EXECUTIVE SUMMARY
OCTOBER 2012

# International AntiCounterfeiting Coalition

# *IACC Payment Processor Portal Program: First Year Statistical Review*

Prepared by Kristina Montanaro,
IACC Associate Counsel & Director of Special Programs

This summary has been prepared for presentation to the U.S. Intellectual Property Enforcement Coordinator (IPEC).

## INTRODUCTION

This document summarizes the findings and recommendations of the IACC in its evaluation of the IACC Payment Processor Initiative & Portal Program (the "Portal Program"). The IACC launched the Portal Program in January 2012, after a short beta testing period in December 2011. The purpose of this report is to evaluate the successes and challenges of the program to date, and to provide recommendations for its continued viability.

## PRINCIPAL FINDINGS

Statistics for the program to date have demonstrated remarkable success, with 906 individual merchant accounts terminated as a result of rights-holder reports. Because counterfeiters and other criminal entities often use one merchant account to process illegal transactions for multiple rogue sites, these numbers likely correspond to a much higher number of sites no longer able to take payment.

Despite these successes, there have been significant challenges involved in administering the program. The most significant of these is the propensity of counterfeit sellers to evolve their payment processing systems to avoid detection and subsequent termination. Rogue sites are increasingly relying on the services of a select few illegitimate payment service providers ("PSPs") that utilize highly-sophisticated anti-fraud technologies to intentionally block investigative transactions.

Continued viability of the program will require improvements in trace messaging operations, enhanced collaboration and targeting between program partners, and additional financial investment.

## BACKGROUND

As legitimate retailers have increasingly leveraged the Internet as a platform for sale and distribution of their goods to consumers, so too have counterfeiters and IP pirates. Where such illicit activity was once confined to brick-and-mortar shops, the Internet's maturation as a commercial platform has created new opportunities for sales and advertising of illegal goods, as well as an ever-widening pool of potential customers.

According to data provided by MarkMonitor, in the past decade, there have been approximately 2 billion new Internet users, representing a 425% growth since 2000. In 2010, 1 in 4 consumers reported that they had used the Internet for shopping. It is anticipated that the number of Internet users, and accordingly, the number of Internet shoppers, will only continue to grow in the coming years.

As the e-commerce world has developed, incidents of online sales of counterfeit and pirated goods have grown exponentially among all industries. The Internet provides criminals with a highly desirable environment for illegal sales, as e-commerce is characterized by minimal cost of entry, ease of operation, decreased overhead, and a decreased risk of prosecution.

The Internet has in turn raised various practical difficulties for traditional IP enforcement, including virtual anonymity of infringers, jurisdictional issues, high enforcement costs, inability to collect judgments, and an ease of relocation for the infringer. The U.S. Customs and Border Protection Office of International Trade has noted the "[c]ontinued growth of websites selling counterfeit and piratical merchandise directly to consumers" as a contributing factor to a trend of increased importation of such goods via mail and express courier shipments.[1] Such "direct-to-consumer" trafficking represents a marked shift from the traditional distribution chain characterized by the importation of large-scale, container-load shipments, and eliminates the opportunity for enforcement against mid-level distributors who previously were tasked with getting the product to retail markets after it entered the country. And, whereas in the past, seizures of entire containers of counterfeit goods could be viewed as a significant financial hardship to counterfeiters, the seizure of individual customers' orders have only a minimal impact.

Based on such difficulties associated with traditional enforcement mechanisms, rights-holders have begun to explore alternative enforcement methods. The "follow the money" approach is one such method that has emerged. Because the only real deterrent to counterfeiters is to make counterfeiting less profitable as an industry, payment processing has been identified as an effective choke-point in the fight against counterfeit goods. By working with the payment industry, rights-holders can diminish the ability of counterfeiters and IP pirates to process online payments, thereby decreasing the profitability of their illegal businesses.

The main objective of the Portal Program is to provide a streamlined, simplified procedure that allows rights-holders to report online sellers of counterfeit or pirated goods directly to credit card and payment processing networks in a more time- and cost-efficient manner, thereby facilitating action against the corresponding merchant accounts and diminishing the ability of such sellers to profit from their illicit sales. To implement this program, the IACC has developed an access-controlled portal system to facilitate the flow of information between and among participating rights-holders, the IACC, the National Intellectual Property Rights Coordination Center (the "IPR Center"), and credit card and payment processing network partners (the "Card Networks"), utilizing a master IACC portal (the "Umbrella Portal") as the clearinghouse for such information. The portal system contains analytical tools, as well as a reporting mechanism that provides disposition results and statistical data to the reporting rights-holders.

Card Network partners to the program include MasterCard, Visa International, Visa Europe, PayPal, American Express, and Discover / PULSE / Diners Club. Additionally, the IACC has retained G2 Web Services as the vendor charged with development and maintenance of the

[1] CBP Office of International Trade, Intellectual Property Rights Fiscal Year 2011 Border Seizure Statistics, http://www.ce-ip.com/downloads-free/2011-Border-Seizure-Statistics.html.

portal system. Apart from its role as the vendor for the program, G2 also acts as a monitoring agent for several major credit card and payment processing networks and over 180 acquiring banks.

The Portal Program is dependent on Card Network policies, which prohibit merchants from using card services for illegal transactions. Use of card services for sales of counterfeit or pirated goods constitutes a breach of these policies, and thus provides for remediation of the corresponding merchant account. Because merchants are bound by Card Network policies regardless of jurisdiction, the Portal Program has global reach.

There are currently thirty-one rights-holder participants to the Portal Program. These participants are representative of several product sectors, including apparel, footwear, and luxury goods, electronics, automotive, tobacco, pharmaceutical, business and entertainment software, and consumer products.

## PROGRAM GOALS

The IACC has identified several goals for the Portal Program, as well as underlying strategies to accomplish each overall goal:

- Goal 1: Increase the cost of doing business for and decrease profits to the counterfeiter.
    - Assist Card Networks in identifying merchants who are violating Card Network policies, so that those merchants may lose their ability to process payments and the acquiring banks of such merchants may potentially incur fines for their violations; and
    - Improve investigation techniques, so that it becomes more difficult and more expensive for counterfeit merchants to develop measures to evade detection.[2]
- Goal 2: Shrink the universe of third-party acquiring banks willing to do business with rogue merchants.
    - Maximize financial disincentives for third-party acquiring banks to do business with merchants willing to violate Card Network policies; and

[2] One trend identified over the past few months is that whenever the IACC improves its investigation abilities, the counterfeit merchants will follow suit with enhanced measures to avoid detection by the IACC and the Card Networks. However, any measures taken to avoid detection in turn decreases the market share of the merchant and/or increases the probability that the merchant will be fined. For example, if a merchant employs sophisticated anti-fraud measures in order to block investigative transaction, this will likely increase the cost of doing business, and will also result in a significant decrease in sales to the actual customer. *Infra* p. 25; *see also* Brian Krebs, Rogue Pharma, *Fake AV Vendors Feel Credit Card Crunch*, Krebs on Security, Oct. 8, 2012, http://krebsonsecurity.com/2012/10/rogue-pharma-fake-av-vendors-feel-credit-card-crunch/ (describing how "security measures can be self-defeating").

    - Participate in trainings of payment industry personnel to increase awareness as to the risk associated with taking on counterfeit merchants.

- Goal 3: Facilitate efficient use of resources.

    - Provide a centralized reporting system for rights-holders, with a standardized procedure for submitting claims regarding merchant violations to the Card Networks;
    - Provide for effective use of each program participant's individual expertise;
    - Allow for elimination of duplicate reports from different rights-holders; and
    - Reduce administrative burdens (both for IACC-member rights-holders, as well as the Card Networks).

- Goal 4: Disrupt and dismantle counterfeit networks.

    - Increase intelligence regarding networks of counterfeit sellers and their affiliates; and
    - Encourage collaboration between the payment industry, rights-holders, academic experts, and law enforcement to address criminal networks.

