Bullet-Proof Payment Processors

Hongwei Tian
New York University
Brooklyn, USA
ht974@nyu.edu

Stephen M. Gaffigan
SMGPA
stephen@smgpa.net

D. Sean West
SMGPA
sean@smgpa.net

Damon McCoy
New York University
Brooklyn, USA
mccoy@nyu.edu

***Abstract*—Abusively advertised online counterfeit luxury goods sales are a complex operation that requires accessible and reliable payment processing to transfer money from customer to merchant. Payment interventions have become one of many methods to combat this activity. In this paper, we examine the effectiveness of an intervention in the face of bullet-proof payment processors and possibly lessening fines levied by Visa Asia against banks found underwriting accounts for merchants violating intellectual property. Our study includes measurements from 424 successful test counterfeit luxury goods purchases over two years and direct interactions with payment processors associated with our purchases. We find that our long-running payment intervention results in a test purchaser detection and evasion arms-race with the bullet-proof processors. We also find that only one bank, the Bank of China, continues onboarding a majority of counterfeit luxury goods merchants for the entire two year period.**

***Index Terms*—Security, Measurement, Economics**

I. Introduction

Online sales in the United States were over $430 billion USD in 2017 and have been growing at a rate of over 15% each year for the last three years [1]. This environment provides a fertile ground for counterfeit luxury goods sellers to profit from this growth in online sales by duping victims into buying what they think are slightly discounted legitimate luxury goods. Prior studies have shown that these counterfeit luxury goods merchants are advertising their goods using "black hat" Search Engine Optimization (SEO) techniques [2] and Online Social Networking (OSN) advertisements [3]. The advertising, domain name, and hosting of counterfeit luxury goods has been difficult to disrupt using technical and policy-based interventions [2].

However, prior studies have shown that the credit card payment processing for trademark infringing goods can potentially be disrupted [4], [5]. This is interesting since one study based on leak data found that 95% of the revenue for illegal online pharmaceuticals was acquired using credit card payments [6]. This suggests a "choke-point" for online counterfeit luxury goods sales that might be feasible to disrupt [7].

In this paper, we conduct a two-year payment intervention with the assistance of six major luxury brands that are targeted by counterfeiters. We are motivated in part by our initial success of disrupting payments for illegal online pharmaceuticals and counterfeit software [5]. However, adversaries adapt to intervention strategies and we wanted to understand the sustainability and current effectiveness of payment interventions in the face of their adaptations.

Our study consists of 424 successful test purchases over a two-year time span from August 2014 until April 2016 and interactions with payment processors. We find that the primary adaptation is third-party "bullet-proof" payment processors that establish accounts with banks likely using shell companies and then sell access to these merchant accounts to online counterfeit luxury goods merchants. They also provide test purchase detection and filtering services that help insulate these illicit merchants from fines and disruption of their payment processing. We also find that Visa Asia is likely backing off from their enhanced fines and enforcement for intellectual property violations. However, we have no confirmation of this since Visa does not make their fines or enforcement actions public.

As our payment intervention progressed, we encountered a typical arms-race of evolving test order filtering methods by bullet-proof processors and us training our volunteer purchasers to evade filtering. This probably caused filtering of legitimate customers as the detection became more stringent. A one time experiment with another luxury brand found that order filtering was much less and that more counterfeit websites were able to accept credit card payments successfully. This indicates that our intervention might not have been as effective at limiting the availability of credit card processing for brands not included in our study.

Our work makes three key contributions. First, we longitudinally illuminate the "bullet-proof" payment processors and banks that are involved in acquiring credit card payments for counterfeit luxury goods merchants. Second, we document the adaptation of these companies when continuous pressure is applied over two years. Finally, we expose the likely changes to fines and enforcement that make up Visa's self-regulation of their payment network and cardholder association member banks with regards to merchants engaged in intellectual property infringement.

The rest of our paper is structured as follows. In the next section, we provide a background on the structure of counterfeit goods merchants, online credit card payment mechanics, IP enforcement policies of Visa, and third-party payment processors. We then present the analysis of our two-year payment intervention and related work. Finally, we provide a discussion and conclusions.

978-1-5386-4922-0/18/$31.00

II. Background

In this section, we explain both the business structure of online counterfeit luxury goods sales as well as the structure of the payment card ecosystem and how the two integrate in practice.

A. Online Counterfeit Luxury Goods Sales

There are several components to the online sale of goods. First is the acquisition of traffic, i.e., visitors to an online site that might be converted into potential customers. In the context of counterfeit luxury goods this acquisition of traffic is often done using "black hat" Search Engine Optimization (SEO) techniques. One common method is compromising legitimate sites and leveraging their search engine ranking to pollute longer tail search queries. For example, "cheap michael kors black friday" instead of the shorter, more competitive search terms. These high ranking URLs within hacked websites are doorway pages configured to redirect visitors to counterfeit luxury goods sites that offer to sell luxury goods at steep discounts [1].

This part of the online counterfeit luxury goods sales ecosystem has been the target of domain seizure and search engine blacklisting interventions. A prior study of these interventions has shown that they appear to have a short-term impact in reducing the prevalence of search engine pollution but not a long-term one [2].

Once customers decide to purchase a product, money must change hands from the customer to the online merchant. There are many options for online payments: wire transfers, PayPal, crypto currencies, and ACH (eCheck). A prior study of online counterfeit pharmaceutical programs found that, while there are other payment options, 95% of all revenue was from credit card payments [6]. We will go into more detail about how payment processing is done for these sites below.

The final step is goods fulfillment and customer service. Based on the results of our purchasing of counterfeit luxury goods, they were all drop shipped from China and most were of relatively poor quality. The customer service was handled by email.

Based on our analysis it does not appear that the affiliate sale model [2] is widely used for counterfeit luxury goods sales. Instead, most entities appear to operate a large set of websites and focus on black hat SEO to acquire traffic. These website merchants largely outsource payment processing and fulfillment to third-party services. As part of our study, we primarily focused on studying these third-party payment processors that facilitate the payments for online counterfeit luxury goods sales.

