Priceless: The Role of Payments in Abuse-advertised Goods

Damon McCoy, Hitesh Dharmdasani
George Mason University

Christian Kreibich
University of California, San Diego and International Computer Science Institute

Geoffrey M. Voelker and Stefan Savage
University of California, San Diego

ABSTRACT

Large-scale abusive advertising is a profit-driven endeavor. Without consumers purchasing spam-advertised Viagra, search-advertised counterfeit software or malware-advertised fake anti-virus, these campaigns could not be economically justified. Thus, in addition to the numerous efforts focused on identifying and blocking individual abusive advertising mechanisms, a parallel research direction has emerged focused on undermining the associated means of monetization: *payment networks*. In this paper we explain the complex role of payment processing in monetizing the modern affiliate program ecosystem and characterize the dynamics of these banking relationships over two years within the counterfeit pharmaceutical and software sectors. By opportunistically combining our own active purchasing data with contemporary disruption efforts by brand-holders and payment card networks, we gather the first empirical dataset concerning this approach. We discuss how well such payment interventions work, how abusive merchants respond in kind and the role that the payments ecosystem is likely to play in the future.

Categories and Subject Descriptors

K.4.1 [**Public Policy Issues**]: ABUSE AND CRIME INVOLVING COMPUTERS

Keywords

Security, Measurement,Economics

1. INTRODUCTION

E-mail spam, search spam, blog spam, social spam, malvertising and so on are all advertising mechanisms that exploit a lower cost structure (e.g., via botnets or compromised servers) to reach their audience. While a broad range of efforts focus on attacking these individual mechanisms directly, an alternative research agenda revolves around undermining the economics of the activity itself. In particular, as with all advertisers, the actors employing these abusive techniques are profit-seeking and only participate due to the promise of compensation (e.g., a typical pharmaceutical spammer is paid a 40% commission on the gross revenue of each sale they bring in). Thus, if these payments dried up, so too might the incentive to continue advertising.

In this paper we examine this question by focusing particularly on abusive advertising that is directly capitalized through consumer credit card payments (e.g., counterfeit goods such as pharmaceuticals [11] and some fraud scams such as fake anti-virus [15]). We are motivated in part by our previous work documenting that a small number of banks are implicated in handling credit card payments for the vast majority of spam-advertised goods [10]. In that paper, we hypothesized that interrupting those banking relationships might be an effective intervention for undermining such activity. However, at the time we lacked the data to evaluate this "payment intervention" theory; to the best of our knowledge, few such concerted actions were even being attempted. Over the last year, however, there has been significant adoption of this approach and we are now in a position to examine this question empirically.

Thus, in this paper, we advance our understanding of the role played by merchant banking and provide some of the first evidence about the efficacy of payment intervention. Our work makes three contributions in this vein:

- *Payment mechanics*. We explain the role of the existing consumer payment ecosystem in the monetization of abusive advertising by affiliate programs, the details of which are both critical and unfamiliar to much of the security community.
- *Account dynamics*. We empirically measure and characterize the relationship of 40 sponsoring affiliate programs with the banks and merchant accounts they use to monetize customer traffic and the role of such banks in this ecosystem over two years.
- *Bank intervention*. We opportunistically measure the impact of targeted efforts to terminate a subset of these merchant accounts and characterize the emerging structure of this conflict.

Overall, we find that reliable merchant banking is a scarce and critical resource that, when targeted carefully, is highly fragile to disruption. As a testament to this finding, we document the decimation of online credit-card financed counterfeit software sales due to

CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA.

a focused eradication effort. We further document how less carefully executed interventions, in the pharmaceutical sector, can also have serious (although less dramatic) impacts, including program closures, pursuit of riskier payment mechanisms, and reduced order conversions. Finally, we document the set of countermeasures being employed now by surviving merchants and discuss the resulting operational requirements for using payment intervention as an effective tool.

2. BACKGROUND

In this section we explain both the business structure of modern abuse-advertised goods as well as the structure of the payment card ecosystem and how the two integrate in practice.

2.1 Affiliate marketing

Since at least 2005, abuse-advertised goods and services have been dominated by a business model comprised of independent advertisers acting as free agents paid on a commission basis by the sponsors they shill for. This arrangement, frequently called the "affiliate program" model (or sometimes "partnerka"), has been highly successful—allowing botnet operators to focus on acquiring traffic (e.g., via spam or search), while sponsors handle the "back end" including software, fulfillment, customer service and payment processing. This relationship is well documented in the work of Samosseiko [14], Levchenko *et al.* [10], Stone-Gross *et al.* [15, 16], Kanich *et al.* [6], Leontiadis *et al.* [9] and McCoy *et al.* [11] among others.

Mechanically, the relationship works as follows: individual affiliates attempt to drive traffic to particular Web sites (e.g., through e-mail spam, search engine optimization, social network abuse, malware installed on the host, etc.). In some cases the domain names and Web sites are held and hosted by the affiliate program, but in other situations they are managed by the affiliate. Users who visit this site are greeted with a storefront typically designed by the affiliate program that provides a selection of products and a standard shopping cart interface (most affiliate programs provide a broad range of "templates" targeted towards different markets). If a customer selects products for purchase and then clicks on the "checkout" button, they are diverted to a "billing page" where they are asked to provide their name, address and payment credentials.

There are two kinds of billing pages provided in the industry: on-site and off-site. On-site billing pages are organically integrated in the Web site the customer visited, while offsite billing involves redirection to a different Web site (typically with domain names like "secure-billing.com"). In *both* cases however it is this external site, operated by the affiliate program, that accepts the billing information (the onsite billing "veneer" is typically implemented as an RPC-like protocol using PHP and forms). Thus, it is this point of accepting the billing information where the relationship with the customer is handed from the advertising affiliate to the sponsoring affiliate program.[1] Ultimately, it is the primary responsibility of the program to convert the latent demand attracted by its affiliate advertisers into concrete purchases; obtaining money from traffic.

2.2 Payment cards

In the retail environment purchases can be settled using cash, but online purchase transactions are typically executed via payment card networks such as provided by Visa, MasterCard and American Express. In one recent empirical study covering several years of transactions for a large online pharmacy, McCoy *et al.* [11] found that over 95% of all revenue was delivered via such networks.[2]

Thus, managing and maintaining reliable access to such payments is critical to all such business and ultimately provides the money (paid on a commission basis) that funds the creation of spam and SEO-focused botnets. In the remainder of this section, we provide an overview of how modern payment networks operate and, in particular, how they interact with online merchants such as those in our study.

The basic transaction

While a wide variety of payment card systems exists, we focus on Visa and MasterCard because they have by far the largest consumer footprint and ultimately are the networks by which all but a small fraction of abuse-driven advertising is monetized.

Visa and MasterCard are so-called "open loop" systems, because they implement multi-party payment networks that interconnect a range of distinct member banks. In particular, there are at least five parties in every such transaction: the cardholder, issuing bank, card association, acquiring bank, and merchant. The cardholder is the individual making a purchase who obtains a payment card (e.g., credit, debit, prepaid, etc.) via an issuing bank. The card number is structured into two key fields: a six-digit Bank Identification Number (BIN) that identifies the issuing bank of record and, typically, a 10-digit Primary Account Number (PAN) that identifies the cardholder's account (credit or debit) held by that bank.

To make a purchase, the cardholder provides their card number and associated personal information to a merchant (e.g., via an Internet form) and the merchant then passes this information, along with the price of the service, to their acquiring bank. This bank, sometimes also called the "merchant bank", then uses the card association network (e.g., VisaNet) to reach the issuer and requests an "authorization" for the amount specified (frequently in real-time) using a variant of the ISO 8583 protocol [4].

In considering whether to approve this transaction the issuer has available a range of features including the BIN of the merchant bank, the country of operation, the Merchant Category Code (MCC) of the merchant terminal (e.g., MCC 5912 is used for pharmaceuticals [18]), the size of the request, the amount of money available to the cardholder and so on. As well, the merchant may elect to pay for the Address Verification Service (AVS) that verifies if the street address and ZIP provided by the customer match that registered with the issuing bank.[3] If the authorization request is approved, then the money (or credit) is held at the issuer, the acquiring bank is notified (again via the card association network) and the acquiring bank informs the merchant that the purchase request is approved. On a longer time basis (e.g., 24 hours) a batch settlement transaction is used to make this request concrete and money is transferred from the cardholder's issuing bank to the merchant's acquiring bank.[4] Note that authorization does not imply settlement and the merchant is free to not complete the transaction (in which case the hold on

[1] Should the customer complete a sale the affiliate who delivered that customer is eventually paid a commission (typically 40% of gross revenue for pharmaceuticals, and a bit more for counterfeit software or fake anti-virus) via some separate payment mechanism (e.g., WebMoney or Liberty Reserve).