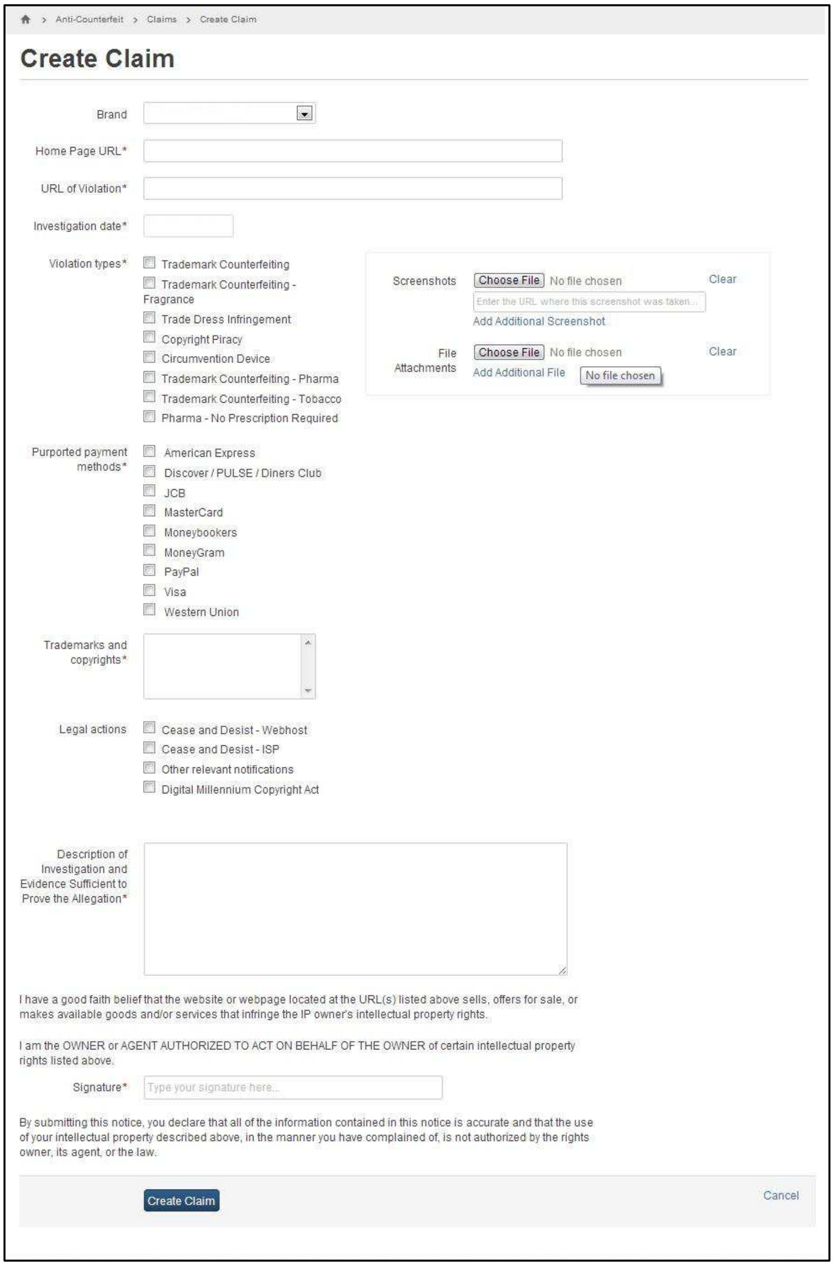
## THE PROCESS

Each participating rights-holder has its own access-controlled, brand-specific portal ("Brand Portal") for submitting reports regarding online sellers to the Umbrella Portal. The reporting process proceeds as follows:

- Step 1: Rights-Holder Investigation
  Each action within the portal system begins with the rights-holder's own investigation. The rights-holder determines which URLs to report through the portal,[3] and must complete a standardized claim form for each individual URL. Each rights-holder may submit a maximum of twenty-five claims per month.[4] The standardized claim form is pictured below:

[3] The IACC has instructed participating rights-holders to select only standalone, rogue websites (as opposed to online marketplaces or auction sites) for submission through the portal system.

[4] The 25-claim-per-month limit is an internal limit imposed by the IACC to help manage IACC and Card Network resources.



> Anti-Counterfeit > Claims > Create Claim

Create Claim

Brand

Home Page URL*

URL of Violation*

Investigation date*

Violation types*
- □ Trademark Counterfeiting
- □ Trademark Counterfeiting - Fragrance
- □ Trade Dress Infringement
- □ Copyright Piracy
- □ Circumvention Device
- □ Trademark Counterfeiting - Pharma
- □ Trademark Counterfeiting - Tobacco
- □ Pharma - No Prescription Required

Screenshots Choose File No file chosen Clear
Enter the URL where this screenshot was taken...
Add Additional Screenshot

File Attachments Choose File No file chosen Clear
Add Additional File No file chosen

Purported payment methods*
- □ American Express
- □ Discover / PULSE / Diners Club
- □ JCB
- □ MasterCard
- □ Moneybookers
- □ MoneyGram
- □ PayPal
- □ Visa
- □ Western Union

Trademarks and copyrights*

Legal actions
- □ Cease and Desist - Webhost
- □ Cease and Desist - ISP
- □ Other relevant notifications
- □ Digital Millennium Copyright Act

Description of Investigation and Evidence Sufficient to Prove the Allegation*

I have a good faith belief that the website or webpage located at the URL(s) listed above sells, offers for sale, or makes available goods and/or services that infringe the IP owner's intellectual property rights.

I am the OWNER or AGENT AUTHORIZED TO ACT ON BEHALF OF THE OWNER of certain intellectual property rights listed above.

Signature* Type your signature here...

By submitting this notice, you declare that all of the information contained in this notice is accurate and that the use of your intellectual property described above, in the manner you have complained of, is not authorized by the rights owner, its agent, or the law.

Create Claim Cancel

In completing the standardized claim form, the rights-holder must include screenshots portraying three aspects of the site: (1) the homepage, (2) a representative product that the rights-holder finds to be infringing, and (3) the payment methods purportedly accepted by the site. If the rights-holder has taken any legal actions (e.g., sending a Cease & Desist letter) in advance of submitting the claim, they may indicate such on the claim form and attach any corresponding documentation, but they are not required to do so. The rights-holder also has the option to complete an additional "test purchase" form, if the rights-holder chooses to undertake a test purchase prior to submitting the claim.

- Step 2: IACC Review & Trace Messaging

  Once the rights-holder submits the completed claim to the Umbrella Portal, the IACC then reviews the claim for sufficiency and compliance with Card Network policies regarding claim eligibility. If the IACC finds the claim to be deficient, it can either reject the claim or send it back to the rights-holder to correct the deficiency. Also during this step, the system will alert the IACC if there is an existing claim pending against the URL in question. If this alert appears, the IACC will merge the new claim with the one previously submitted ("deconflicting" the claim).

  After the IACC reviews the content of the claim, a trace message[5] is conducted. Under the current arrangement with the Card Networks, the IACC has undertaken to conduct all necessary Visa and MasterCard trace messaging for claims originating in the portal.[6] Each trace message is conducted by IACC staff in-house (or in some cases, by G2, at the direction of the IACC). Once trace messaging data is appended to the claim, the IACC will approve the claim for submission.

- Step 3: IPR Center "Hold" Opportunity

  Once the IACC approves the claim, the IPR Center then has a 24-hour opportunity to place a hold on the claim, if it finds that the claim could potentially interfere with ongoing law enforcement investigations. If the IPR Center does not place a hold on the claim within the 24-hour period, the claim is automatically released to G2 for evaluation.

- Step 4: G2 Evaluation

  Provided all threshold requirements are met, the claim will be forwarded to G2. G2 then initiates the merchant identification process by running the URL against the G2 database of known merchant accounts. This database consists of merchant account data G2 has acquired based on its existing relationships with some of the Card Networks and acquiring banks. If the URL is found in the G2 database, G2 can at times identify merchant accounts that would not typically be uncovered by a trace message.

- Step 5: Payment Industry Investigation & Remediation

  After running the URL against its database, G2 then relays the investigation to the identified Card Networks[7] for resolution in accordance with the internal operating procedures and policies of each. The manner for handling the claim then depends on the business model of the individual Card Network, as described below:

[5] A "trace message" is an attempt to make an online purchase using a valid, yet set-to-decline credit card. It is similar to a test purchase, but because the payment is declined, no goods are delivered. The purpose of a trace message is to assist the Card Network in identifying the merchant account associated with the website.

[6] The IACC took on the responsibility of conducting trace messages as a courtesy to the Card Networks for their partnership in the program.

[7] In cases where G2 is able to identify a merchant account apart from the trace message, the claim may be forwarded directly to the G2-client acquiring bank for remediation.

  - **PayPal:** Once PayPal receives a claim, PayPal's investigation team initiates its own version of a trace message, navigating the reported site through the checkout process, to identify the corresponding PayPal merchant account. PayPal may then initiate remedial action against the merchant.

  - **Closed-Loop Networks:** American Express is a closed-loop payment network, meaning that it has direct contractual relationships with merchants.[8] Once American Express receives a claim, it initiates its own merchant identification process, and subsequently, may take action against the merchant account.

  - **Open-Loop Networks:** Visa and MasterCard are both open-loop payment networks, meaning that they do not have direct contractual relationships with merchants, and instead must rely on the appropriate third-party acquiring bank to take action against a merchant. Once Visa or MasterCard receives a claim, each team utilizes the data from the IACC trace message to identify the acquiring bank associated with the merchant, and then relays the investigation on to that bank. The bank then conducts its own investigation, and reports any remedial action taken against the merchant to the Card Network.

    Discover / PULSE / Diners Club has recently altered its business model from a closed-loop network to a primarily open loop network. When Discover / PULSE / Diners Club receives a claim, it initiates its own merchant identification process (including conducting a trace message), and depending on the merchant relationship, will either relay the investigation to the appropriate bank, or may itself take action against the merchant account.

- <u>Step 7: Distribution of Results</u>

  As payment industry investigations are completed, each Card Network updates its corresponding disposition status in the claim summary to reflect any action taken with regard to the merchant account. The reporting rights-holders may access these results in the portal as they are updated by the Card Networks.

[8] This is the general rule; however, in some cases, American Express may take on merchants through third-party acquiring banks. For example, in China, American Express functions as an open-loop network.

## RESULTS

The following results were drawn from claims submitted between December 15, 2011 (the date of the first portal submission) to September 30, 2012.