B. Payment Processors

In the retail environment, cash and POS machines are used for purchases. However, card networks are the typical choice for online purchase transactions, such as Visa, MasterCard, American Express, and Discover. Before we talk about payment processors, we will introduce some background on the mechanics of online payment card transactions.

Payment card transaction. While there are many payment card systems, we focus on Visa and MasterCard because they have the largest consumer market share. Visa and MasterCard are so-called "open loop" networks because they implement multi-party payment networks that interconnect a range of banks that are members of their card associations [3]. In particular, there are at least five parties in every 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 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 amount, to their acquiring bank. The acquiring 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 [8].

In considering whether to approve this transaction the issuer has a range of transaction features available to evaluate including the BIN of the merchant bank, the country of operation, the Merchant Category Code (MCC) of the merchant terminal, the size of the request, the amount of money available to the cardholder and so on. The merchant may also choose to pay for the Address Verification Service (AVS) that can verify if the account holder's name, street address, and ZIP code provided by the customer match that registered with the issuing bank. Most merchants elect to verify only the ZIP code to reduce declined transactions due to slightly incorrect information provided by customers such as a shortened version of their first name.

If the authorization request is approved, then the money (or credit) is held at the issuer. The acquiring bank is then 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 by transferring money from the cardholder's issuing bank to the merchant's acquiring bank. Note that authorization does not imply settlement and the merchant is free not to complete the transaction (in which case the hold on the authorization will eventually timeout and these funds will be available again to the cardholder).

[1] Note that while some of these sites state that the goods are not genuine, most do not provide any indication that the goods are counterfeit.

[2] An affiliate sale model is where an affiliate marketer is paid a commission by an affiliate program for every sale they drive to that program.

[3] American Express and Discover are actually "close loop" networks that directly issue credit accounts and work with a large number of merchants.

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 payment processor (e.g., First Data).

Third-Party Processors. Many merchants contract with a third-party to handle establishing a merchant account with a bank, provide fraud detection, and the technical framework for acquiring and settling transactions using the merchant terminal. There are a variety of third-parties. The largest third-party processors are Independent Sales Organization (ISO) that in some cases can "rent" BINs from banks and who then act as de facto acquirers. There are also Payment Service Providers (PSPs) or Payment Facilitators (PFs) who can contract with an acquiring bank to provide payment services on behalf of merchants contracted directly with the PSP/PF.

In April 2013 Visa started a third-party payment company certification program of vetted Qualified Service Providers (QSP) for the Asia region [9] [4]. MasterCard also maintains a global set of registered payment facilitators that is larger and does not appear to be vetted [11].

High-Risk Merchants. 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 a PF) must be underwritten by the bank against the merchant's risk profile (i.e., the likelihood of fraud, fine assessment, and chargebacks).

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 banks that are willing to underwrite such businesses will charge much higher transaction fees and may also demand up-front money, transaction holdbacks, and a documentation showing a 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 principle, PSP/PFs comply with Visa rules, and thus they will only be able to aggregate high-risk client transactions with acquiring banks who are agreeable.

C. Payment interventions

Self Regulation

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 seemed designed to target online pharmacies and sellers of counterfeit goods specifically. 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. Additionally, the new documents explicitly call out examples of illegal transactions including the "Sale of counterfeit or trademark-infringing products or services", among others [12]. Finally, these changes include a more aggressive fine schedule and, implicitly, represented a statement of more aggressive enforcement actions to be forthcoming.

However, we find indications that Visa might actually be backing off their fines for trademark-infringing products. A briefly public document from 2011 described the new regulations and fines to banks which started at $25,000 per merchant violation and increased to $200,000 after several infractions. Subsequently leaked violation notices from Visa to banks from late 2016 indicate that, at some point after 2011, Visa Asia reduced the fine amount for selling counterfeit luxury goods to $5,000 per merchant violation. The fine amount for miss coded gambling and illegal pharmaceutical transactions remained at $25,000. We have confirmed that these leaked violation notices are correctly formatted and use the standard terms; thus, we accept them as authentic and a strong indication that Visa Asia has reduced the fine amount for selling counterfeit luxury goods. Unfortunately, Visa and MasterCard do not make public their regulations and policies related to the selling of counterfeit and illegal goods and services.

Brandholder 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 2011 GBPP revamp and then subsequently reduced at least by Visa Asia for counterfeit luxury good sales by 2016). 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 brandholders, 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 brandholders 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 brandholders, 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 making test purchases to identify merchant accounts used to monetize reported sites and managing the formal complaint process through the card networks.

[4] Unrelated to counterfeit goods processing we found that GbPay is a Visa qualified processor (QSP). However, GbPay has been closed due to financial crimes [10]. This indicates that Visa's QSP processors might need additional vetting.

A study of this new process found that merchant accounts reported as selling trademark infringing goods to Visa's GBPP group were terminated after around 30 days [5]. In 2011 two brandholders, Microsoft and an unnamed pharmaceutical company, used this complaint process to disrupt payments for a large segment of illegal online pharmaceutical and counterfeit software sales [5].

D. Bullet-Proof Credit Card Processors

Adversaries always adapt, and no stagnant intervention will remain effective indefinitely including undermining the payment ecosystem of illegal online sales. We have discovered in our study of online counterfeit luxury goods merchants that there have emerged criminal payment facilitators, which we call bullet-proof credit card processors, that are offering credit card processing services that are tailored to accept payments for online counterfeit luxury goods.

These bullet-proof processors are in some instances establishing shell companies which appear to be selling low-risk goods. The merchant names in the credit card transactions will sometimes contain a domain name for a website associated with one of these shell companies. The website will sell generic goods and on the face look legitimate. However, the sites are not functional and do not accept payments when someone attempts to checkout.

Bullet-proof processors are using this technique and possibly others to open up a large number of merchant processing accounts at banks and sell access to these merchant accounts to high-risk merchants selling counterfeit luxury goods. A key part of their service offering is order filtering that is designed to detect and block likely test purchases that might result in brandholder complaints and associated fines. The rest of our study will present our methodology for collecting data and analysis of these bullet-proof processors.