[2] A smaller number of transactions are completed using so-called "alternative payment" systems such as PayPal, as well as other money transfer vehicles such as Western Union or the ACH Network (i.e., eChecks), but these are a small part of consumer payments in Western countries.

[3] AVS is typically a bundled service implemented as part of authorization. However, it is possible to separate AVS from authorization and verify address data before issuing an authorization request.

[4] In some cases it is possible for the merchant to use a different BIN for authorization and settlement, but typically only when these belong to the same bank.

the authorization will eventually timeout and these funds will be available again to the cardholder).

In practice, however, there can be quite a bit more complexity than described above. In particular, while the issuing and acquiring banks are ultimately responsible for the transactions made in their name, they will frequently outsource the actual "processing" of transactions to a third party (e.g., First Data). Moreover, while some banks will market accounts directly to merchants, in many cases this is commonly performed by an Independent Sales Organization (ISO) who is sponsored by one or more acquiring banks and may largely "own" the merchant relationship.[5]

High-risk accounts

In all cases, the acquiring bank still holds liability on any transactions (e.g., due to chargebacks from unhappy consumers). Thus, merchant accounts (whether direct or through an ISO) must be underwritten by the bank against the merchant's risk profile (i.e., the likelihood of fraud, fine assessment and charge-backs).

Some businesses are considered inherently high-risk (e.g., online pharmaceuticals, pornography, multi-level marketing, etc.) and many banks may refuse to underwrite such businesses entirely. Those that do will charge much higher transaction fees, and may demand up-front money, transaction "holdbacks" and a documented history of high turnover with low charge-back rates.

Another approach for such merchants (as well as for "startups" without significant processing history) is to use what is called "third-party processing" or aggregation. For example, Visa provides a program for Payment Service Providers (PSPs) who can contract with an acquiring bank to provide payment services *on behalf* of merchants contracted directly with the PSP. In principal, PSPs comply with Visa rules, and thus they will only be able to aggregate high-risk client transactions with acquiring banks who are agreeable.

However, a less benign form of aggregation, sometimes called "factoring", occurs when a merchant or ISO resells access to an existing merchant account with an acquiring bank and launders transactions from multiple merchants through this account (clients who may in fact be in a different line of business or risk category). In extreme cases, a criminal ISO might register a slew of shell companies with one or more banks (sometimes working directly with a bank, sometimes working with a merchant account broker) and then sell a payment processing service that launders transactions through this network of shell accounts. In practice, all these and many other combinations of relationships exist (and different rules can apply in different operating regions as well), but the underlying five-party transaction is consistent across all embodiments.

Merchant costs

From the merchant's point of view, the goal is to obtain the lowest overhead and highest reliability they can in their risk class. Overhead is described in terms of the *discount rate* charged by the service provider in exchange for processing services and is a percentage charged against all revenue. Thus, while a low-risk retail merchant processing cards at the point of sale might be able to find an ISO willing to provide service for a discount rate of under 2%, a third-party aggregator catering to high-risk clients might charge 10% or more. Providers will frequently have different discount rate structures for different kinds of transactions based on their risk profile, but in the high-risk category it is common to ignore these distinctions. In addition to the discount rate, the merchant typically pays monthly fees (e.g., for access to an Internet-based payment gateway, for individual virtual terminals for entering card numbers, etc.) plus per-transaction fees (up to $2 in the high-risk category).

As well, providers differ in how quickly they make payments available to merchants and in the high-risk category most will "hold back" a percentage of revenue as a residual hedge against future liability. These holdbacks are particularly important since most card associations allow cardholders to contest a transaction many months after settlement and if a merchant "disappears" the acquiring bank is responsible for the cost of this chargeback and the associated fees. Thus, it is common practice for high-risk account providers to hold back 10% of revenue for between 90 to 180 days to cover unforeseen losses. The provider in turn can use this money to cover any fines or assessments and, should there be a complaint of criminality, a merchant can stand to lose this sum entirely.

Thus, a merchant must also be careful to minimize the number of chargebacks (both for the chargeback fees incurred as well as the additional scrutiny imposed on accounts with high chargeback rates). For example, in a recent study of several fake anti-virus programs, Stone-Gross *et al.* document how refund requests are manipulated to keep the monthly chargeback rate underneath "trigger" levels [15]. As well, sellers of goods must be careful to filter out fraudulent customers and thus even merchants selling strictly illegal goods such as counterfeit software will employ sophisticated fraud screening before processing a payment.[6]

2.3 Payment interventions

In our 2011 paper on the spam value chain, we empirically documented that for many of the most popular spam-advertised market niches (pharmaceuticals, replica luxury goods and counterfeit software) payments were handled by a small number of acquiring banks (just three were used to monetize the sites advertised by over 95% of spam e-mails in the study [10]). This concentration, in addition to the small number of acquirers accepting high-risk merchants, the long setup time for new banking relationships, and the liability on revenue holdback, makes the payment tier an attractive target for those seeking to combat such actions. To wit: a miscreant can replace a suspended domain name within minutes at a cost of a few dollars, but if a banking relationship is shuttered they may lose hundreds of thousands of dollars in holdback and spend weeks developing a suitable replacement. This observation has been internalized and made independently by a number of stakeholders, culminating in a series of commercial interventions that motivate this paper.

Regulatory tightening

Effective in June of 2011, Visa made a series of changes to their operating regulations in support of their Global Brand Protection Program (GBPP) that seem designed to specifically target on-line pharmacies and sellers of counterfeit goods. First, pharmaceutical-related MCC's (5122 and 5912) were explicitly classified as "high risk" (along with gambling and various kinds of direct marketing services), acquirers issuing new contracts for high-risk e-commerce merchants required significant due diligence (including $100M in equity capital and good standing in risk management programs) and, starting in December 2011, additional registration of PSPs and ISOs dealing in high-risk products and services. As well, the new documents explicitly call out examples of illegal transactions including "Unlawful sale of prescription drugs" and "Sale of coun-

[5]In some cases, the acquiring bank may even "rent" BINs to a large ISO (so-called super-ISOs) who then act as de facto acquirers.

[6]This screening includes matching geo-located consumer IP address, shipping address and credit card address, profiling on e-mail address, country of access and so on (see [5] for one treatment of these issues). In our experience, the most common fraud scoring software among such shops is that provided by MaxMind.

terfeit or trademark-infringing products or services", among others [17]. Finally, these changes include a more aggressive fine schedule and, implicitly, represent a statement of more aggressive enforcement actions to be forthcoming.

Targeted complaints

As per the above regulations (and similar regulations at MasterCard), acquiring banks in violation of these rules can be subject to a range of fines (greatly increased in the new GBPP, and increasing with each additional round of violations). As the ultimate threat, non-compliant banks, ISOs and PSPs could have their ability to issue merchant accounts and services taken away completely.

At roughly the same time (mid to late 2010), a series of negotiations between brand holders, payment providers and the White House's Intellectual Property Enforcement Coordinator established agreements to streamline targeted actions against merchant accounts used to monetize counterfeit goods and services [1, 7]. Through this effort, individual brand holders can submit evidence of infringement (e.g., from undercover purchases of their products placed via online sites) to the card networks, who then identify the associated acquiring bank and request remediation (on penalty of fines and further action for continued or additional non-compliance). Moreover, in addition to the independent actions of brand holders, the International Anti-Counterfeiting Coalition (IACC) announced a larger-scale initiative in September of 2011 [3, 13]. This program, open to all IACC members, provides a standard portal by which brandholders can report infringing e-commerce sites. IACC, with their contractors and the card networks, implements the legwork of identifying merchant accounts used to monetize reported sites and managing the formal complaint process through the card networks.

In the remainder of this paper, we characterize the longitudinal relation between affiliate programs and their acquiring banks as well as the impact of the interventions discussed above—both in the large and in individual campaigns diligently driven by specific brand holders.