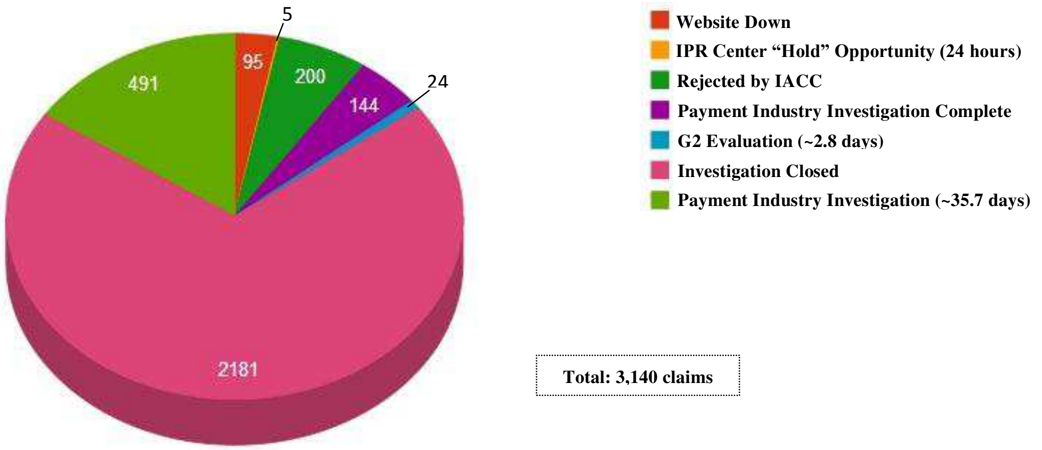
### I. *Results by Claim*

During this period, participating rights-holders submitted a total of 3,140 claims through the portal. The number of claims submitted is broken down by month in the table below:

| Claims Submitted Per Month | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Dec. | Jan. | Feb. | Mar. | Apr. | May | June | July | Aug. | Sept. |
| 31 | 234 | 287 | 413 | 383 | 342 | 373 | 391 | 372 | 275 |

Pie Chart 1 indicates where each claim submitted through the portal system currently lies in the system, as of October 11, 2012.

**Pie Chart 1: December 2011 – September 2012 IACC Portal Claims by Status**



- Websites Marked as Down: The "website down" status indicates that the reported website has become inaccessible at some point before the IACC has had an opportunity to conduct a trace message.[9] Claims in this state remain in a holding pattern, unless and until they later become accessible.

[9] If a reported website becomes inaccessible after the IACC's trace message, the claim will nonetheless continue through the portal process to the Card Networks. So long as the website is accessible during the trace message, the Card Networks can use the trace messaging data to identify the merchant account.

- IACC-Rejected Claims: As Pie Chart 1 indicates, 200 claims have been rejected by the IACC. The IACC rejects a claim if it finds the claim to be noncompliant with the criteria of the Card Networks and the IACC Portal Program. For example, the IACC commonly rejects claims found to be lacking in evidence or falling outside the scope of the Portal Program.[10] The number of rejections dropped significantly in February, when G2 updated the portal to provide the IACC with the ability to send a claim back for "brand re-work" as opposed to rejecting it outright. The number has further decreased over time, as participating rights-holders have become more familiar with Card Network criteria and IACC policies. The number of rejected claims is broken down by month below, along with their percentage of total monthly claims:

| **Claims Rejected by IACC per Month** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dec. | | Jan. | | Feb. | | Mar. | | Apr. | | May | | June | | July | | Aug. | | Sept. | |
| 1 | 3.2% | 60 | 25.6% | 30 | 10.5% | 19 | 4.6% | 17 | 4.4% | 17 | 5.0% | 30 | 8.0% | 14 | 3.6% | 7 | 1.9% | 5 | 1.8% |

- Payment Industry Investigation: Claims in this state have at least one Card Network investigation pending. Claims will remain in this state until all identified "payment channels" (i.e., Card Network relationships) have been updated with a final disposition. The table below breaks down the number of claims currently under payment industry investigation by month submitted by the rights-holder, along with their percentage of total monthly claims:

| **Claims Currently under Payment Industry Investigation, by Month Submitted** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dec. | | Jan. | | Feb. | | Mar. | | Apr. | | May | | June | | July | | Aug. | | Sept. | |
| 4 | 12.9% | 51 | 21.8% | 35 | 12.2% | 55 | 13.3% | 128 | 33.4% | 91 | 26.6% | 34 | 9.1% | 15 | 3.8% | 28 | 7.5% | 43 | 15.6% |

As Pie Chart 1 indicates, the average period from the Card Networks' receipt of a claim until the claim has been updated with a final disposition for all payment channels is approximately 35.7 days. The average payment industry investigation time has decreased significantly over time. The table below provides the average time for payment industry investigation, broken down by claims submitted each month. Please note that these numbers represent only those claims that have completed the payment industry

[10] Generally, claims regarding online marketplace or auction sites are seen as falling outside the scope of the Portal Program, because the infringing sales are not processed through the seller's own individual merchant account. Instead, the sales are often processed through the merchant account for the overall online marketplace site, which may also be used to process many other, non-infringing sales. For this reason, it would be unfeasible to terminate the processing ability of the individual seller without terminating the merchant account for the entire website. It is therefore preferable in these cases for the rights-holder to pursue take-down of the infringing listings through the website's regular reporting avenues.

There are some exceptions to this general rule. For example, in some cases, where the website has been nonresponsive to rights-holder take-down requests, the IACC may approve the claim for submission to the Card Networks. The Card Networks (or the appropriate third-party acquiring bank, as the case may be) can then request that the website remove the reported listings, or may decide to terminate the overall merchant account for the site.

investigation process; thus, the data from later months may not be an accurate reflection of investigation times for all claims submitted in that month.

| **Average Payment Industry Investigation Time (# of days)** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Dec. | Jan. | Feb. | Mar. | Apr. | May | June | July | Aug. | Sept. |
| 52.7 | 50.4 | 38.0 | 36.4 | 30.8 | 27 | 31.1 | 13.3 | 12.2 | 3.5 |

- <u>"Payment Industry Investigation Complete" vs. "Investigation Closed"</u>: Claims in both of these states have completed the full payment industry investigation process. Once a claim has been updated with a final disposition for each payment channel, it will be marked as "Payment Industry Investigation Complete." It will remain in this state until a G2 analyst confirms that all processing steps have been completed and closes the investigation.

### *II. Results by Payment Channel*

From the 3,140 claims submitted during the relevant period, 9,728 payment channels were identifed.[11] This translates to roughly 3.09 identified payment channels for each claim in the Portal Program.[12]

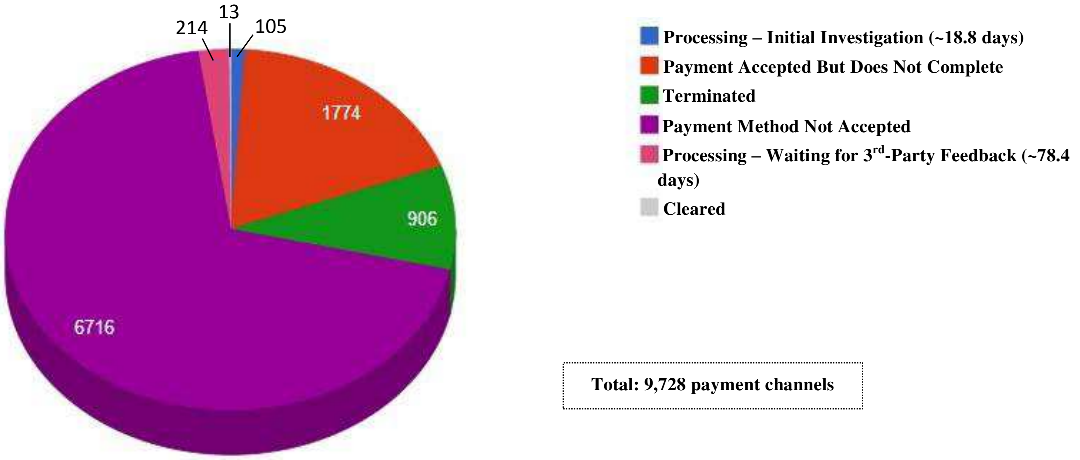
| **Payment Channels Identified Per Month** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Dec. | Jan. | Feb. | Mar. | Apr. | May | June | July | Aug. | Sept. |
| 9 | 284 | 530 | 1,242 | 902 | 1,814 | 1,503 | 1,163 | 1,425 | 916 |

Pie Chart 2 displays the dispositions of all payment channels identified from claims submitted through the portal system, as of October 11, 2012.

[11] The number of identified payment channels measures the number of purported payment methods for each claim where the payment method is an IACC-partner Card Network. For example, if a site advertises that it accepts PayPal, Visa, MasterCard, and Western Union, the claim would then have three identified payment channels (as Western Union is not currently a partner to the Portal Program). Every Card Network that is identified as a payment channel will receive the claim, even if that payment method is not actually accepted upon checkout.

[12] This number is slightly skewed, as PayPal is always identified as a payment channel, even if the website does not purport to accept PayPal. PayPal has requested that the IACC mark it as such, so that PayPal can receive every claim submitted through the portal system. Because in some cases, infringing websites may use PayPal payment services, even though they do not advertise PayPal as a payment method on their homepage, PayPal has undertaken to investigate every website reported by the rights-holders.