III. Methodology

In this section, we will present our methodology for studying bullet-proof processors in the counterfeit luxury goods ecosystem. Our methodology is largely based on that of Levchenko et al. [4] and McCoy et al. [5], in which we identify trademark infringing websites and then complete test purchases to discover the merchant account accepting payments for these websites.

A. Website Identification

The first step in our process is to identify infringing websites for six major luxury goods brandholders [5] that provided us with permission to perform test purchases and file complaints against the merchant accounts with Visa's GBPP group. The majority of sites we identified were from searching for common long tailed keyword queries that were often polluted using black hat SEO techniques. We used several techniques to identify which websites in the search engine results were selling counterfeit goods. One of the methods we used is similar to that from a prior study by Wang et al. [2] of visiting each page and detecting which ones redirect to another site. These are almost always compromised doorway pages that redirect to websites selling counterfeit goods. We also built heuristics to detect websites that were directly SEOed instead of using compromised doorway pages. Finally, we identified some counterfeit websites promoted by email and Online Social Network (OSN) spam campaigns.

All the suspected sites are then manually vetted to ensure they are selling counterfeit goods with trademarks from one of the six brandholders. We then analyze the websites to remove sites likely operated by the same merchant using a few methods such as shared analytics identifiers, whois registration information, and identical products and pricing.

The next step is to attempt to identify the third-party payment processor(s) used by each site. Initially the third-party payment processors operated their own payment gateway sites that each had unique HTML code and images that were relatively easy to cluster. These domains were fairly long-lived and we could link them to their associated third-party payment processor based on analysis of the code they provided to merchants to include in their websites which often included the processor's name. For other processors, we established a merchant account which we then used to link the third-party payment processor based on the code they provided to us. This code included on the merchants' website would also often include a string that identified the merchant's third-party processing account. We used this to detect sites that were all using the same processing account. During the latter part of our study, it became increasingly difficult to identify the merchant account. The third-party processors have largely stopped operating their own payment gateway sites, and they have changed their code to no longer publicly leak the identity of the merchant or processor.

The counterfeit websites were then ranked using several metrics such as their visibility in search engine rankings and customer complaints received by the brandholders. From this set of counterfeit websites approved by the brandholders, we selected a few of the highest ranking websites to attempt purchases from each month. At some points in the study we focused on a particular processor, but we still attempted to complete a few purchases handled by other major processors to track their operations.

B. Test Purchasing

A test purchase is required in order to discover the merchant account that is accepting payments for a website selling counterfeit goods. As in prior studies, we focused on Visa since it has a larger market share in the United States [4], [5]. We first attempted purchases using Visa prepaid cards from multiple issuers which were all filtered by these bullet-proof processors likely using a list of prepaid card BINs. In order to evade this filtering, we set up a business account with a major US bank and issued credit cards to people that volunteered to assist us in placing test purchases. These cards worked for the first three months of our study until the bullet-proof processors started filtering purchase attempts even by new volunteers that

[5] They do not wish to be publicly named.

had never attempted a prior purchase. For the rest of the study, we recruited people to complete test purchases using their personal credit cards. Our recruitment strategy was a snowball approach of paying each purchaser a $75 payment for each successful purchase and a $25 payment for each successful purchase completed by someone they referred to us. Before they were assigned sites to attempt purchases from we warned them of the risk of credit card fraud which none of our purchasers reported. The other impact that we warned our purchasers about is that most of them were added to blacklists and subsequent attempts to purchases counterfeit goods are filtered. We made it clear that assisting in our study was completely voluntary. In total, over 80 people attempted purchases for our study. Most of them complete between zero to two purchases. All the goods that we received were confirmed to be counterfeit.

We did not track failed purchases since it was sometimes difficult to know when a purchaser actually attempted and the cause of the failed purchase attempts. Our data set represents 424 successful purchases completed over two years, from July 2014 to February 2017. We bind the websites in order to protect both the privacy of our purchasers and brandholders. All of these test purchases were reported to Visa's GBPP group, and the merchant accounts were terminated or remediated after an investigation. Visa provided us with the result of the investigation and the bank associated with each purchase. There were five instances where the bank was not identified due to complex ISO relationships. We were able to identify the third-party payment processor for 221 of these purchases. When there was any uncertainty about the processor, we marked the processor as unidentified. We also collected qualitative data from contacting a subset of the third-party payment processors and from monitoring underground forums.

Based on our monitoring of these underground forums, we were able to confirm the closure and change in policies of some of the bullet-proof processors. We also used these forums to identify likely bullet-proof processors that were advertising their services to counterfeit merchants. Finally, we used these underground forums to obtain contact information for bullet-proof processors.

C. Limitations

Our set of websites that were targeted for test purchases has several limitations and biases. Our payment intervention is limited to only six brandholders, we primarily identified websites from search engine results, and the brandholder ultimately approved and ranked the set of sites from which we attempted test purchases. This means we could have missed some processors that forbid merchants from selling counterfeit goods for these brandholders.

The different levels of filtering also likely biased our data collection. Some payment processors used by counterfeit luxury goods merchants were probably not bullet-proof processors and did not make any attempts to filter our test purchases. Some bullet-proof processors were more aggressive and likely filtered more of our test purchases.

For these reasons, our study is likely not useful for ranking the prevalence of third-party payment processors and might not provide a comprehensive view of these bullet-proof processors. However, we believe it does provide a qualitative understanding of how these bullet-proof processors operate and the interplay of these criminal payment facilitators with other stakeholders in this ecosystem, such as counterfeit luxury goods merchants, Visa, and banks.

IV. Analysis

We first present our dataset of test purchases and then our quantitative and qualitative analysis of this dataset. Finally, we present an analysis of our qualitative data collected from contacting a subset of third-party payment processors.

A. Test Purchase Dataset

Our first dataset is 424 successful purchases completed over two years, from July 2014 to February 2017.