3. METHODOLOGY

Our work builds on our previous efforts in Levchenko *et al.* [10], in which we actively identified the acquiring banks used to process consumer orders from Web sites sponsored by particular affiliate programs. This task thus comprises two parts: affiliate program identification and payment tracking.

In contrast to this previous work, we are not concerned with automatically classifying arbitrary Web pages and thus it is sufficient for us to identify a small number of reference sites sponsored by each program.[7] While there is still no "silver bullet" approach for identifying such sites, the combination of our own domain knowledge and the open nature of most affiliate programs substantially helped our efforts. For each program identified in Levchenko *et al.*, we already have a long list of reference sites as well as a handcrafted classifier for identifying the template structure of the sites advertised by each program [10].[8] We also identified a number of new programs by monitoring underground forums [12], since new programs must advertise to acquire new affiliates [11]. From these we then identified representative sites either from forum-documented "public" sites or by joining the program as an affiliate (and thus obtaining reference templates that can be matched against search or spam-advertised sites). Finally, we benefit from the efforts of independent researchers such as XyliBox [19] and members of the criminal and civil investigations community who have shared data with us on request. Taken together, we were able to identify 40 different programs (25 focused on pharmaceutical sales and 15 on the sale of counterfeit "OEM" software). We try to use the "official" names for each program, but when we could not make this determination we instead use the most predominant storefront "brand" advertised as a proxy.

Having obtained these representative sites, we are next interested in tying the affiliate program to a particular acquiring bank at a particular point in time. Here too we continue the approach of Levchenko *et al.*, where we placed 76 credit card purchases over three months and then worked with the issuing bank to identify the individual acquirers used in each transaction. We build on this dataset working in partnership with multiple payment card issuing institutions who have provided us with full transactional data for each purchase. Thus, in addition to the Bank Identification Number (BIN) for the acquiring institution on both authorization and settlement, we also receive the textual order descriptor, the Card Acceptor ID (an acquirer-unique identifier for the merchant) and the country in which the acquirer resides (among other quantities). We follow closely the operational guidelines outlined in Kanich *et al.* [5] for successfully placing such orders (e.g., distinct IP addresses, geo-located to match shipping address, geo-located to match distinct phone numbers, etc.).[9]

For this paper, we focus on a subset of this dataset comprising pharmaceutical and OEM software affiliate programs.[10] Together, this combined dataset includes 676 ordering attempts, of which 429 were successful, covering over two years of activity. Table 1 lists the affiliate programs we engaged with and our purchasing activity with them.

Our dataset has a number of limitations, which we make clear here. First, all of our orders (both the original 76 from Levchenko *et al.* and the subsequent purchases) are obtained using the Visa card network. Thus, our results do not capture information relating to the other major open loop card player, MasterCard. However, for reasons that are not completely clear, MasterCard merchant accounts appear much harder to obtain for pharmaceutical affiliates [11]. Indeed, at any given point in time only a small minority of the programs we studied had working MasterCard processing available. The second major limitation is that our samples are neither uniform nor do they always cover the same period of time. In particular, we did not start our recent study for some time after the original 76 purchases and thus there is a large gap between roughly April of 2011 and August of 2011 during which few orders were placed. Similarly, we examine a number of additional programs for which we, by definition, have no prior history. As well, while we attempted to place orders at least once a month for each program, this was not always possible due to the operational complexities of obtaining new credit cards, IP addresses and phone numbers as

[7] In principle, one might be concerned that different sites advertising the same program might process payments differently, but multiple studies confirm that the affiliate program sponsor centralizes payment handling in such arrangements [6, 10, 11].

[8] For example, trustedtablets-online.com is a well-known site belonging to the RXPartners affiliate program, identified by name on its affiliate forum, but also via a range of features including the brand name (trusted tablets), the phone support numbers, structural elements in the HTML code, the live-support referrer fields, the structure of its cookies and its offsite billing page (checkoutpage-secure.com) among others.

[9] Our purchasing activity has been explicitly reviewed and approved by our institution and we believe that the value of our work outweighs the relatively minor ethical concerns resulting from the small financial support provided to these programs through the few thousand dollars worth of our purchases.

[10] We also explored a range of fake anti-virus and replica goods programs, but with insufficient fidelity to include in this analysis.

well as churn in program sites and temporary interruptions in processing. Finally, as we will describe later, it is clear that a subset of the programs have become far better at counter-intelligence on such undercover purchases and thus some subset of our refusals may not be due to true payment processing problems but an active attempt to "blind" such measurements.

In addition to our own ordering data set, we also have the benefit of third-party information as well. In particular, we became aware of targeted complaint activity driven by particular brand holders starting in November of 2011. In a large number of these instances we have been able to obtain key information (combining data from brand holders and financial services) about when particular complaints were made—providing an empirical basis for a natural experiment examining the impact of these payment-oriented interventions. We present a subset of this data, consisting of roughly 170 complaints against the merchant accounts of over 25 distinct affiliate programs.

Finally, we also obtained qualitative data by continuously monitoring related underground forums focused on the pharmaceutical and OEM software niches, as well as the affiliate "news" pages for roughly a dozen of the programs that we joined. These sources allowed us to capture anecdotal reports both from individual affiliates concerning their revenue impact and from affiliate program managers who would inform their affiliates about the challenges that they were experiencing. Thus, this data provides a form of validity check on the conclusions we reach from analyzing the empirical purchasing and complaint data alone.

4. ANALYSIS

Using the data we have described, we now examine how affiliate programs rely upon the global banking infrastructure to process payment card transactions. Specifically, we examine which banks are used to support these activities over time, how the affiliate programs are distributed and concentrated among the banks, the strategies that the programs employ in using banking resources while balancing risk and overhead, and how the programs react to pressure such as active takedown interventions.

4.1 Aggregate bank activity

In aggregate, we executed 429 orders from 25 pharmaceutical and 15 software affiliate programs. These in turn were processed through 30 acquiring banks: 25 distinct banks processing for pharmaceutical programs, 15 banks processing for software programs, and 10 banks processing for both. Five of the banks we saw only processed one or two purchases in less than a month, and appear to be banks that the affiliate programs used on a trial basis but where the business relationship was not successful.[11] Discounting these banks, we found 25 banks supporting the card processing activities of the 40 programs combined.

Examining how these banks are used over time reveals some interesting dynamics. Figure 1 shows the set of banks processing Visa payment transactions for the affiliate programs we purchased from over two years: one graph for pharmaceutical programs, the other for OEM software. Each row corresponds to a bank and each point on a row corresponds to a purchase from an affiliate program that authorized using that bank; the parenthetical number next to the bank name denotes the number of purchases that bank processed. We display the rows of banks in increasing time order of appearance in our data set. Finally, the lines show our estimate of when a bank is actively engaged in supporting affiliate programs. We connect points on a row with a line if successive purchases from any program used the same bank within two months (this cutoff is somewhat arbitrary, but is responsive to our typical purchasing interval of one month). For larger time periods, we assume that a given bank is not being used by the program. In reality, either we did not make purchases from programs using the bank, or programs stopped using the bank during that time; we do not have the observations to distinguish.

