of typosquatting threats. They can warn users visiting such pages or receiving e-mails containing these domain names of potential risks.
- **IT security researchers** can get hints and clues to reveal trends in registrations of typosquatting domains.

If you find this interesting, visit the web page of the Typosquatting Data Feed to give it a try or subscribe.