Payment Processors

Table I provides a list of all 32 payment processors that we identified. We find that for the 221 purchases where we were able to identify the payment processor, five payment processors account for over 68% of the payments processed for counterfeit goods. This demonstrates some concentration where a few bullet-proof payment processors handle much of the online counterfeit goods payments. ALIPAY, TENPAY, and SKRILL are digital wallet services similar to PayPal. These are likely abused by individuals. We did not encounter any order filtering or other indications from these digital wallet services that they were bullet-proof payment processors.

There were also 203 purchases for which we were not able to identify the third-party payment processor. The majority of these identified purchases occur before the bullet-proof payment processors stopped operating their own payment gateway sites and instead changed their APIs to callback functions between the merchant's website and the processor which are not publicly visible. We are currently working on overcoming this limitation by identifying payment processors based on other features, such as confirmation email templates and order number spaces. Based on manual analysis of confirmation emails and contact information we can link some transactions back to bullet-proof processors. However, we have not done this linking systematically and did not include the results in this paper.

Acquiring Banks

These counterfeit goods purchases, in turn, were processed through nine acquiring banks. For five of the purchases the acquiring bank was not identified by Visa which could be caused by complex ISO relationships. Three of the acquiring banks, Citizens Bank, Allied Irish Bank and Industrial & Commercial Bank of China, processed less than five purchases for brief periods of time around one to two months.

Table II shows the merchant banks and their frequencies in our dataset. We find that three banks, the Bank of China, Bank

TABLE I
SUMMARY OF PAYMENT PROCESSORS AND THEIR FREQUENCIES.

Payment Processors	Number of Purchases
UNIDENTIFIED	203
PAYWORKS	53
REALYPAY	39
MONEYBRACE	27
FASHIONPAY	20
GLEEPAY	13
DHPAY	9
HSDSPAY	8
SCOINPAY	7
ALTERCARDS	5
PAYEASE	4
HOOPPAY	4
ONEKPAY	4
ALIPAY	3
GLBPAY	3
VIMAPAY	3
SHOPIFY	2
TENPAY	2
NOWIPAY	1
SCHOOLPAY	1
AMOPAY	1
SKRILL	1
POCKETPAY	1
ETONPAY	1
CCWONLINE	1
SFEPAY	1
GCBILLPAY	1
Federal Pacific Credit	1
IMPAY	1
ACCREDITPAY	1
WPAYMENT	1
GLOBALPAY	1
CARDPAY	1

of Communications, and Harbin Bank processed 91% of the transactions in our dataset while other banks processed fewer than ten counterfeit goods transactions over two years. Figure 1 shows the set of banks processing Visa transactions for the counterfeit goods we purchased over two years. Each row corresponds to a bank, and each point on a row corresponds to a purchase processed by this bank as merchant bank; the color of the point represents the payment processor processing this purchase; the parenthetical number next to the bank name denotes the number of purchases that bank processed. The corresponding top five payment processors are identified using different colors. We display the rows of banks in increasing time order of appearance in our data set.

TABLE II
SUMMARY OF MERCHANT BANKS

Merchant Bank	Counts	Percentage
BANK OF CHINA	275	64.25%
BANK OF COMMUNICATIONS	104	24.30%
HARBIN BANK CO., LTD.	10	2.34%
LOTTE CARD CO., LTD.	9	2.10%
KOREA EXCHANGE BANK	8	1.87%
OTHERS	13	3.98%
UNKNOWN	5	1.16%
Total	424	100%

Looking at the acquiring banks longitudinally, we find that the bulk of the counterfeit goods purchases acquired by the Bank of Communications bulk were concentrated between August 2014 and April 2016 with only a single purchase appearing after this date. This reduction in acquiring for counterfeit goods merchants indicates that the Bank of Communications might have improved their vetting of third-party payment processors and merchants sometime before April 2016. We find that the two Korean banks, Lotte and Korea Exchange Bank, improved their vetting and ceased on-boarding counterfeit goods merchants within the first few months of our study. However, it is unclear if these banks cracked down on all counterfeit goods merchants or only those selling brands that generate Intellectual Property (IP) complaints to Visa.

Once the Bank of Communications largely stopped on-boarding counterfeit goods merchants, at least for these six brands, after April 2016, then the percentage of purchases with the Bank of China as the acquiring bank increases to 73% (46/63). We also observed in the latter part of our study that the bullet-proof payment processors are probing Harbin Bank, which is a smaller Chinese bank. This might also indicate an overall tightening of merchant account availability for merchants selling counterfeit goods for these six brands.

B. Payment Processor and Banking Relationships

Figure 2 shows a longitudinal mapping of the payment processor to the acquiring bank for the 221 purchases where we were able to identify the processor. The bulk of our successful purchases were processed by five payment processors: PAYWORKS, MONEYBRACE, FASHIONPAY, REALYPAY, and GLEEPAY. Looking at Figure 2 you can see that it is horizontally divided into two parts, with most purchases processed by the top five payment processors before January 2015. After this time it becomes difficult for us to identify the payment processors and thus there are mostly unidentified payment processors in our dataset.

Figure 3 shows the processors and corresponding merchant banks. From this figure, it is apparent that Bank of China is the merchant bank used by most of the payment processors. We also see that the top processors open up merchant accounts

