**WHOIS Query for Compliance Purposes**

**Goal/Scenario #1**

**Background**: When a merchant applies for a credit card merchant account (that is, in order to be paid by customers via Visa, MasterCard or other popular methods), they must submit an application to a payment provider. “Payment provider” includes banks such as WellsFargo or Chase that are directly contracted with the credit card companies, and also includes downstream companies such as Vantiv or Elavon that are not banks but provide merchant accounts to merchants.

Before a payment provider can provide a merchant account to a merchant, they must verify that the merchant is not engaged in transaction laundering. Transaction laundering refers to a situation where an illicit merchant engaged in various types of illegal activity, such as illegal pharmaceutical sales, illegal gambling, child pornography, or other types of illegal or fraudulent activities, sets up a seemingly legal business selling shoes, books or some other innocuous product or service in order to obtain a merchant account under false pretenses. (If you’ve ever wondered, transaction laundering is what enables online criminals to obtain Visa, MasterCard and other credit card accounts.) The merchant account is granted to the merchant on the basis of the seemingly legitimate business, but then the illegal transactions are processed through the merchant account. (A real-life example of this is below.)

Payment providers must investigate (“underwrite”) the merchant that applied for a merchant account before granting a merchant account, and afterwards perform ongoing persistent monitoring of all merchants, usually through a third-party contractor. At present, there are seven companies, including LegitScript, certified by MasterCard as “Merchant Monitoring Solution Providers.” (Visa does not have a comparable program, but informally recognizes the same entities.) If a payment provider is found to have granted a merchant account to a merchant engaged in transaction laundering, the credit card networks can (and do) levy hundreds in thousands of dollars per transaction. Moreover, payment providers may be held civilly or criminally accountable by regulatory agencies (i.e., in the US, the FTC or others).

**Goal**: Conduct due diligence on a merchant, and persistently monitor a merchant, to determine whether it is engaged in transaction laundering by identifying the other domain names under the merchant’s control.

**Brief Format Use Case**

**Use Case:** **Queries for Compliance Purposes**

**Main Use Case:** Investigative analysis of the merchant website amishteacups.com, a website for a business submitted to a payment provider in order to obtain a merchant account. In order to evaluate whether the merchant may be engaged in transaction laundering, Whois data from all domain names in all zone files were analysed. In these cases, full and complete access to all Whois data elements currently available for all domain names on the Internet are necessary to adequately evaluate the likelihood of transaction laundering (i.e., in order to “reverse query” Whois data).

**Casual Format Use Case**

**Title:** amishteacups.com, buypuppiesonline.com

**Primary Actor:** LegitScript

**Other stakeholders:** Credit Card Networks (Visa, MasterCard, etc.); Banks; Payment Providers.

**Scope:** Initial steps utilized to confirm compliance of merchant account applicant.

**Level:** The user collects WHOIS information for the merchant account applicant, and performs reverse WHOIS queries to identify associated websites, individuals and organizations.

**Data Elements:** The initial step is to collect data from the WHOIS record of the domain name. The data collected includes the following:

IP Address

Registrar

Domain Creation Date

Name Server(s)

Registrant, Administrative, Technical, and Billing Data: Name (Individual), Organization Name, Address, Telephone Number, Fax Number, and Email Address

Mail servers

SOA record

**Story:**

LegitScript assessed the merchant URL amishteacups.com and buypuppiesonline.com (identical websites provided in a merchant application) to evaluate whether the merchant is involved in transaction laundering. In this case, we performed a reverse Whois query based on the Whois email address in the record for amishteacups.com, *karl636donasen1967(at)gmail.(dot)com*. Our reverse query of this email address established that the same email was used to register the following domain names:

* amishteacups.com
* australiamedsonline.com
* bestsirupshoponline.com
* buylaboratorysupplies.com
* delnaud-labs.com
* educationforchilden.com
* goldmedications.com
* k2bathsaltonline.com
* k2bathsaltsonline.com
* newlandmedication.com

Subsequently, a test buy from goldmedications.com established that the merchant descriptor was indeed the Amish Tea Cups business.

Without the ability to perform reverse WHOIS queries, it would not have been known that the website amishteacups.com is a transaction laundering website. Transaction laundering websites are specifically established to facilitate financial transactions for illicit products through a legitimate appearing website.

It should be noted that this is not an uncommon example: LegitScript and other compliance entities perform hundreds or even thousands of such evaluations each month. In this particular example, the Whois email was the factor that revealed transaction laundering, but any other field may be equally relevant depending on the merchant URL provided to the bank.

In this example, a few things are critical to note. First, this is a critical means of preventing fraud and illegal activity in the payments space. Second, this role is performed by private entities, not law enforcement or regulators. Third, access to a single domain name’s Whois record is not effective: only identifying all domain names registered with the same common data point revealed the transaction laundering.

This is one of numerous examples of how private industry has developed methodologies that allow successful prevention, disruption and dismantling of cybercrime, and the ability to freely access, collect, and perform reverse WHOIS queries is not only necessary, but is critical to protect unsuspecting consumers from performing financial transactions on websites engaged in transaction laundering, as well as prevent, identify, disrupt and dismantle cybercriminal networks.