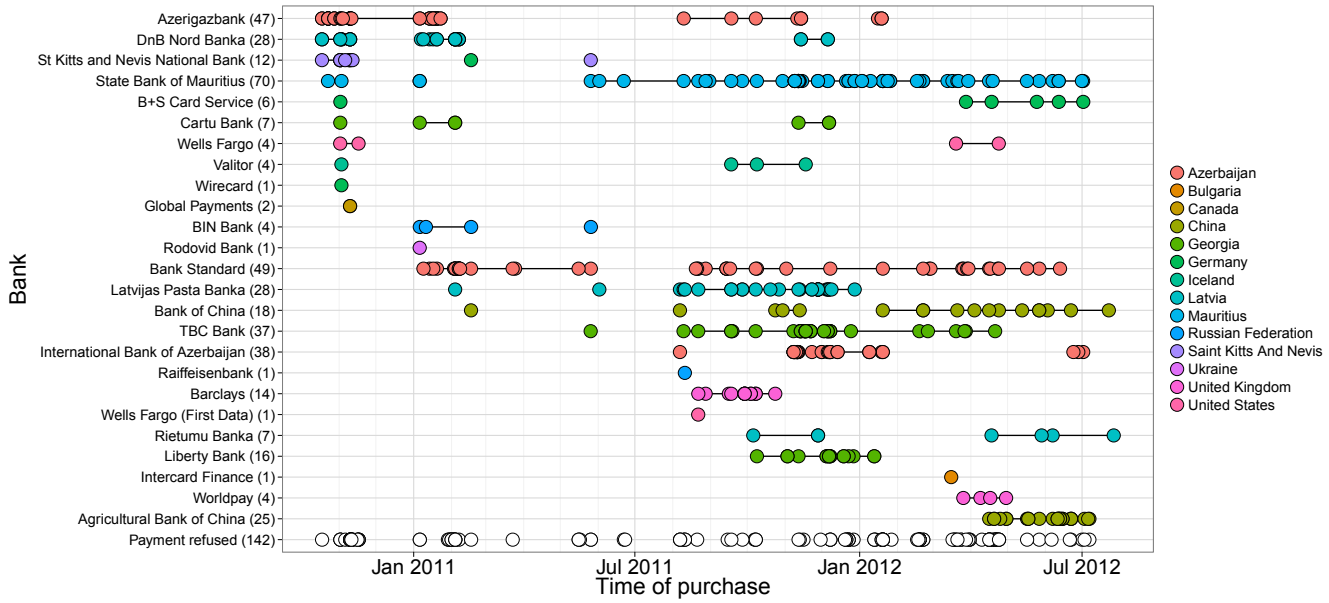
[11]This is consistent with McCoy *et al.*'s observation that while the Glavmed affiliate program contracted with a range of payment service providers, many of them were unable to provide reliable service and were only used briefly [11].

Pharmacy		*Software*	
Affiliate	*Auths* : *Refs*	*Affiliate*	*Auths* : *Refs*
33Drugs	24 : 3	BuyCheap OEM*	3 : 0
4Rx	8 : 1	CD OEM*	12 : 0
CashAdmin	3 : 4	ChineseOEM Keys*	2 : 1
Club-First	13 : 5	down.cd*	1 : 0
DrBucks	5 : 5	EuroSoft*	37 : 16
Eva	12 : 18	genuineOEM*	1 : 1
Glavmed	28 : 10	OEMCash	4 : 0
Greenline*	11 : 5	OEMPay	4 : 7
Mailien	16 : 11	OEM Soft Store*	6 : 1
MedInc	7 : 5	omegaBidSoft*	19 : 4
Meds Partners	12 : 0	Royal/Quality Soft.*	16 : 17
Online Pharm.*	21 : 11	Soft Sales*	22 : 19
OXOPharm	6 : 1	The Software Sellers	1 : 24
PharmCash	10 : 7	topOEM*	1 : 2
PH Online*	8 : 4	Zinester	1 : 13
Private Partners	7 : 3		
Rx-Affiliate Net.	14 : 0		
RxCash	8 : 4		
RxCashCow	8 : 4		
Rx-Partners	10 : 9		
Rx-Promotion	20 : 8		
Stimul Cash	9 : 5		
World Pharm.*	6 : 2		
Zed (Herbal)	27 : 9		
Zed (Pharma)	6 : 8		
Total	299 : 142	Total	130 : 105

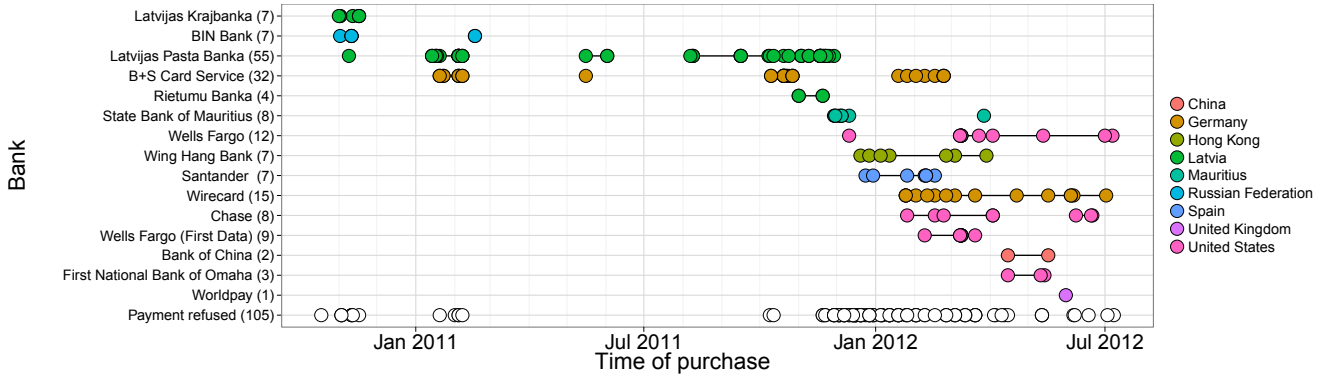
Table 1: Summary of order data set for pharmaceutical and OEM software affiliate programs. Each program shows the number of successful authorizations ("Auths") vs. the number of orders that were refused *before* authorization ("Refs"). *These affiliate programs are named for the most popular storefront "brand", not their official names.

For the pharmaceutical affiliate programs in Figure 1(a), we see that activity is concentrated in a relatively small number of banks. When purchasing from all of the affiliate programs, most of the purchases go through just twelve banks with the remaining banks processing fewer than ten purchases. Further, the set of concentrated banks shifts over time. In the first half of our data set affiliate programs concentrate credit card processing in Azerigazbank and Bank Standard in Azerbaijan and DnB Nord Banka in Latvia. However, in mid-February of 2011 DnB Nord Banka terminates virtually all such merchant accounts (the parent company DnB Nord released this statement, "We bought a bank this winter which a customer engaged in spam activity. This company is no longer one of our customers." [2]), and Azerigazbank is used far less frequently after being identified in [10].

In the second half, credit card processing continues with Bank Standard but otherwise shifts to Latvijas Pasta Banka, the State Bank of Mauritius and two Georgian banks, TBC and Liberty. In the past few months processing shifts from Bank Standard to the International Bank of Azerbaijan and some programs move from the



(a) Pharmaceutical programs



(b) Software (OEM) programs

Figure 1: Bank processing purchases over time for (a) pharmaceutical affiliate programs and (b) software (OEM) affiliate programs. Solid dots denote successful purchases processed through a bank. Open dots denote orders where our orders were refused. Numbers in parentheses at the end of bank names denote the number of purchases processed by the banks.

State Bank of Mauritius to two Chinese banks, the Bank of China and the Agricultural Bank of China. For banks such as Global Payments, Rodovid, Raffeisenbank, Intercard, and Wirecard, we see them processing credit cards for just one or two purchases at one point in time. Again, we suspect that these represent situations where affiliate programs were experimenting with new banks for credit card processing, but the bank relationship did not succeed.

Bank activity for software affiliate programs shows similar behavior, yet is even more pronounced than with pharmaceuticals. Initially just four banks handle processing for purchases from 13 software programs: Latvijas Pasta Banka, Latvijas Krajbanka, BIN Bank, and B+S Card Service. In late November 2011, though, we see processing gradually expand to eleven new banks, with three of the old banks having disappeared completely (Latvijas Pasta Banka, Latvijas Krajbanka, and BIN Bank). This sudden change corresponds to two unrelated events. First, Latvijas Krajbanka became embroiled in a major Baltic banking crisis caused by the nationalization of Bankas Snoras (due to massive fraud). Second, at roughly the same time, a major software manufacturer executed a comprehensive series of targeted complaints against merchant accounts used to receive payment for online counterfeit software sales. This campaign is ultimately very successful, corroborated by the large number of payment refusals we see starting at this time period as well (explained in more detail in Section 4.4).

4.2 How programs use banks

In the previous analysis, we collapsed all affiliate programs together. Next we examine the dynamics of these relationships: how distinct programs are distributed and concentrated among the banks, and how these relationships change over time.

As per Section 2.2, there can be a number of relationships between an affiliate program and the merchant account receiving its Visa transactions. In most cases a given merchant account, as represented by the merchant ID, is uniquely used by a given program. For example, the 33Drugs program (aka DrugRevenue) uniquely used a particular account (3755600) with the Latvian bank Pasta Banka for over a year, an account with the merchant descriptor "33medscom1877340891".