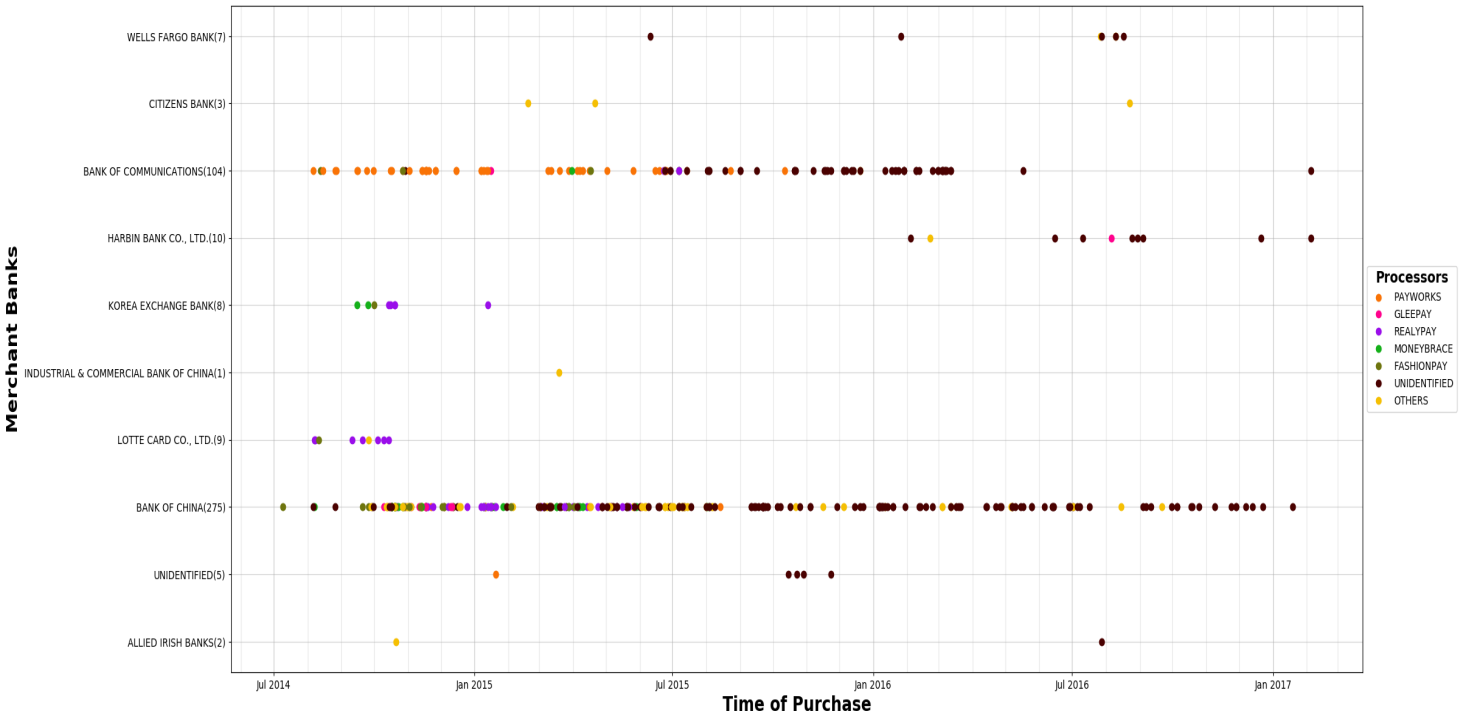

Fig. 1. Bank processing purchases over time. Solid dots denote successful purchases processed through a bank. Numbers in parentheses at the end of bank names denote the number of purchases processed by the banks.

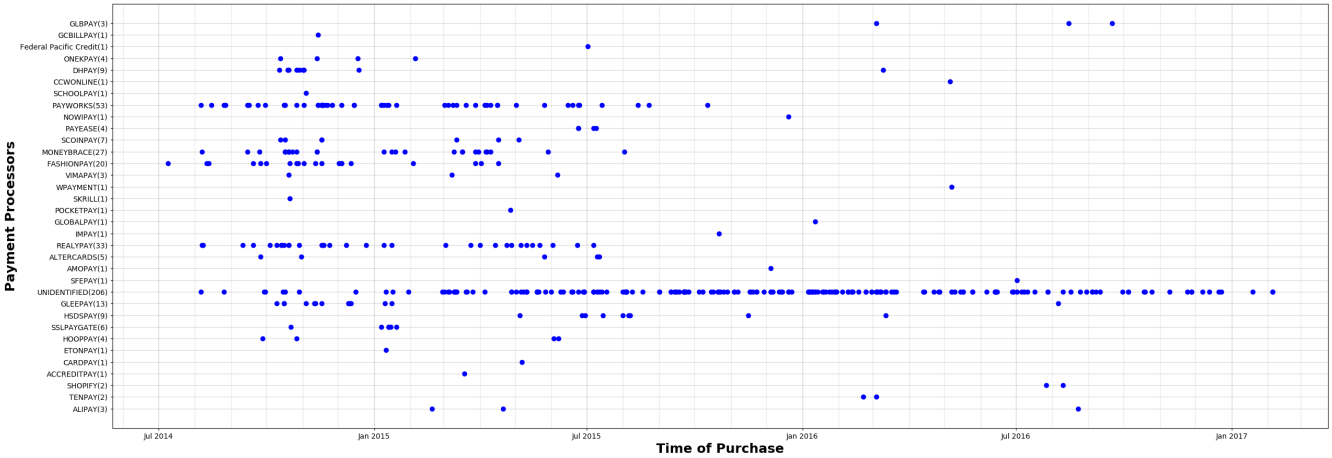

Fig. 2. Payment processors processing purchases over time. Solid dots denote successful purchases. Numbers in parentheses at the end of payment processor names denote the number of purchases processed by the payment processor.

with multiple banks. For example, Payworks mostly uses Bank of Communication as its merchant bank, but it also use Bank of China periodically. Also, processors shift from one bank to another, e.g, GleePay used Bank of China and Bank of Communications from Oct 2014 to Jan 2015, then it shifted from Bank of China to Harbin Bank.

C. *Order Filtering*

It is difficult to fully enumerate which payment processors actively attempted to filter test purchases and reverse-engineer their methods for detecting likely test purchases. We will provide some qualitative experience from our two years of attempted test purchases.