**Pie Chart 2: All Payment Channels from December 2011 – September 2012 Claims, by Disposition**



These numbers reflect the overall dispositions for all of the Card Networks. There are seven potential disposition statuses in the system:

1) Processing – Initial Investigation: This disposition is used to indicate that a claim is under initial investigation by the Card Network. During this phase, the Card Network conducts its own investigation and attempts to identify the merchant account. As Pie Chart 2 indicates, the average time for this phase is approximately 18.8 days. The table below breaks down the number of initial payment industry investigations currently pending by month submitted by the rights-holder, along with their percentage of total monthly identified payment channels:

| **Initial Payment Industry Investigations Currently Pending, by Month Submitted** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dec. | | Jan. | | Feb. | | Mar. | | Apr. | | May | | June | | July | | Aug. | | Sept. | |
| 2 | 22.2% | 6 | 2.1% | 3 | 0.6% | 5 | 0.4% | 4 | 0.4% | 0 | 0.0% | 7 | 0.5% | 18 | 1.5% | 15 | 1.1% | 138 | 15.1% |

2) Processing – Waiting for Third-Party Feedback: An open-loop Card Network updates the disposition to this status once it has identified the third-party acquiring bank responsible for the merchant relationship and has requested that the third-party take action to resolve the violation. As Pie Chart 2 indicates, the average time for this phase is approximately 78.4 days. Again, this number represents only those investigations that are complete; thus, it may not be an accurate reflection of current response times.

The table below breaks down the number of investigations currently awaiting third-party feedback by month submitted by the rights-holder, along with their percentage of total monthly identified payment channels.

**Investigations Currently Awaiting Third-Party Feedback, by Month Submitted**

| Dec. | | Jan. | | Feb. | | Mar. | | Apr. | | May | | June | | July | | Aug. | | Sept. | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0.0% | 21 | 7.4% | 51 | 9.6% | 21 | 1.7% | 51 | 5.7% | 152 | 8.4% | 51 | 3.4% | 16 | 1.4% | 11 | 0.8% | 7 | 0.8% |

3) Disputed: This disposition may be used where the merchant disputes the rights-holder's claim, arguing that no content on the website is in violation of Card Network or third-party acquiring bank policies. If this occurs, the Card Network may contact the rights-holder to request indemnification or additional evidentiary support. To date, no claims submitted through the IACC Portal Program have resulted in dispute.[13]

4) Cleared: This disposition is used where the merchant removes the violating content from its website, and the Card Network, or third-party acquiring bank, as the case may be, finds that the merchant is now in good standing and may continue to process transactions. As Pie Chart 2 indicates, 13 investigations have resulted in this status.

   This is a common result where the reported website sells other non-infringing goods in addition to the reported items. Because the IACC Portal Program focuses mainly on true "rogue" websites, which exist solely to make illegal sales, this disposition is rarely used.

5) Terminated: This disposition indicates that the Card Network or third-party acquiring bank has severed its relationship with the merchant and closed the corresponding merchant account. As a result of claims submitted through the portal system, 906 individual merchant accounts have been terminated (9.3% of all identified payment channels). The table below breaks these terminations down by month of submission by the rights-holder, along with their percentage of total monthly identified payment channels:

**Investigations Resulting in Termation, by Month Submitted**

| Dec. | | Jan. | | Feb. | | Mar. | | Apr. | | May | | June | | July | | Aug. | | Sept. | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 22.2% | 67 | 23.6% | 52 | 9.8% | 164 | 13.2% | 82 | 9.1% | 102 | 5.6% | 77 | 5.1% | 103 | 8.9% | 72 | 5.1% | 38 | 4.1% |

[13] In a few claims, the merchants have contested rights-holders' allegations that the advertised products were illegal, but those claims have since been resolved and have resulted in "cleared" dispositions.

Because counterfeiters commonly use one merchant account to process transactions for multiple rogue sites, these numbers likely correspond to a much higher number of websites no longer able to take payment.

Counterfeiters and other criminals use various tactics in setting up merchant accounts,[14] which result in different termination outcomes. Three common tactics include (i) opening multiple accounts at the same bank, (ii) opening multiple accounts at different banks, and (iii) aggregation.

**i. Multiple Merchant Accounts**

A seller may set up multiple merchant accounts at the same acquiring bank in order to manage risk. This allows the seller to spread the risk of charge-backs over multiple accounts to avoid fees, and also provides the seller with other options should one merchant account be terminated.

In some cases, depending on the Card Network, where a third-party acquiring bank reports to the Card Network that it has terminated the merchant account, the Card Network will run a follow-up trace message on the reported website. If the trace message is successful, this indicates to the Card Network that the seller has another merchant account. If this merchant account sits at the same third-party acquirer as the first account, the Card Network will again relay the investigation to the third-party.

**ii. Multiple Acquiring Banks**

A seller sets up merchant accounts at multiple acquiring banks for the same reasons listed above. Similarly, if a third-party acquirer reports to the Card Network that it has terminated a merchant account, in some cases, the Card Network will run a follow-up trace message to identify any remaining merchant accounts.

**iii. Aggregation**

Aggregation is a very common counterfeiter tactic and is in itself a violation of Card Network policies. It is characterized by a single merchant, who acts as a front for a network of sellers, who in turn each may have a network of websites. This tactic provides for anonymity of sellers making transactions through the shell merchant account, and

[14] For more on these tactics, see Attachment 1: Damon McCoy et al., Priceless: The Role of Payments in Abuse-Advertised Goods (Oct. 2012), Section 4.3.

shields those sellers from the due diligence requirements associated with the acquiring bank's "on-boarding" process.

If the acquiring bank terminates the shell merchant account, this results in the termination of payment facilities for all websites processing payments through that account.

This tactic is to be distinguished from the use of legitimate payment facilitators/PSPs. PSPs function in much the same way, in that they form a direct relationship with the acquiring bank to provide payment services for a network of sellers. Legitimate PSPs, however, are registered with the Card Networks and are bound by Card Network policies.

The cost of termination for the counterfeit seller is high. Securing a new merchant account generally takes a minimum of a week, assuming the seller can satisfy the due diligence requirements of the new third-party acquiring bank.[15] As such, merchant account termination can be a highly effective result from the rights-holder's perspective, particularly as compared to website take-downs, which involve a minimal cost to the counterfeit seller.[16]

6) Payment Method Not Accepted: This disposition indicates that the payment method is not actually accepted during the checkout process on the website, although the site may advertise otherwise (e.g., by displaying the payment brand logos on its homepage).

Out of 9,728 total identified payment channels, 6,716 were not actually offered as payment methods upon checkout (69%). These are broken down by month of submission by the rights-holder, along with their percentage of total monthly identified payment channels, in the table below:

**Payment Methods Not Accepted, by Month Submitted**

| Dec. | | Jan. | | Feb. | | Mar. | | Apr. | | May | | June | | July | | Aug. | | Sept. | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 22.2% | 151 | 53.2% | 320 | 60.4% | 795 | 64.0% | 639 | 70.8% | 1,282 | 70.7% | 1,081 | 71.9% | 823 | 70.8% | 992 | 69.6% | 623 | 68.0% |

[15] Attachment 2: Kirill Levchenko et al., Click Trajectories: End-to-End Analysis of the Spam Value Chain (May 2011), Section IV.C.

[16] *See* Attach. 1, Section 2.3 ("[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).

In most cases, rogue websites advertise several payment methods that they do not accept. This provides an air of legitimacy and allows the seller to lure consumers in with familiar, trusted payment brands. Once they arrive at the checkout page, many consumers are then so invested in the purchase that they are less likely to back out when the seller asks that they instead use a less-familiar means of payment, such as a wire transfer or e-check.

While the Card Networks have no means of terminating the payment facilities of these sellers, the portal system nonetheless delivers these claims, so that the Card Networks may take action to address the unauthorized use of their own intellectual property.

7) Payment Accepted But Does Not Complete: After receiving a claim, the Card Network will mark it with this disposition if, at the time of the trace message, the website appeared to accept that particular payment method, and in fact took the card number, but the transaction details do not appear in the Card Network's system (i.e., the transaction was never processed by the seller). This can occur for any number of reasons, including the following:

**a) The merchant account has already been terminated.**
Where a merchant account has already been terminated (possibly as a result of a portal claim regarding another URL), the website may nonetheless appear as if it accepts the payment method. The checkout process may remain fully functional, but the seller will not be able to process the transaction.

b) **The website has a broken e-commerce platform.**
Even where the seller has a functioning merchant account, the seller may be unable to process the transaction due to technical issues with the checkout process or payment processing service.

**c) The website is a phishing operation.**
Some rogue sites will not process the transaction, but will capture the card number for purposes of phishing.[17]

**d) The website employs sophisticated anti-fraud measures.**
Many rogue sites, or more frequently, the PSPs or aggregators utilized on such sites, employ sophisticated anti-fraud software to block

[17] In fact, several cards used for IACC trace messaging have been compromised in this manner.

potentially investigative transactions before they are processed.[18] These programs give every transaction a “fraud score” based on certain indicators, such as whether the geo-located IP address of the consumer matches the billing and shipping address provided during checkout.[19]

Unfortunately, there is no way to identify with certainty the reason the seller failed to process the transaction. In any case, if the seller does not attempt to process the transaction, there will be no record of the transaction in the Card Network’s system. And without such record, there is very little chance that the merchant account (assuming one exists) will be identified and consequently terminated.