There are a small number of cases in which different programs may share accounts—either because they are really are co-owned, or because they use a third-party payment processor who factors their purchases through a set of managed accounts. We have seen

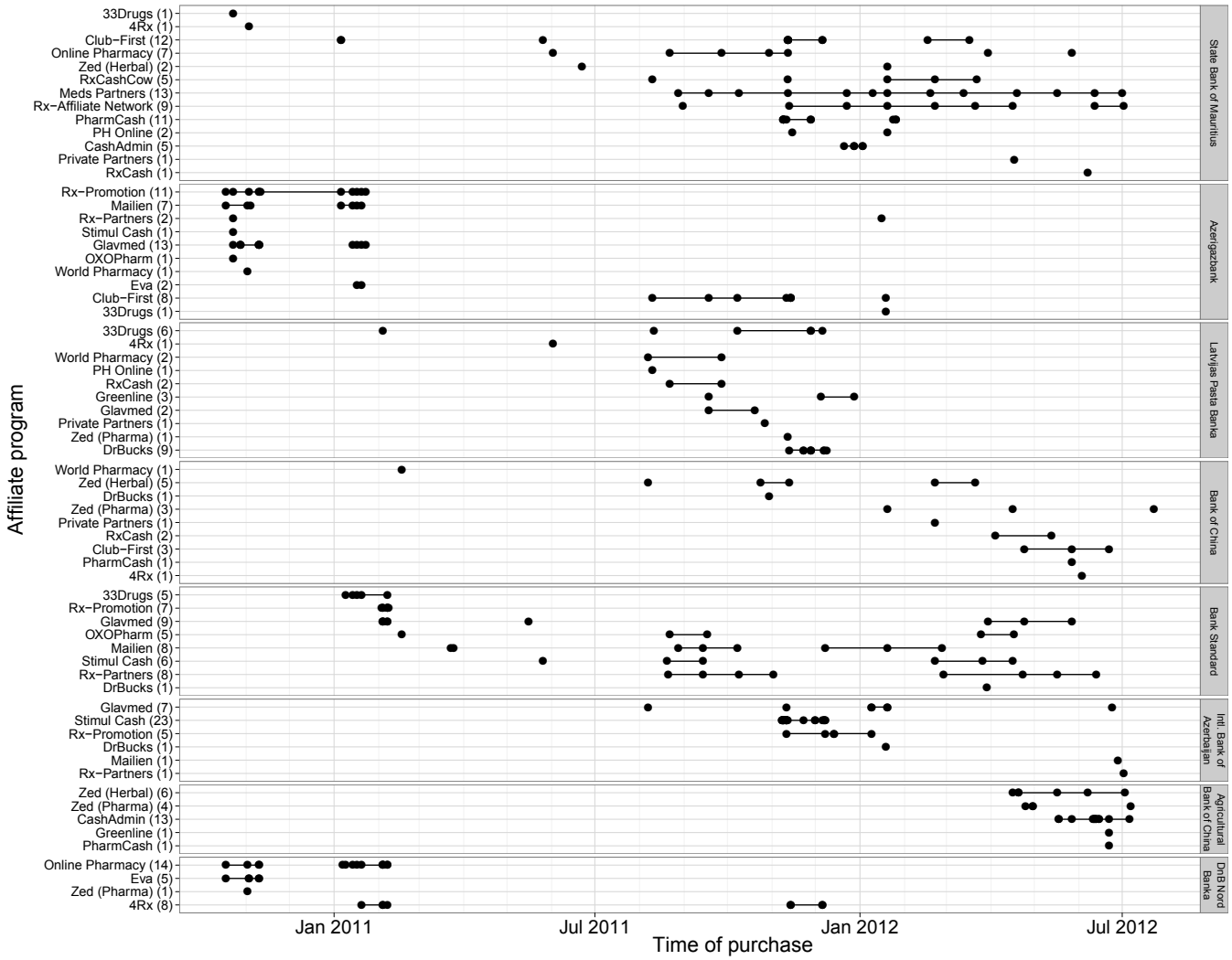


Figure 2: Breakdown of pharmaceutical programs associated with heavily used banks. Numbers in parentheses after program names denote the number of purchases made through that program that were processed by that bank.

examples of both behaviors. For example, the Rx-Partners and Stimul-cash programs consistently use the same accounts over the entire duration of our study. The reason for this sharing is that the Stimul-cash program was acquired by the owners of Rx-Partners (roughly in 2008) and thus shares back-end processing.[12] Conversely, we see a large number of distinct OEM software affiliate programs using the same accounts at Pasta Banka in early 2011, but using different accounts at other periods (suggesting a shared third-party payment provider during the time of sharing).[13]

With this in mind, Figure 2 expands the data shown in Figure 1(a) by identifying which affiliate programs processed payments using the various banks: for each bank we include a row for each affiliate program that used its services for acquiring. Note that many programs used multiple banks over time, and so rows for the same program appear under multiple banks (behavior we explore further in Section 4.3). Once again, we connect points with a line if successive purchases occured within a two-month window to suggest continuous support by a bank for that program. For instance, we placed 13 orders from sites sponsored by Meds Partners between July 2011 and July 2012 that were processed through the State Bank of Mauritius; these purchases are shown as a line connecting three points on the Meds Partners row for that bank. Finally, we sort the banks in decreasing order of the number of programs that use a bank, and only show banks used by at least four programs.

Here we see the coordinated movements that explain some of the previous changes in bank "popularity". For example, a series of programs including most of the biggest players—Rx-Partners, Stimul-cash, OXOPharm, Mailien, Glavmed and Rx-Promotion—all transfer in February of 2011 from processing payments through Azerigazbank to Bank Standard, and move again within Baku to the International Bank of Azerbaijan for periods in late 2011. This level of synchronicity suggests the use of a shared payment provider among these actors. Conversely, there are particular programs that

[12]However, less obviously, the OXOPharm affiliate program *also* shares the same accounts. This could be because the three share a payment provider or because there is some undisclosed business relationship between the two.

[13]We also find short-lived sharing arrangements indicative of shared third-party processing between Glavmed and World Pharmacy (Azerigazbank), Glavmed and Dr. Bucks (Bank Standard and International Bank of Azerbaijan), Private-partners and RxCash (Liberty Bank), ZedCash and Stevna (Pasta Banka), CashAdmin, Greenline and PharmCash (Agricultural Bank of China), as well as Greenline and and TopOEM (Wells Fargo).

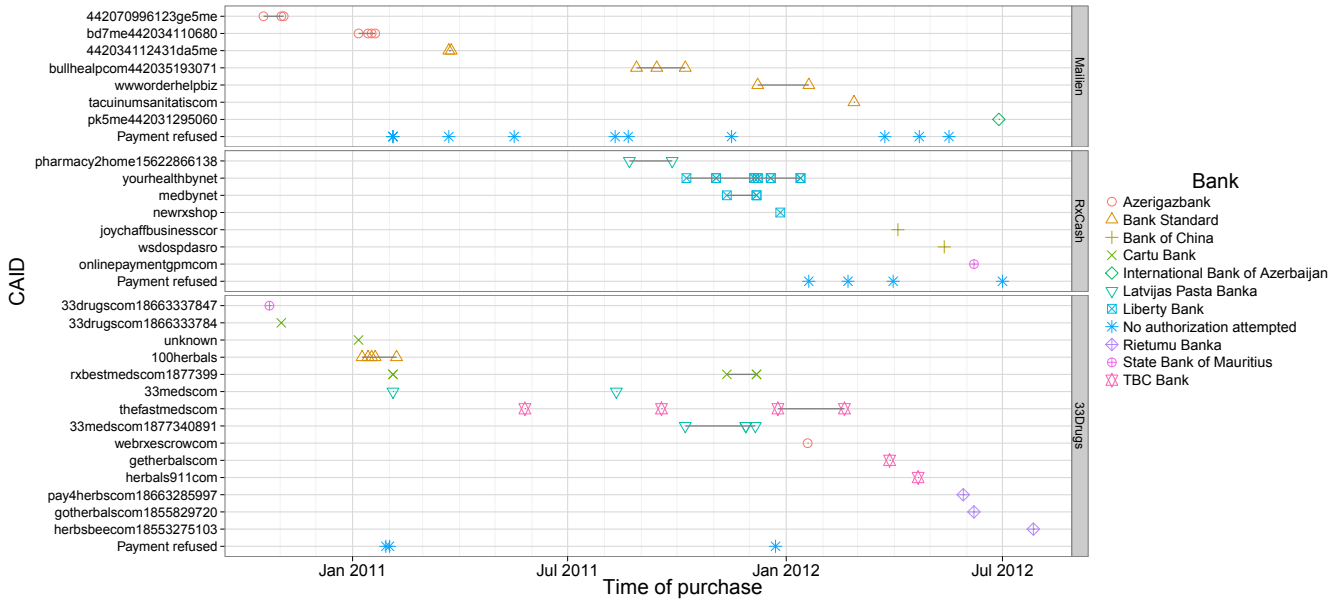


Figure 3: Various strategies affiliate programs use for processing card payments at banks: one terminal at a bank at a time (Mailien), multiple terminals at one bank simultaneously (RxCash), terminals at multiple banks simultaneously (33Drugs).

establish unique relationships with banks, such as ZedCash which moves all of its processing (including replica and herbal sales) to Bank of China and Agricultural Bank of China with whom it continues to operate today. Finally, State Bank of Mauritius and the two Georgian banks, TBC and Libery, come to dominate the "mid-tier" of pharmaceutical programs starting in roughly August of 2011.