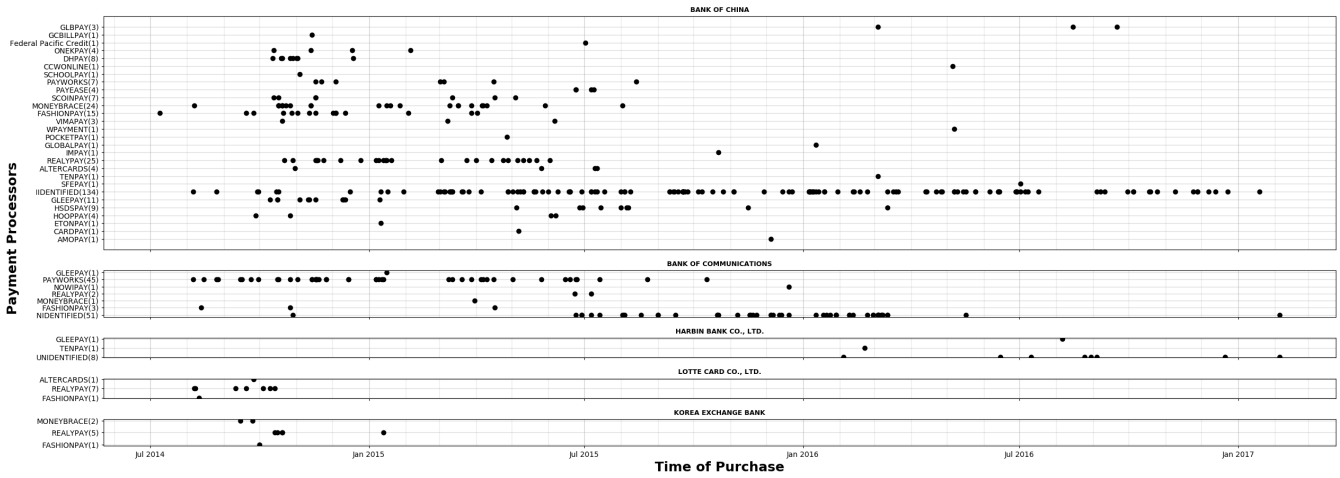

Fig. 3. Payment processors processing purchases over time for top 5 merchant banks. Solid dots denote successful purchases. Numbers in parentheses at the end of payment processor names denote the number of purchases processed by the payment processor.

At the start there was little order filtering by counterfeit goods payment processors for the six brands that were a part of our core study. Our prepaid credit cards were blocked, but this could be caused by a standard fraud detection system. Within the first three months of our study, our business credit cards that we issued to purchasers, which all have the same BIN (same initial 6 digits), were filtered by bullet-proof processors. We tested this by issuing a card from this BIN to someone that had never attempted a counterfeit goods purchases. This purchaser after being blocked when using a credit card from this presumably blacklisted BIN was then able to complete a purchase from the same website for the same product using their personal Visa credit card. These credit cards are not blocked by likely non-bullet-proof processors such as AliPay.

We found that credit card number and IP address were likely two of the most common features that were used for filtering. One of the authors tested this by obtaining a new credit card and IP address that evaded filtering one five sites. Anecdotal some of our volunteer purchasers were also able to evade filtering by changing these two features. However, we cannot definitively say how filtering worked in most instances.

We also found that Realypay which was a highly prominent bullet-proof payment processor started having website operators include Java-Script on their site that set a tracking cookie in purchasers' browsers. This tracking cookie detected the referrer value and if it was empty the attempted purchase would be blocked. This was presumably a method for detecting test purchasers that directly copied assigned URLs into the browser address bar. Once we instructed purchasers to enter the site using a search engine, this Java-Script based tracking cookie was discontinued.

We also found that website operators began stating in email messages that they were filtering credit card purchases for these specific brands, likely because of the perceived risk from prior account closures due to complaints from test purchases. We also encountered instances where counterfeit goods merchants would create two sites where one of the sites accepted credit card payments but did not sell goods for any of the targeted brands. They would then operate another site that only accepted wire transfers and sold products for the targeted brands. These brand removal strategies were also encountered in our prior study of illegal pharmaceutical websites [5].

Towards the end of our study, most of our purchasers were only able to complete a single purchase before they were blacklisted. This indicates that the filtering was likely no longer keying in on any suspicious features and was simply an aggressive rate limiting at the end of our study. We attempted to space out purchases to evade this rate limiting but were unsuccessful at enabling a purchaser to complete additional purchases even when spacing out purchases by several months.

Our final experiment on order filter was performed after our two-year study period. For this experiment, we recruited another brandholder and conducted experiments where already blocked purchasers attempted to purchase a product for this new brand. They then attempted to complete a purchase for one of the six heavily targeted brands to confirm they were still blocked. The success rate for websites selling this new brand were much higher and none of the purchasers were able to complete a purchase for one of the six original brands. This highlights that these bullet-proof processors and merchants were likely more cautious when processing payments for brands they know are actively conducting test purchases.

D. Result of Contacting Payment Processors

In order to understand if some of these payment processors are complicit, we contacted payment processors that were identified as accepting payment for counterfeit goods merchants. We attempted to contact them by email, phone, and social networks (e.g., QQ). We attempted to contact all 32 payment processors we identified processing payments for counterfeit goods and a random subset of six payment processors, who have been qualified by Visa [9] and Mastercard [11]. The complete list of processors we contacted can be found in Appendix A. We received replies from 12

processors. Six of the payment processors appear to have previously supported counterfeit goods merchants but are no longer operating based on information we found online: ACCREDITPAY, GCBILLPAY, HSDSPAY, NOWIPAY, RealyPay, and VIMAPAY. Note that for all six of these closed payment processors we experienced order filtering which is indicative of bullet-proof processing. It is unclear why these bullet-proof payment processors closed and we could find no direct explanations online.

For those payment processors that responded, we pretended to be a potential merchant looking for a payment processor for our website. We also directly informed them that we are going to sell counterfeit goods on our website and ask them to provide payment processing service. For those payment processors who agree, we further ask about potential fees, such as an initial fee, annual fee, transaction fee, and if they restrict merchants from selling counterfeit goods for any brands. In this way, we can get the list of payment processors who provide "bullet-proof" payment processing for counterfeit goods merchants.