As Pie Chart 2 demonstrates, this disposition is quite common. 18.2% of all payment channels have resulted in this disposition (compared to 9.3% resulting in termination). The table below breaks down the number of these dispositions by month submitted by the rights-holder, along with their percentage of total monthly identified payment channels:

| **“Payment Accepted But Does Not Complete” Dispositions, by Month Submitted** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dec. | | Jan. | | Feb. | | Mar. | | Apr. | | May | | June | | July | | Aug. | | Sept. | |
| 3 | 33.3% | 37 | 13.0% | 104 | 19.6% | 251 | 20.2% | 126 | 14.0% | 262 | 14.4% | 287 | 19.1% | 200 | 17.2% | 330 | 23.2% | 110 | 12.0% |

## *III. Non-Partner Card Network Statistics*

As the IACC Portal Program has progressed, commonly-used, non-partner credit card networks and payment service providers have been added to the standardized claim form as purported payment methods, so that the numbers for claims involving these payment methods may be tracked. In addition to partner Card Networks, the portal system now also compiles claims against websites purporting to accept JCB, Moneybookers, MoneyGram, and Western Union.[20]

Because these entities are not currently partners to the IACC Portal Program, they do not currently receive claims through the portal. However, if and when they do join the initiative, all previously-submitted claims involving these payment methods will be provided to the corresponding entities for their review.

[18] Anti-fraud measures, in themselves, have a legitimate purpose. Most websites employ such measures to determine the legitimacy of transactions. Some criminal enterprises, however, utilize these measures to identify investigative transactions and thus avoid detection by the Card Networks.

[19] Attach. 1, fn. 6.

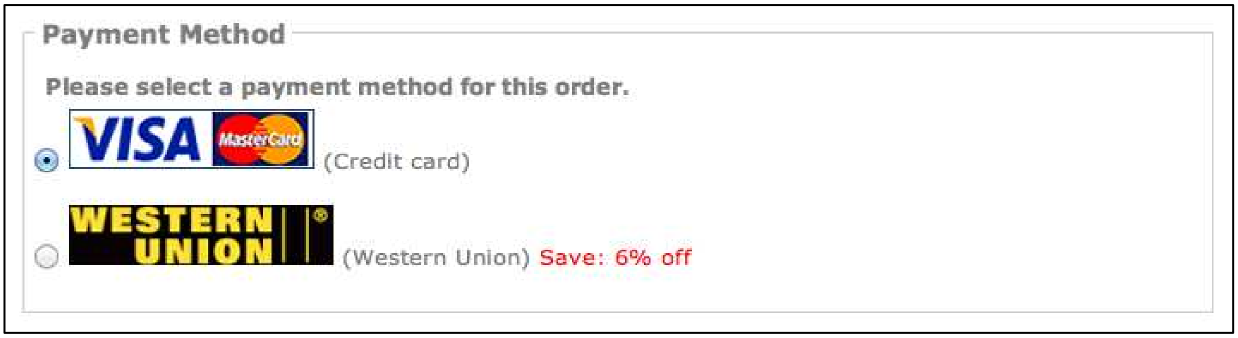
[20] These payment methods were identified by IACC trace messaging analysts as being among the most commonly-advertised on reported websites.

- JCB (Japan Credit Bureau)
  JCB was added to the standardized claim form as a purported payment method in late January 2012. Since the time it was added, it has been identified as a purported payment method in 896 claims (30.1 % of all claims). Beyond being one of the most frequently advertised payment methods, JCB also appears to be one of the more commonly-accepted upon checkout, based on IACC trace messaging data.

- Moneybookers
  Moneybookers, a PSP, was added to the standardized claim form in late February 2012. Since the time it was added, it has been identified as a purported payment method in 128 claims (4.8% of all claims).

- MoneyGram
  MoneyGram was added to the standardized claim form in late February 2012. Since the time it was added, it has been identified as a purported payment method in 89 claims (3.3% of all claims).

- Western Union
  Western Union was added to the standardized claim form in late January 2012. Since that time, it has been identified as a purported payment method in 1,199 claims (40.3% of all claims). Trace messaging analysts note that Western Union has also become more commonly available on reported sites in recent months, with many sites advertising discounts for customers who choose to pay via Western Union (see image below). This may be an indication that counterfeit sellers, now faced with an enhanced risk of termination by the Card Networks as a result of the IACC Portal Program, are increasingly forced to rely on Western Union payments.



Payment Method

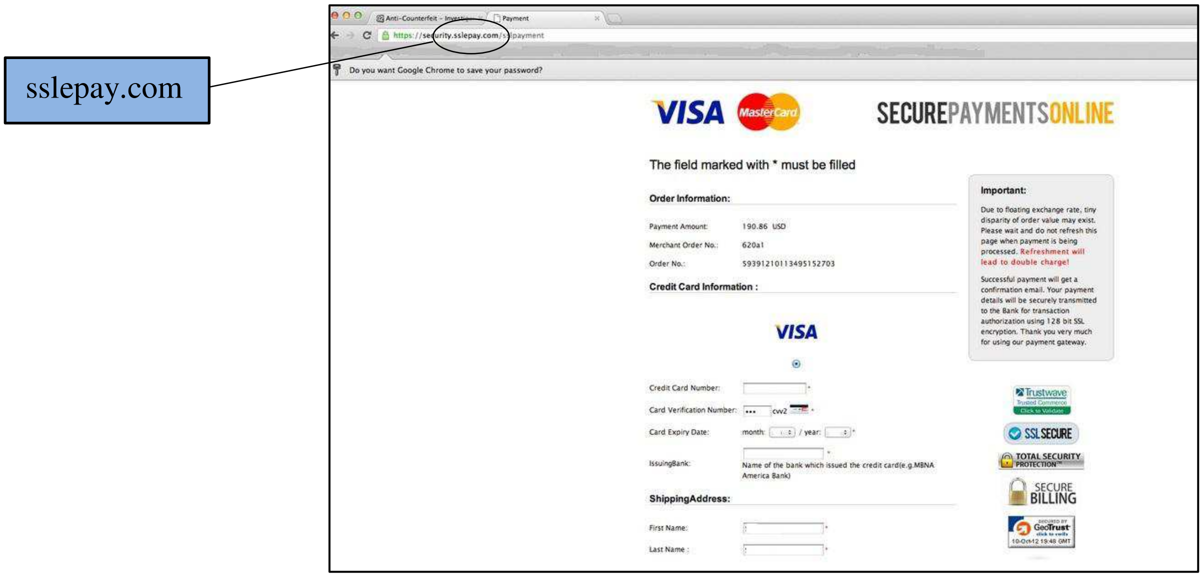
Please select a payment method for this order.

● (Credit card)

○ (Western Union) Save: 6% off

## *IV. PSP Trends*

In late March 2012, the IACC also began keeping record of PSPs[21] used by the reported websites, as identified during the trace messaging process. When the IACC initially began recording this information, the PSPs used by reported sites appeared somewhat varied, and many sites did not use a PSP. However, in recent months, there has been a drastic increase in the number of sites using PSPs, and those PSPs have become decreasingly varied, with more and more sites depending on a select few PSPs for payment processing. The top three most commonly identified PSPs are (1) sslepay.com, (2) realypay.com, and (3) 95epay.com. During checkout on a rogue website, the consumer will typically be redirected from the shopping site's checkout page to any one of these PSP sites. The PSP is easily identifiable by the URL found on the payment form, as shown below:


sslepay.com
Anti-Counterfeit – Investig...
Payment
https://security.sslepay.com/sslpayment
Do you want Google Chrome to save your password?
VISA
MasterCard
SECUREPAYMENTSONLINE
VISA
Trustwave Trusted Commerce Click to Validate
SSL SECURE
TOTAL SECURITY PROTECTION™
SECURE BILLING
SECURED BY GeoTrust click to verify 10-Oct-12 19:48 GMT

The field marked with * must be filled

**Order Information:**

Payment Amount: 190.86 USD

Merchant Order No.: 620a1

Order No.: 593912101134951527O3

**Credit Card Information :**

●

Credit Card Number: *

Card Verification Number: ••• cvv2 *

Card Expiry Date: month: / year: *

IssuingBank: *
Name of the bank which issued the credit card(e.g.MBNA America Bank)