For software affiliate programs (graph not shown), we found that most programs process orders simultaneously through four banks (again suggesting a shared third-party processor) until November 2011 when the programs all scramble to find alternate payment arrangements (Sections 4.4 and 4.5).

4.3 Program banking strategies

Programs use different strategies for managing payment processing that vary in terms of overhead and risk management. Figure 3 shows examples of four strategies among pharmaceutical programs. For each program, we show rows corresponding to individual merchant descriptors (text strings that are provided to the issuer and would appear on the customer's payment card statement) used to process the credit cards for the orders we placed through the program. Each merchant descriptor corresponds to a "terminal", a specific merchant account at a bank tied to processing orders with a specific merchant category code (MCC).[14] We plot points on a row for the purchases we made that were processed using that specific terminal. Since each terminal is tied to a specific bank, we mark points on a row that identify the bank the terminal is associated with. Rows for a program with the same mark indicates that we observed a program using multiple terminals at a bank, and rows with different marks indicate that a program uses multiple banks. As before, we draw a line between purchases processed using the same terminal if they appear within two months of each other. When appropriate, on a separate row for each program we also show points when we attempted purchases from the program but the merchant rejected our order (i.e., did not attempt to authorize our card).

[14]Technically, identical descriptors could be used for different accounts, but since we have access to the CAID information we can ensure that each of these corresponds to a unique merchant ID.

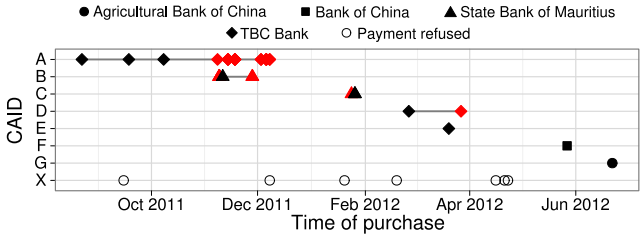


Figure 4: Example of a program receiving complaints to a card network. Rows denote distinct merchant descriptors; row "X" shows refused orders.

Some programs like Mailien use a single terminal at a bank at a time, only switching when forced to. Staying with one bank minimizes the cost and overhead of establishing merchant accounts with another bank, but leaves the affiliate program open to the risk of losing all processing capability if the bank terminates their relationship. For example, when Azerigazbank globally stops processing for these kinds of merchants, Mailien switches to Bank Standard and uses single terminals serially over time. As per the previous description of risk, it is precisely during these times when Mailien is switching between banks or merchant accounts at a bank that our orders are unable to be processed.

To further reduce risk, other programs use multiple terminals at a bank simultaneously. When RxCash processes cards through Liberty Bank, for example, it appears as if it is using at least two terminals at a time on two different occasions.

Finally, some programs like 33Drugs maintain simultaneous relationships at multiple banks at a time. Between July 2011 and January 2012, our purchases are processed through four different banks on existing terminals that we had originally seen used in early 2011. Maintaining active merchant accounts at multiple banks simultaneously has both cost and time overheads associated with it, but it also reduces risk since the program is not dependent on a single bank for processing cards and it gives the program flexibility in

routing orders to different banks (e.g., to balance processing load, adjust to bursts of chargebacks through particular banks, etc.).

4.4 Payment under pressure

As a rule, any payment relationship takes time and money. If a payment mechanism is working smoothly there is little reason to change it. Thus, absent outside forces acting, we would expect that an affiliate program (or a third-party processor acting on their behalf) would prefer to use a single merchant account for as long as possible.[15] Conversely, if a merchant account disappears (i.e., this account is never again used to receive payment for orders placed with the same affiliate program) this suggests that the account was closed due to some external pressure. This pressure could include high charge-back rates, the bank getting nervous, changes in payment service provider and so on. However, we are most interested in the role played by targeted pressure: the extent to which interventions in the payment ecosystem can be effective.

Serendipitously, there have been a range of such actions over the last year which present an opportunity to directly measure the effectiveness of this class of intervention. Moreover, we have obtained data about the precise accounts targeted and the time at which these complaints were delivered, providing us with an empirical basis for evaluating outcomes.

As one example of this activity, Figure 4 shows the merchant descriptors (anonymized by request) used by the PharmCash program over time. The black points are product purchases made by our group, while the red points denote orders made by an affected brandholder used to generate complaints to the card association. PharmCash, a modest-sized pharma affiliate program, initially had two terminals, one with the State Bank of Mauritius and the other with TBC Bank. Complaints occured in mid-November 2011 identifying both terminals, and within two months we no longer see those terminals being used (note that this is an outlier in our dataset and in all but a handful of cases a terminal "disappears" within 30 days of a complaint being delivered). Shortly thereafter, we see PharmCash using two *new* terminals, one at each bank. Another round of complaints appears to terminate both of these terminals and PharmCash opens yet two more terminals at the Bank of China and Agricultural Bank of China.

Taking into account the "takedown" complaint data set, we do find encouraging evidence that such financial takedowns are effective. As a broad analysis, we examine what happens with purchases to an affiliate program after each of its merchant descriptors becomes inactive, i.e., we no longer see the merchant descriptor processing purchases in our data set. After a merchant descriptor becomes inactive, there are five possible outcomes for the next purchase to the affiliate program: the purchase is processed on (1) another "old" descriptor we had seen before at the same bank; (2) a new descriptor at the same bank; (3) an old descriptor at a new bank; (4) a new descriptor at a different bank; or, (5) we have no further successful purchases through the affiliate program. Note that the data is right-censored, particularly for very recent purchases, due to our definition of "inactive". Although we believe the analysis accurately reflects both our experiences and reports from affiliate programs themselves, continued purchasing (which we are doing) will further solidify the results.

Table 2 shows the breakdown of merchant descriptors for the entire data set that fall into these five possible outcomes, with a row showing the number and percent of merchant descriptors with a particular outcome. For comparison, we separate the merchant descriptors into those where complaint purchases were not made (185) and those where complaints were made (48). We also further break them down by product category. As an example, among merchant descriptors used by pharmaceutical affiliate programs that received no complaints, in 17 cases subsequent purchases to those programs used a merchant descriptor we had seen before at the same bank.

Broadly speaking, complaints are highly correlated with programs moving processing to new banks or halting processing altogether. Looking at the "Combined" column for descriptors that had no complaints, we see that 36% of subsequent purchases were processed on (old or new) descriptors at the same bank, while only 18% of subsequent purchases were not successful. In contrast, only 11% of subsequent purchases to programs that received complaints were processed on descriptors at the same bank, while 69% were processed on descriptors at a new bank and nearly 21% of subsequent purchases were not successful. Note that even when processing is not completely curtailed, forcing a move to a new bank can cause significant losses due to both opportunity cost during the switching period and the likely forfeiture of holdbacks at the bank they leave (which in many cases can be in excess of $1M).

4.5 Qualitative assessments

Note that the effect of complaints in this data are particularly dramatic for software programs, where purchases on descriptors after complaints nearly always went to either a new descriptor at a new bank or were unsuccessful: programs clearly had to scramble to find processing at new banks if at all. We believe that one reason this campaign was so successful is that it targeted all OEM software programs and aggressively pursued each new account they obtained—effectively promising that any new banking relationship they created would swiftly be ruined. Even those specializing in high-risk processing would have no interest in taking such a client.