Table III shows the summary of our contact with payment processors. Five processors replied and claimed not to allow merchants to sell counterfeit goods: AsiaPay, DHPay, PayDollar, Payworks, and Shopify. Payworks responded that they only provide services for in-store selling but no longer provided services for online transactions, which may be the reason why there are no counterfeit goods purchases processed by Payworks after October 2015. Shopify and Asiapay say that authorization from the brandholder is required for resellers. Seven processors confirmed that they allowed merchants to sell counterfeit goods, placing them in the category of clearly bullet-proof payment processors: EtonPay, FashionPay, GlbPay, GlobalPay, HoopPay, King365Pay, SfePay.

We include a complete list of restricted brands for each processor and their fees in Appendix B. Chanel was included on five out of six restricted brand lists. Other commonly prohibited brands that appeared on at least three payment processor's lists include Abercrombie & Fitch, Canada Goose, Gucci, and Louis Vuitton. We also obtained fees for four of the six bullet-proof processors. These bullet-proof payment processors charge elevated processing fees of 5% all the way up to 8% charged by FashionPay. These payment processors also often charge yearly fees of a few hundred USD to a few thousand. This is a steep premium from the standard 2-3% processing fees and no yearly fee that legitimate payment processors charge. These elevated fees are presumably used to cover fines and chargebacks incurred by their customers that are likely primarily high-risk counterfeit goods merchants.

TABLE III
SUMMARY OF CONTACTING PAYMENT PROCESSORS

Supporting Counterfeit Goods Transactions	7
Do not allow Counterfeit Goods Transactions	5
Do not reply	21
Closed	6
Total	39

V. Related Work

Levchenko Et Al. [4] initially pointed out a potentially choke-point in the payment processing for illegal pharmaceuticals and counterfeit software. Follow up work measured the effectiveness of two payment interventions showing that this is a viable strategy for disrupting the credit card payments for trademark infringing products sold online. Another study highlighted how fake anti-virus companies manipulated the refund and chargeback rates of credit card payments to avoid detection and fines [13] Other work shows that High Yield Investment Programs (HYIPs) also had a concentration in payment methods [14]. Wang Et Al. [2] empirically showed that the marketing of counterfeit luxury goods sites was difficult to disrupt. Clayton Et Al. [7] produced a framework for reasoning about interventions and their likely successfulness by reviewing prior work looking for choke-points at the hosting, domain, payment, and other layers of many cybercrime activities. We use measurement and analysis techniques from many of these prior studies in our measurement. Our additional contributions are to provide an understanding of how effective payment interventions are in the face of adapting adversaries and self-regulation from Visa. We also provide insight into how payment interventions function in the counterfeit luxury goods space where there are many luxury brands that can be targeted.

VI. Discussion and Conclusions

Visa's GBPP and MasterCard's corresponding program offers a streamlined process for trademark holders to file Intellectual Property (IP) infringement complaints that will trigger an investigation that results in the termination or remediation of the merchant account within about 30 days. This self-regulation process is likely much easier to navigate and more expedient than official legal proceedings. However, as with any policy it is imperfect. We found indications based on leaked violation notices sent to banks that Visa Asia is currently levying a fine of $5,000 USD for each IP violation. This is less than the $25,000 fine for mis-coded gambling and illegal pharmaceutical transactions. We cannot confirm that these are the current fine amounts since Visa does not make their self-regulation or fine amounts public. This lack of transparency makes it difficult to understand the impact of payment interventions. We also found that the banks and Visa are likely not refunding any of the money remaining in the counterfeiter's account to the customers or the infringed upon trademark holders. It is unclear what is happening to these funds, but court filings show that the Bank of China previously seized funds from a counterfeiter's account to cover their own legal costs [15]. More transparency about the current IP infringement policies that Visa and MasterCard have set in place for their card association member banks would be useful in understanding the process and potentially improving it.

From the analysis of our two-year study, we were able to identify bullet-proof payment processors that are supporting the online sale of counterfeit goods. These bullet-proof processors appear to be adjusting the level of order filtering and availability of merchant accounts based on the perceived risk of the brand being sold. They are also able to continue to open up new merchant accounts primarily at the Bank of China. We also find through a smaller experiment that our payment intervention likely did not reduce the availability of credit card merchant processing accounts for counterfeit goods associated with other brands. Some of the original bullet-proof processors either closed down or no longer support counterfeit goods merchants. It is unclear if this is correlated with our intervention. However, "start-up" bullet-proof payment processors have emerged.

We found that over time our intervention turned into a "cat and mouse" game where the bullet-proof payment processors would devise new test purchase detection and filtering methods. We, in turn, would devise methods of evading them until the payment processor implemented strict one purchase limits to impede the ability of our purchasers to discover merchant accounts. However, this also likely reduced their revenue from legitimate repeat customers. We overcame this by recruiting additional purchasers at the expense of additional effort in training new purchasers to evade their detection and filtering methods and correctly gather evidence.

Before our study began, luxury counterfeit goods merchants had already largely abandoned more hardened payment channels such as PayPal that will quickly detect counterfeit goods sales and freeze the merchant's assets that are in their accounts. Towards the end of our study we found that luxury counterfeiters were starting to probe newer and less protected pay channels such as Amazon Pay and establishing fake merchant stores on Amazon in order to accept payment for counterfeit goods. This will likely always be an issue of counterfeit goods merchants abusing new payment platforms that have not implemented stronger fraud detection and effective policies for dissuading the use of their payment channels by counterfeiters.

Our payment intervention appears to have increased the perceived risk of fines when bullet-proof processors and banks acquiring payments for counterfeit goods associated with the six brands in our study. This caused many of the bullet-proof processors to forbid merchants from selling these six brands' counterfeit products and implement aggressive order filtering that likely blocks many legitimate purchases. It also appears to have caused some banks, such as those in South Korea and the Bank of Communications, to implement stricter vetting of merchants. If most luxury brands do not also actively work on disrupting payments for their brands then the primary effect of our intervention might be to shift the efforts of counterfeiters away from these six brands and cause counterfeiters to intensify their efforts on other brands. Ultimately, the continued effectiveness of trademark infringement based payment interventions likely depends on what policies and fines Visa and MasterCard are willing to enforce and if additional luxury brands are willing to support IP violation claims.