**ShippingAddress:**

First Name: *

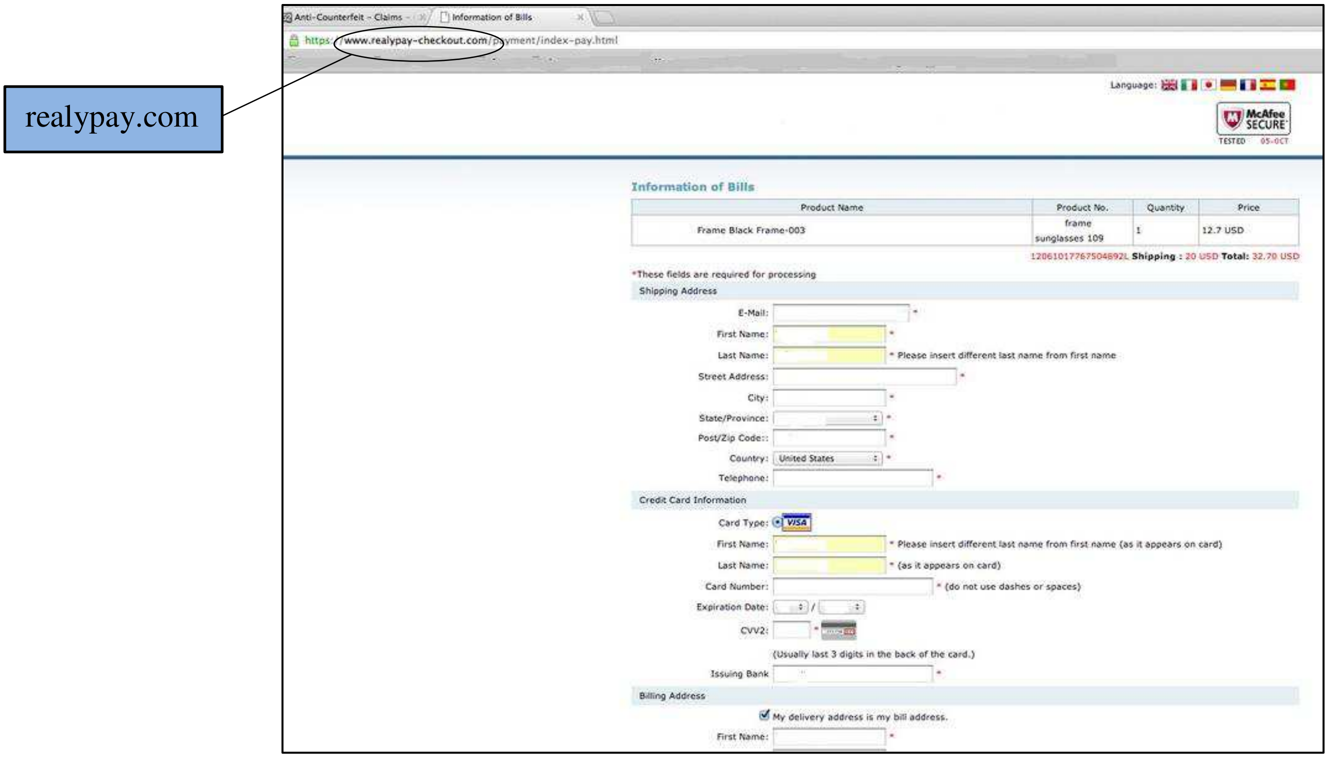
Last Name : *

**Important:**

Due to floating exchange rate, tiny disparity of order value may exist. Please wait and do not refresh this page when payment is being processed. Refreshment will lead to double charge!

Successful payment will get a confirmation email. Your payment details will be securely transmitted to the Bank for transaction authorization using 128 bit SSL encryption. Thank you very much for using our payment gateway.

[21] This report uses the term PSP here in a generic sense, to include both legitimate, registered PSPs and non-registered aggregators, as well as account brokers, merchant servicers, and ISO/MSPs with third-party servicers. For the reader's reference, these terms are not mutually exclusive, as each can provide a variety of different payment services.


realypay.com
Anti-Counterfeit – Claims
Information of Bills
https://www.realypay-checkout.com/payment/index-pay.html
Language:
McAfee SECURE
TESTED 05-OCT

Information of Bills

| Product Name | Product No. | Quantity | Price |
|---|---|---|---|
| Frame Black Frame-003 | frame sunglasses 109 | 1 | 12.7 USD |

12061017767504892L **Shipping :** 20 USD **Total:** 32.70 USD

*These fields are required for processing

Shipping Address

E-Mail: *

First Name: *

Last Name: * Please insert different last name from first name

Street Address: *

City: *

State/Province: *

Post/Zip Code:: *

Country: United States *

Telephone: *

Credit Card Information

Card Type: ● VISA

First Name: * Please insert different last name from first name (as it appears on card)

Last Name: * (as it appears on card)

Card Number: * (do not use dashes or spaces)

Expiration Date: /

CVV2: *

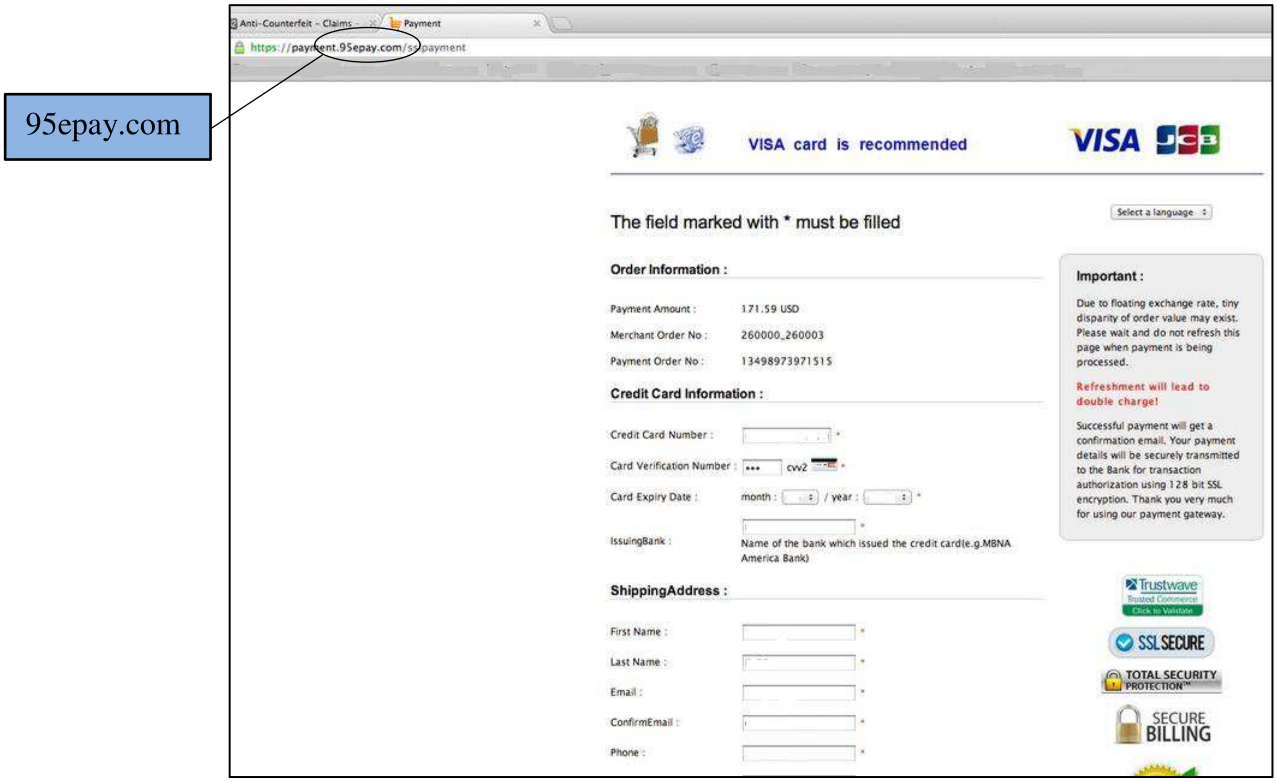
(Usually last 3 digits in the back of the card.)

Issuing Bank *

Billing Address

☑ My delivery address is my bill address.

First Name: *



The field marked with * must be filled

**Order Information :**

Payment Amount : 171.59 USD

Merchant Order No : 260000_260003

Payment Order No : 13498973971515

**Credit Card Information :**

Credit Card Number : *

Card Verification Number : ••• cvv2 *

Card Expiry Date : month : / year : *

IssuingBank : * Name of the bank which issued the credit card(e.g.MBNA America Bank)

**ShippingAddress :**

First Name : *

Last Name : *

Email : *

ConfirmEmail : *

Phone : *

**Important :**

Due to floating exchange rate, tiny disparity of order value may exist. Please wait and do not refresh this page when payment is being processed.

Refreshment will lead to double charge!

Successful payment will get a confirmation email. Your payment details will be securely transmitted to the Bank for transaction authorization using 128 bit SSL encryption. Thank you very much for using our payment gateway.

Other common PSPs include ECPSS Payment Gateway (which appears to be the same entity as sslepay.com), billingcheckout.com (which appears to be the same entity as realypay.com), wedopay.net, sfepay.com, fashionpay.com, glbpay.com, and iPS ePayment. Often, these PSPs will appear as different checkout options on the same rogue site (the most frequent combination being sslepay.com and realypay.com), and the consumer will be encouraged to try each option until finding one that works.

The IACC submits records of commonly used PSPs to the relevant Card Networks each month. The Card Networks have indicated that most of these entities are considered "rogue PSPs," or aggregators, as opposed to legitimate, registered PSPs.

## CHALLENGES

The single most prevailing, yet unanticipated, challenge for the IACC Portal Program has been trace messaging.[22] Since the inception of the program, the IACC has conducted over 5,000 individual trace messages for claims submitted through the portal system. There have been several difficulties associated with this task.