We also have strong qualitative evidence of this efficacy (with two exceptions we explain in the next section). In a number of these cases we had access to affiliates operating inside the program and announcements of payment processing problems were distributed to them. Wrote the operators of OEMPay in late November 2011 (translated from the Russian), "Starting today our bank has stopped working. Due to this, we have made the decision to close our affiliate program for the duration of our search for new processing. We ask you to remove your traffic and for your understanding in view of the situation". Similarly, we had access to a number of Russian-speaking underground forums in which the OEM software business was discussed. Wrote one participant (again translated from Russian), "The sun is setting on the OEM era" and one week later, "All OEM affiliate programs have closed".

While the pharmaceutical complaints are not yet as comprehensive, this is undoubtedly because the space is larger, more sophisticated and more profitable. Even still there is significant concern among those working with such programs as well. Wrote one eloquent affiliate in March of this year, "Right now most affiliate eprograms have a mass of declines, cancels and pendings, and it doesn't depend much on the program IMHO, there is a general sad picture, fucking Visa is burning us with napalm."

5. ECOSYSTEM RESPONSE

No intervention exists in a vacuum and undermining the payment ecosystem is no different. We have witnessed a range of responses to pressure against payment processing and, while we are not in a position to place these countermeasures on a comprehensive quantitative footing, we have more than enough qualitative experience to identify several broad classes of behaviors. In this section we

[15]To wit, one of the authors recently placed an order from Amazon, which processed the order using the same merchant account as an order placed two years ago.

Outcome		No Complaints			Complaints		
		Pharma	Software	Combined	Pharma	Software	Combined
Same bank	Old descriptor	17 (12%)	3 (6.8%)	20 (11%)	2 (6.3%)	1 (6.3%)	3 (6.3%)
	New descriptor	32 (23%)	15 (34%)	47 (25%)	1 (3.1%)	1 (6.3%)	2 (4.2%)
New bank	Old descriptor	15 (11%)	5 (11%)	20 (11%)	9 (28%)	4 (25%)	13 (27%)
	New descriptor	51 (36%)	13 (30%)	64 (35%)	16 (50%)	4 (25%)	20 (42%)
No successful purchases		26 (18%)	8 (18%)	34 (18%)	4 (13%)	6 (38%)	10 (21%)

Table 2: Outcomes of subsequent purchases to affiliate programs after a merchant descriptor becomes inactive for descriptors that do not receive a complaint (left) and those that do (right).

describe these actions concretely followed by a broader discussion about the nature of this conflict going forward.

5.1 Order filtering

Since it is ultimately brandholders and their contractors driving many of these targeted actions, affiliate programs can reduce their risk by reducing their customer footprint. In particular, if they can prevent an undercover buy from producing an authorization then there is no way to tie a Web site selling brand-infringing goods to the merchant account (and hence bank) normally used to process its payments. While there is no perfect way to filter out undercover buys (any more than there is a perfect way to filter out spam e-mails) we have seen merchants take a number of steps that increase the operational cost and complexity of undercover purchasing.

Phone verification

As early as 2010, we experienced that some pharmaceutical programs (fourteen all told over the last two years) would hold an order until they had called and confirmed our order over the phone. Typically, the customer service personnel ask about the details of our order and our credit card number (and sometimes about any past orders we had made, indexed by address and phone number of credit card). In our experience, this verification is primarily for first orders, with subsequent orders from the same individual going unchallenged. However, this verification incurs additional operation overhead for undercover purchasers and requires that they both "maintain cover" and execute complete orders. By contrast, however, we have never received calls from software merchants, replica merchants or sellers of fake anti-virus software.

Documentation requirements

In addition, some pharmaceutical programs have started to request additional documentation before they will process payment. Notably, RxPayouts (also known as RxCashCow) and 33Drugs have requested scans of drivers licenses and physical credit cards, or credit card statements, before processing our orders. Such actions presumably filter out some fraud, but by the same token have the more important effect of further complicating operations for those making undercover purchases (i.e., now an undercover purchaser using fabricated names must also be willing and able to fabricate identity documents as well).

Most recently, another major private program, Club-first, has requested a scan of a prescription before processing an order for a new customer. We can attest that this has not been the case previously. Moreover, we have observed the operator of Club-first remarking, on a well-known Russian-speaking forum focused on various kinds of abusive advertising, that there were large numbers of "test purchases" causing trouble. Thus, we infer that this prescription requirement is a measure designed to counter this activity.

However, these restrictions can also be self-defeating as many consumers regard these requirements as invasive and thus these customer requirements can dramatically reduce sales. For example, in response to RxPayouts' photo ID requirement for new customers (started in late January of 2012), there was an uproar among its affiliates. On one English-speaking forum catering to pharmaceutical affiliates, an RxPayouts affiliate wrote, "This new rule is killing me, my conversion rate for new customers have dropped to cero [sic]. As soon as my new customers find out they have to fax their customer service a Photo-ID, they cancel their order." Another commented "right now I am getting approx. only 10% of my orders being completed."

Blacklisting

Before processing a transaction, it is common to evaluate the fraud risk of a customer. New customers, for example, have higher risk. If the transaction is from an IP address used by a previous customer who has had a chargeback or a decline in the past, then it has higher risk. We are aware of shop runners manually filtering out the orders of particular individuals whom they believe to be under-cover operatives [8]. We have encountered shops that filter out IP addresses used on previously unsuccessful orders, and we have encountered shops that refuse to process payments on credit cards with particular BINs (indeed, this approach forced our group to partner with multiple issuers to obtain a diverse set of BINs for the payment cards used in our study).[16] Similarly, we have identified distressed programs that use IP geo-location to specialize payment options (i.e., to weed out US purchases). For example, after having a number of merchant accounts shut down the 4RX program stopped offering Visa to US customers, but accessing one of the sites via a European IP address would still provide a Visa payment option. All of these techniques raise the stakes for undercover purchasing since it again creates an increased "cover burden" for IP diversity, geographic diversity, BIN diversity, name diversity, etc.

Finally, we are aware that there are some programs who have chosen to "weather the storm" by *only* accepting orders from existing customers. This strategy again can have significant revenue drawbacks; even so, McCoy *et al.* have previously documented that repeat orders can constitute 30% of overall sales [11].

5.2 Complaint bypass

The nature of the complaint process used for these targeted interventions is that a brand holder makes a claim that a given site is infringing on their intellectual property. Having identified the acquiring bank, the "lever" for forcing action is embedded in the card association's contract rules that stipulate that the acquirer should not support infringing merchants. However, it is only the brand

[16]We identified BIN filtering by placing orders from programs using two fresh cards with new IP addresses, addresses and names but from different issuers (and hence completely different BINs).

holder who has "standing" to issue such a complaint, since presumably only they are in a position to know that a site is not duly authorized to sell these goods.

During the OEM software action, we identified two affiliate programs, that we call OmegabidSoft and CD OEM, who actively took advantage of this structure to maintain their existing banking relationships. In particular both programs removed the software offered by the brandholder making the complaint and thus, while they continued to sell counterfeit software by other brands, the complainant no longer had standing to make a case. We believe that this is the reason that the two associated banks, B+S Card Services and Wirecard, continued to allow these merchant accounts to process orders in spite of multiple such complaints. In principal, another affected brandholder (i.e., whose software was still being sold) could have complained as well, but this would require more organization than existed in this initial effort.

For similar reasons, in the last two months a number of pharmaceutical programs have started replacing brand name drugs with their generic equivalents (e.g., Sildenafil Citrate instead of Viagra, Tadalafil instead of Cialis, etc). The operators of these programs argue to their affiliates that such actions will eliminate the brand and trademark issues and thus undermine the ability of brandholders to shutdown both individual sites as well as the associated merchant accounts. The tradeoff in brand avoidance is the impact on consumer conversion (e.g., do US customers know what Sildenafil Citrate is?). It also remains unclear to what extent this ruse will work. While trademark infringement indeed provides a clear "bright line" standard to evaluate, card associations may still have sufficient flexibility in their contracts to include patent violations as well.