ACKNOWLEDGMENT

This work was funded in part by the National Science Foundation through CNS-1619620 and CNS-1717062 and by gifts from Comcast and Google. We thank Melissa McCoy for her editing assistance, the anonymous reviewers for their useful feedback, and the many anonymous people that assisted by placing purchases.

REFERENCES

[1] "U.S. Census Bureau QUARTERLY RETAIL E-COMMERCE SALES 4th QUARTER 2017."

[2] D. Y. Wang, M. Der, M. Karami, L. Saul, D. McCoy, S. Savage, and G. M. Voelker, "Search + seizure: The effectiveness of interventions on seo campaigns," in *Proceedings of the 2014 Conference on Internet Measurement Conference*, ser. IMC '14. ACM, 2014, pp. 359–372.

[3] "Online Advertising Techniques for Counterfeit Goods and Illicit Sales," 2014.

[4] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, 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 2011 IEEE Symposium on Security and Privacy*, ser. SP '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 431–446.

[5] D. McCoy, H. Dharmdasani, C. Kreibich, G. M. Voelker, and S. Savage, "Priceless: The role of payments in abuse-advertised goods," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12. ACM, 2012, pp. 845–856.

[6] D. McCoy, A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, G. M. Voelker, S. Savage, and K. Levchenko, "Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs," in *Proceedings of the 21st USENIX Conference on Security Symposium*, ser. Security'12. USENIX Association, 2012.

[7] R. Clayton, T. Moore, and N. Christin, "Concentrating correctly on cybercrime concentration," in *Proceedings (online) of the Fourteenth Workshop on the Economics of Information Security (WEIS)*, Delft, Netherlands, Jun. 2015.

[8] *ISO 8583:Financial transaction card originated messages Interchange message specifications*, Std., 2003.

[9] Qualified payment processors for visa. [Online]. Available: https://www.visa.com.cn/support/small-business/qsp.html

[10] Zhang xiaolei, the actual controller of qianbao.com, has been arrested according to law. [Online]. Available: http://www.xinhuanet.com/2018-02/01/c_1122356205.htm

[11] Qualified payment processors for mastercard. [Online]. Available: https://www.mastercard.us/en-us/merchants/start-accepting/payment-facilitators.html

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

[13] B. Stone-Gross, R. Abman, R. A. Kemmerer, C. Kruegel, and D. G. Steigerwald, "The underground economy of fake antivirus software," in *WEIS*, 2011.

[14] T. Moore, J. Han, and R. Clayton, "The postmodern ponzi scheme: Empirical analysis of high-yield investment programs," in *Financial Cryptography and Data Security*, A. D. Keromytis, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 41–56.

[15] M. Schiefelbein, "Chinese banks a haven for Web counterfeits," http://www.latimes.com/business/la-fi-china-banks-counterfeiting-20150511-story.html, 2015.

APPENDIX A
CONTACTED PROCESSORS

The complete list of the 39 payment processors that we attempted to contact:

GLBPAY, King365pay, PAYWORKS, ONEKPAY, DHPAY, MONEYBRACE, GLOBALPAY, POCKETPAY, SKRILL, WPAYMENT, FASHIONPAY, TENPAY, ALIPAY, GLEEPAY,

SHOPIFY, HOOPPAY, CARDPAY, ETONPAY, SFEPAY, AMOPAY, ALTERCARD, SCOINPAY, PAYEASE, Federal Pacific Credit, SCHOOLPAY, IMPAY, ASIAPAY, PAYDOLLAR, RealyPay, ACCREDITPAY, HSDSPAY, VIMAPAY, GCBILLPAY, NOWIPAY, 99BILL, EZPAY, GHL, IPS, PAYFORASIA.

APPENDIX B
PAYMENT PROCESSORS SUPPORTING COUNTERFEIT GOODS TRANSACTIONS AND THEIR RESTRICTED BRANDS

GlbPay

- **Mastercard Authorized**
- **Restricted Brands**
  - LV
  - UGG
  - MK
  - Coach
  - Katespade
  - Lululemon
  - Abercrombie&Fitch
  - Goyard
  - CanadaGoose
  - Tiffany
  - Gucci
  - VCD
    DVD chanel
  - Toms
  - Swatch and Monster Headphones
  - Brands of watches in Switzerland;
  - Counterfeit Medicine
  - Counterfeit Tobacco
- **Charges**
  - Annual Fee: $5000
  - Transaction Fee: 5%

King365Pay

- **Restricted Brands**
  - Chanel
  - Abercrombie&Fitch
  - Coach
  - Gucci
  - Louis Vuitton
  - Tiffany
  - Michael Kors
  - UGG
  - Canada Goose
  - Oakley
  - Rayban
  - watches
  - Virtual Products
  - DVD
  - Medicines and drugs.
- **Charges**
  - Annual Fee: $5000, $8000, $12000 Depends on which combo the customer choose
  - Transaction Fee: 5%
  - Rolling reserve: 10%, return to merchant account in 180 days

FashionPay

- **Restricted Brands**
  - Chanel
  - Abercrombie&Fitch
- **Charges**
  - Annual Fee: $3000, $4000, $5000 Depends on which combo the customer choose
  - Set Up Fee: Same with Annual Fee
  - Transaction Fee: 8%
  - Rolling reserve: 10%, return to merchant account in 180 days

HoopPay

- **Restricted Brands**
  - Chanel
  - GHD
  - Birkenstock
  - Calvin Clein
  - Levis
  - Abercrombie&Fitch
  - Gucci
  - Louis Vuitton
  - Tiffany
  - Michael Kors
  - UGG
  - Canada Goose
  - Oakley
  - RayBan
  - Longchamp
  - True Religion
  - Goyard
  - Lululemon

EtonPay

- **Restricted Brands**
  - Louis Vuitton
  - Canada Goose
  - Gucci
  - Chanel
  - Toms
  - Calvin Clein

SfePay

- **Restricted Brands**
  - Chanel
  - Canada Goose
- **Charges**
  - Annual Fee: 3000 RMB
  - Transaction Fee: 5%