- Trace Messaging Costs

  Currently, all trace messaging efforts are funded by the IACC and participating rights-holders. For the first term of the program, all participating rights-holders were charged a trace messaging fee of $900.00 for the year; however, this amount has not come close to covering the actual costs associated with trace messaging. For those conducted in-house, each trace message costs the IACC $6.00 in labor. For more difficult trace messages, the IACC will often request that they be conducted by G2. G2 charges between $45.00 and $50.00 per trace message.

  In addition to labor costs, the IACC has also made significant investments in the infrastructure required for trace messaging operations. This includes everything from computers, phones, and credit cards, to IT assistance and sophisticated security and privacy tools. Lastly, in May 2012, the IACC opened a satellite office to function as a secure, off-site headquarters for all trace messaging efforts.

- Finding Payment Cards

  In order to protect the identities (and credit scores) of trace messaging staff, the use of personal cards must be avoided. However, finding the appropriate cards to use for trace messaging has presented its own difficulties.[23] In looking for the rights cards, several aspects were evaluated:

[22] This challenge of trace messaging was unanticipated for the IACC; because, based on the best practices documents negotiated with the Card Networks in 2011, the assumption was that the Card Networks would conduct their own trace messaging for the program. The IACC later agreed to undertake this task after subsequent negotiations with the Card Networks, as a good faith effort to alleviate some of the resource strain caused by the sudden increase in rights-holder reports.

[23] For more on the difficulties of finding appropriate payment cards for investigative use, see Attachment 3: Chris Kanich et al., No Plan Survives Contact: Experience with Cybercrime Measurement, Aug. 2011, 5-6.

- **Card Value:** Because the goal of trace messaging is not the actual purchase and receipt of hard goods, which would be cost-prohibitive and present complications regarding shipping and receiving, cards with little to no monetary value must be used. Although the transaction will eventually be declined for insufficient value, the merchant must first submit the transaction through the Card Network system, which creates sufficient record for the merchant account to later be located.

- **Potential for Alias Use:** Because the cards must be used along with created aliases, they cannot be acquired through standard credit card application processes, which present undesirable due diligence complications. For this reason, the only feasible option has been to obtain prepaid cards,[24] which can be purchased anonymously.

- **Access to Transaction Records:** One difficulty associated with prepaid cards is finding a prepaid card issuer that provides cardholder access to transaction records. Only a few issuers provide prepaid cardholders with online access to transaction history, and only a small subset of these few will provide details for transactions that were not approved. Without these details (which typically include the transaction date and amount, merchant name and ID number, and country of the merchant), it becomes much more difficult for the Card Network to locate the merchant account, and for the IACC to confirm that the trace message was successful.

  For the IACC, the solution to this issue was to contact a major prepaid card issuer directly. With the encouragement of one Card Network partner, and for a minimal fee paid by the IACC, the issuer agreed to supply the IACC with a large number of cards with a zero balance, and to provide an online interface (usually reserved for bank use only) with access to transaction details.

- **Number of Cards:** In order to conduct several hundred trace messages per month, a large quantity of cards must be kept on hand. Conducting multiple, consecutive transactions for counterfeit goods using the same card number will often trigger fraud check systems, and this is particularly true when those transactions are consistently declined. Because suspicious

[24] One common difficulty for investigations using prepaid cards is that most U.S. prepaid card issuers, in response to the Credit Card Reform Act of 2009, restrict the use of their cards to domestic transactions, and the cards will thus be declined for any transactions with foreign acquiring banks. *See* Attach. 3, at 5. Because the IACC is not making actual purchases, however, this has not presented an insurmountable hurdle. As long as the transaction shows up in the Card Network system, the reason it is declined is irrelevant.

card numbers are often blocked, trace messaging cards and aliases must be constantly rotated.[25]

- **BIN Diversity:** A related difficulty of conducting consecutive, declined transactions is that when the cards are obtained through a single issuer, the merchant (or PSP used by the merchant) may grow suspicious of, and even block, all transactions for cards with that particular issuer's Bank Identification Number (BIN)[26]. For this reason, BIN diversity is recommended[27]; however, given the difficulties in finding even one bank to accommodate the IACC's trace messaging needs, BIN diversity is simply not feasible at this point.

- Evading Fraud Checks
  The biggest hurdle for trace messaging, and thus, for the entire program, has been in identifying potential fraud check triggers and finding ways to avoid setting them off. Counterfeit sellers and other criminal entities often employ anti-fraud measures to block investigative transactions,[28] and some of these measures can be very sophisticated.

  - **Address Verification Service (AVS)**: Provided through the Card Networks, AVS is a standard tool that verifies the numeric street address and ZIP code that the consumer provided in registration for the card. For this reason, each prepaid card must be registered with the address of the corresponding alias on the issuer's website.

  - **IP Geolocation:** Many rogue websites appear to use fraud check systems that provide IP geolocation tools, which match the IP address location of the consumer to the AVS information, as well as the shipping and billing addresses provided during checkout.

    In order to combat this, the IACC uses a proxy service that allows the trace messaging analyst to select an appropriate IP address location for the alias used. While in some cases this can be a solution, in others, the fraud check system may be able to identify the use of a proxy, and will nonetheless block the transaction. Trace messaging analysts will generally reattempt the transaction without the proxy, but then the IP address location will likely not match that of the alias.

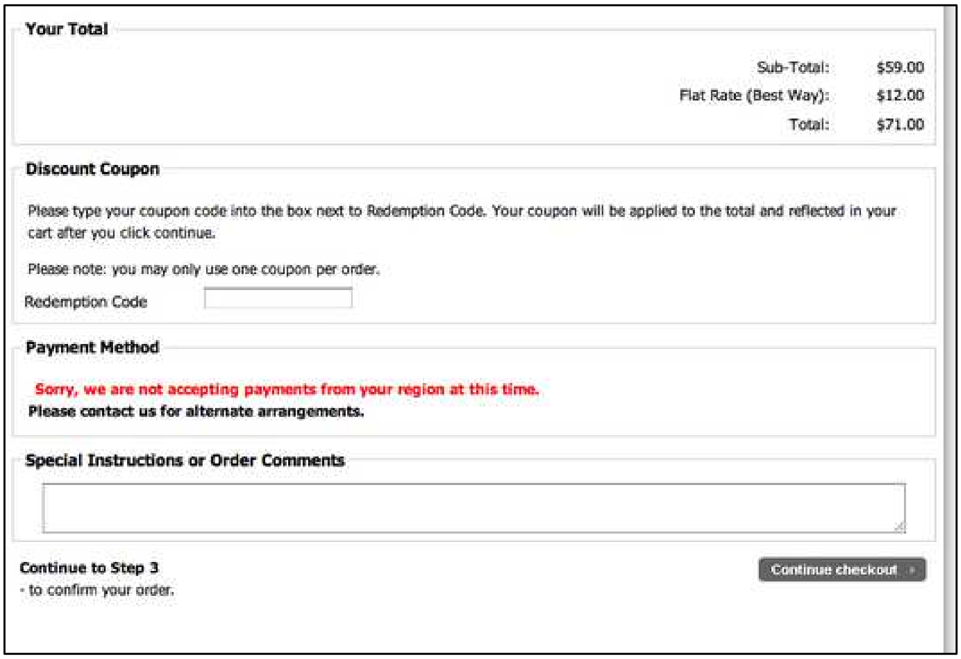
[25] Researchers in this field even advise conducting only one purchase per card. Attach. 3, fn. 3. Unfortunately, this practice is not currently practical, given the volume of claims submitted through the portal system, the cost of the cards, and the constraints on card availability.

[26] The BIN number consists of the first six digits listed on a card. This number is used to identify the issuing bank.

[27] *See* Attach. 1, at 10.

[28] For more information on the use of fraud check technologies by criminals, see Attach. 1, at 10, and Attach. 3, at 5-6.

In addition to geolocating the IP address to determine if it matches the billing and shipping addresses provided, some merchants will filter out IP addresses used for previous transactions that resulted in a decline, or may even blacklist all IP addresses from a particular location. For example, some rogue sites will block purchases for all U.S. consumers, resulting in a message like that pictured below:



**Your Total**

| | |
|---|---|
| Sub-Total: | $59.00 |
| Flat Rate (Best Way): | $12.00 |
| Total: | $71.00 |

**Discount Coupon**

Please type your coupon code into the box next to Redemption Code. Your coupon will be applied to the total and reflected in your cart after you click continue.

Please note: you may only use one coupon per order.

Redemption Code

**Payment Method**

**Sorry, we are not accepting payments from your region at this time.**
**Please contact us for alternate arrangements.**

**Special Instructions or Order Comments**

**Continue to Step 3**
- to confirm your order.

- **Confirmation of Residential Location:** Some merchants will use tools to validate that the shipping address provided is a residential location. In order to combat this, the IACC uses addresses of foreclosed homes for aliases.

- **Email Flagging:** Some anti-fraud measures will flag a consumer's use of a free email account as an indication of risk. The IACC currently uses Yahoo! email accounts for aliases, but is now considering a switch to Google Apps as a host for email services from newly-created domain names.