5.3 Evasion

Independent of targeted complaints, affiliate programs must first deal with additional scrutiny from card associations and the complexity of obtaining new merchant accounts when the old accounts have been shut down. For example, from surveying forums catering to merchant account brokers, it is clear that it has become extremely difficult to obtain new merchant accounts for online pharmacies.

Thus, many pharmaceutical programs have engaged in one or more efforts to bypass these restrictions in practice. The most clear-cut of these is miscoding. When this study was started in 2010, close to 90% of pharmaceutical transactions were correctly coded with either MCC 5192 or MCC 5122 (the appropriate codes for pharma) and virtually all such transactions from "long-lived" banks. The reason to code these transactions correctly is that miscoding is a serious infraction, potentially carrying large penalties. However, after these two codes were specifically called out in Visa's GBPP announcement (Section 2.3), correct coding swiftly diminished. Indeed, almost 50% of pharmaceutical transactions over the past eight months are miscoded (e.g, as Cosmetics, Grocery Stores, etc.), and in the last two months this fraction is closer to 70%. Today, the only bank that both correctly codes such transactions and supports large numbers of affiliate programs is the State Bank of Mauritius.

Associated with this change, we observe compelling evidence that some programs (or their PSPs) are driven to ever more risky processing arrangements, including laundering the nature of their business through an existing business of some other character. For example, between August and October of 2011, both RXAffiliateNetwork and ZedCash used processing laundered through the merchant account of an online wallet provider (similar to PayPal) using it as an aggregator. On another occasion we observed an OEM software affiliate (that we call Eurosoft) processing through the existing merchant account of a rental car agency in Spain. Finally, with increased pressure on OEM software affiliate programs, we have recently found them attempting to execute payment through banks located in the United States (which have not otherwise played a role across our dataset). While we do not present the data here, we have witnessed similar attempts with fake anti-virus affiliate programs as well. All of these arrangements are considerably more fragile than traditional merchant accounts because they are *de facto* violations and are aggressively shut down by many banks as soon as they are made aware (and for the same reason there is no requirement for a complainant to have standing).

5.4 Alternative payments

Finally, while payment card networks have, by far, the largest footprint for Western consumers, they are not the only mechanism for payment. Thus, we have seen a number of pharmaceutical programs with disabled processing (e.g., 4RX) attempt to continue business after losing Visa and MasterCard processing fusing a combination of Western Union and eCheck payments (eCheck is basically payment via ACH transfer from a checking account, the mechanism used by online bill pay in the US). A few US-based pharmaceutical programs, notably Health Solutions Network (which we did not study in our analysis), enabled Cash-On-Delivery (COD) payments for their customers when their Visa processing was disabled. Ultimately, the effectiveness of such mechanisms depends on their familiarity and overhead to consumers, the readiness of alternative sites offering more traditional payments, and the extent to which consumers are well motivated. Indeed, while we witnessed some programs (notably in the OEM software space) attempt to continue their businesses using alternative payment mechanisms including PayPal and, most recently, Bitcoin, by all accounts this has not been successful.

6. CONCLUSION

Security interventions should ultimately be evaluated on both their impact in disrupting the adversary and their cost to the defender. On both counts, the payment tier of abuse-advertising appears to be a ripe target. For the few tens of dollars for a modest online purchase, our data shows that it is possible to identify a portion of the underlying payment infrastructure and, within weeks, cause it to be terminated. This termination cost is inevitably far higher—in fines, in lost holdback, in time and in opportunity cost—than the cost of the intervention itself. Moreover, as we have shown, there are at any time only a modest set of banks providing high-risk services and a smaller set still that cater significantly to this clientele. Thus, relatively concentrated actions with key financial institutions can have outsized impacts. Finally, based on our observations, this approach is most successful when there is both comprehensive intelligence about the full set of programs involved and a willingness to "follow up" on a per-program basis relentlessly. Taking down accounts "here and there" does raise the cost structure for program sponsors, but ultimately it takes focus to convince such operators to close up shop.

Acknowledgments

This study involved support from a great number of individuals and organizations who we would like to thank. On the purchasing side, we are deeply indebted to our card issuers and people that helped place trace purchases on our behalf, without whom this study would have been impossible. As well, we have benefited from strong relationships with key brand holders and financial service providers whose insight and support has been equally critical. Throughout our efforts we have benefited from legal and ethical guidance from Erin Kenneally, as well as oversight from Daniel Park, UCSD's

Chief Counsel, and Patrick Schlesinger from UC's System-wide Research Compliance office. We would also like to thank Brian Kantor and Cindy Moore for supporting our ongoing systems and storage needs and, finally, we recognize the anonymous reviewers for their helpful feedback and critiques.

This work was supported in part by National Science Foundation grants NSF-0433668, NSF-0433702, NSF-0831138 and CNS-0905631, by the Office of Naval Research MURI grant N00014-09-1-1081, and by generous research, operational and/or in-kind support from Google, Microsoft, Yahoo, Cisco, HP and the UCSD Center for Networked Systems (CNS) among others.

7. REFERENCES

[1] 2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement. http://www.ice.gov/doclib/iprcenter/pdf/ipec-annual-report.pdf, Feb. 2011.

[2] M. Hypponen. A Norwegian bank (DnB NOR) co-operates with some of the largest spammers in the world. https://twitter.com/#!/dnbnor_hjelp/status/73305600066461696, May 2011.

[3] IACC Has New Tools To Cut Off Money to Bad Sites. https://iacc.org/news-media-resources/press-releases/iacc-has-new-tools-to-cut-off-money-to-bad-sites.php, 2011.

[4] ISO 8583-1:2003 — Financial transaction card originated messages — Interchange message specifications, 2003.

[5] C. Kanich, N. Chachra, D. McCoy, C. Grier, D. Y. Wang, M. Motoyama, K. Levchenko, S. Savage, and G. M. Voelker. No Plan Survives Contact: Experience with Cybercrime Measurement. In *Proceedings of the 4th Workshop on Cyber Security Experimentation and Test (CSET)*, Aug. 2011.

[6] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. M. Voelker, and S. Savage. Show Me the Money: Characterizing Spam-advertised Revenue. In *Proceedings of the USENIX Security Symposium*, Aug. 2011.

[7] B. Krebs. White House Calls Meeting on Rogue Online Pharmacies. http://krebsonsecurity.com/2010/08/white-house-calls-meeting-on-rogue-online-pharmacies, Aug. 2010.

[8] B. Krebs. Gateline.net Was Key Rogue Pharma Processor. http://krebsonsecurity.com/2012/04/gateline-net-was-key-rogue-pharma-processor, Apr. 2011.

[9] N. Leontiadis, T. Moore, and N. Christin. Measuring and Analyzing Search-Redirection Attacks in the Illicit Online Prescription Drug Trade. In *Proceedings USENIX Security 2011*, Aug. 2011.

[10] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Felegyhazi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and S. Savage. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In *Proceedings of the IEEE Symposium and Security and Privacy*, Oakland, CA, May 2011.

[11] D. McCoy, A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, G. M. Voelker, S. Savage, and K. Levchanko. PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. In *Proceedings USENIX Security 2012*, Aug. 2012.

[12] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker. An Analysis of Underground Forums. In *Proceedings of the ACM Internet Measurement Conference*, Nov. 2011.

[13] Rooting Out Rogue Merchants: The IACC Payment Processor Portal Mid-Year Review and Vision for the Future. IACC 2012 Spring Annual Meeting (as found at iacc.org), May 2012.

[14] D. Samosseiko. The Partnerka — What is it, and why should you care? In *Proc. of Virus Bulletin Conference*, Sept. 2009.

[15] B. Stone-Gross, R. Abman, R. Kemmerer, C. Kruegel, D. Steigerwald, and G. Vigna. The Underground Economy of Fake Antivirus Software. In *Proceedings of the Workshop on Economics of Information Security (WEIS)*, 2011.

[16] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In *Proceedings of the 4th USENIX Conference on Large-scale Exploits and Emergent Threats (LEET)*, 2011.

[17] Visa Global Brand Protection Program. http://blog.instabill.com/media/blogs/instabill/pdf/GlobalBrandprotectionProgram.pdf[17], 2011.

[18] Visa Commercial Solutions. Merchant Category Codes for IRS Form 1099-MISC Reporting. http://usa.visa.com/download/corporate/resources/mcc_booklet.pdf.

[19] XyliBox. http://www.xylibox.com/.

[17] Originally posted on the Instabill site, later removed.