- **Blocking of Prepaid Cards:** While the IACC has put significant effort into selecting the appropriate cards for use in trace messaging, and has taken all practical measures to ensure that these cards appear to be registered as regular credit cards (i.e., with the name and address of the alias), there is some suspicion that merchants may nonetheless be able to identify the cards as prepaid, and are blocking them as such. Unfortunately, at this time, there appears to be no feasible alternative to the use of prepaid cards.

- **Phone Verification:** Some very sophisticated merchants (most commonly those in counterfeit tobacco and pharmaceutical sales, but in some cases others) will call the phone number supplied by the consumer during checkout to "confirm" the order. This requires the use of various phone numbers during trace messaging, as well as a trace messaging analyst to answer phones and return messages from sellers. The IACC has set up a virtual phone system with several phone lines, which all forward to the same phone at the IACC satellite office.

Nonetheless, this fraud check has presented several difficulties, as the analyst manning the phone is faced with the difficult task of playing whichever alias identity the caller is trying to reach, and improvising in any questions the caller might ask. This can understandably become more awkward (and can result in blacklisting) when one caller makes calls regarding several individual orders placed by different aliases, only to be answered by the same person each time.

- **Documentation Requirements:** In many cases, counterfeit tobacco and pharmaceutical merchants will also request additional documentation, such as copies of drivers' licenses, credit cards, and prescriptions, before running the card transaction. There is currently no way to combat these checks, as the IACC is unwilling to forge identity documents and prescriptions for use in trace messaging.

While the fraud checks described above have always presented a challenge for the program, it appears that in recent months, more and more rogue sites are employing these measures in an effort to intentionally block IACC trace messages.

At the inception of the program in January 2012, there were 94 claims regarding websites purporting to accept one particular Card Network as a payment method. From these reports, IACC trace messaging analysts were able to conduct 53 successful trace messages (56.4%) for that payment method. In 26 (27.7%) of the remaining claims, trace messaging analysts were able to complete the checkout process (entering a full card number), but the transactions were never processed by the merchant (resulting in "Payment Accepted But Does Not Complete" statuses for these payment channels).

In September 2012, by comparison, there were 232 total claims regarding websites purporting to accept the same payment method. From these claims, IACC trace messaging analysts were only able to conduct 7 successful trace messages (3%), compared to 165 (71%) instances where the card number was entered, but the transaction was never processed by the merchant.

The IACC believes that this decline in successful trace messages is in large part due to the fact that rogue websites are increasingly relying on the services of a select few illegitimate PSPs that utilize highly-sophisticated fraud checks as part of the checkout process. In a recent submission to one of the Card Networks, the IACC provided PSP data for sites where the IACC was unable to conduct a successful trace message. The majority of the sites listed relied on two PSPs specifically, realypay.com and sslepay.com, with many of the sites providing both as available payment methods. For this period, about 67% of all instances where the IACC was unable to get a trace message through for this Card Network, the website used one or both of these PSPs.

Perhaps more concerning is the fact that wherever a rogue site uses one of the big three PSPs identified in the section on PSP Trends above (including realypay.com, sslepay.com, and 95epay.com), or one of their related affiliates, IACC trace messaging analysts are consistently unable to get a trace message through.

As explained above, it is very difficult to determine the reason behind an unsuccessful trace message. However, given the patterns identified during trace messaging, the IACC feels certain that the trace messaging issues with respect to these PSPs in particular are owed to the fact that these entities have taken on sophisticated anti-fraud measures in order to deliberately block potentially investigative transactions. This is furthermore confirmed by reports from IACC brands that have received complaints from real consumers who were able to complete card transactions on such sites.

Given the fact that more and more rogue websites are now relying on these PSPs, it would appear that wherever a counterfeit seller wishes to evade detection by IACC/Card Network investigations, there is a very real incentive to turn to one of the big three PSPs for payment services (and these entities are most likely marketing their services to counterfeiters and other criminals accordingly). A simple Google search of each of these entities provides a number of consumer reviews complaining of sites trafficking in counterfeit goods. The actions of these PSPs not only frustrate the efforts of rights-holders, but also introduce an increased risk of fraud in the Card Network systems and damage Card Network reputations to the consumer.

From the rights-holder perspective, the use of heightened anti-fraud measures does have some desirable consequences to counterfeit merchants. For one, these measures represent a significant investment for the seller. Moreover, the use of these measures is accompanied by a high likelihood of false positives (transactions from actual customers often do not satisfy such stringent security checks), which can dramatically reduce sales.

Regardless, the IACC is currently working with the Card Networks and G2 to identify alternative ways to address particularly evasive PSPs.

## NEW DEVELOPMENTS & OFF-SHOOTS OF THE PROGRAM

- Expanded Participant Access

  On September 23, 2012, the IACC extended and expanded its contract with G2. One significant change to the contract was an expansion in the scope of participants permitted access to the Portal Program. The portal system is now available for use by the following entities:

    - IACC-member rights-holders,
    - IACC-member associations and their sub-members (including non-members of the IACC),
    - IACC-member law firms and their IACC-member clients,
    - IACC-member product security firms and their IACC-member clients, and
    - IACC-member investigative firms and their IACC-member clients.

- Enhanced Services Provided by G2

  While system-wide success has been evident, the IACC has nonetheless received requests for additional research and intelligence gathering tools to assist individual rights-holders in quantifying their ROI for the program. Based on those requests, G2 has developed an enhanced services menu, tailored to fit the needs of IACC Portal Program participants, with offerings to compliment the existing portal system. These optional services will be provided by G2 for an additional cost to the participant.

  By expanding access to G2's enhanced services, the IACC intends to increase the efficiency and impact of the system. These enhanced services will allow for rights-holders to take a more targeted approach, based on affiliate network mapping and other intelligence.

- Bank and PSP Training

  One important off-shoot of the Portal Program has been the IACC's collaboration with a few of the Card Networks in training Card Network employees, acquiring banks, and PSPs on the risks associated with taking on counterfeit merchants. Since the spring of 2012, the IACC and representative rights-holders have participated in three such events, including one taking place in Beijing, one in Bangkok, and one in New York. These provide the IACC and rights-holders a valuable opportunity, not only to support the efforts of the Card Networks as partners to the Portal Program, but also to influence the decision-making of those payment industry executives and employees who have the biggest impact on e-commerce.

- IACC "Designs Faux Real" Campaign

  A separate off-shoot of the Portal Program is the "Designs Faux Real" consumer education campaign, which launched in May 2012. The campaign was conceived by the IACC, in collaboration with MasterCard and the IPR Center, as a way to educate the most difficult consumers: those who actively search out counterfeit goods online. The idea was to create a "fake, fake shopping site," which consumers looking to purchase counterfeit goods would visit, thinking it was like any other counterfeit shopping site. While browsing the site, those consumers would then learn about the potential harms of shopping for counterfeits online (particularly, identity theft and credit card fraud).

The www.designsfauxreal.com site is currently live; however, it has not been formally released. The IACC is now working with the IPR Center, so that it might use the site as a public education tool in future Operation: In Our Sites seizures.

## RECOMMENDATIONS

The IACC has several recommendations for continued viability of the program:

- Improved Trace Messaging Operations
  In order for the program to continue its initial success, trace messaging operations must be improved, so that where there is an underlying merchant account, the merchant does not suspect IACC transactions to be fraudulent. The following improvements are recommended:

  - **New Trace Messaging Cards:** The IACC has requested any assistance the Card Networks might be able to provide in obtaining BIN-diverse, non-prepaid Visa and MasterCard payment cards for IACC trace messaging efforts. The IACC takes a number of steps to avoid being blocked by entities that employ anti-fraud measures. At this time, however, the IACC's only option is to use prepaid cards from one issuer source. Accordingly, there is a significant possibility that several merchants and PSPs are blocking transactions from all cards with this issuer's BIN number and/or all prepaid cards.

  - **Enhanced Transaction Details:** Ideally, any issuing bank that is willing to provide cards for trace messaging should also be able to provide additional details for each transaction, including Acquirer Reference Numbers (ARNs), so that this information might be recorded and tracked.

  - **Additional IP Address Options:** In order to avoid triggering fraud checks, the IACC needs to identify options for improving IP diversity. Consultation from professionals in the field would be helpful in this respect, but such assistance requires additional financial investment by the IACC.

  - **Additional Email Address Options:** Similarly, the IACC needs to explore additional options for alias email addresses. As explained above, the IACC is considering a switch from Yahoo! Mail accounts to newly-created domain names hosted by Google Apps.

- **Additional Staff for Trace Messaging:** Additional staff resources to devote to trace messaging operations, including phone verification (which requires several analysts on call to answer phones at any given time) would be very beneficial.

- **Enhanced Targeting Efforts:** In order to maintain continued viability of the program, the IACC, participating rights-holders, and the Card Network partners must work together to come up with a more targeted approach to addressing rogue websites and PSPs. Research by experts in the field has demonstrated that with comprehensive intelligence as to the extent of the particular affiliate network, as well as a persistent "follow up" strategy, concentrated actions taken against key merchant accounts can have a dramatic impact.[29]

  One example of the success of this method is a recent campaign by one rights-holder. Experts believe that the success of that program is in part owed to the relentless tactics of the rights-holder, who targeted all merchant accounts for an affiliate, then aggressively attacked each new merchant account obtained – creating a substantial disincentive for any acquiring bank that previously might have been willing to take on such a merchant. [30]

  Such coordination is crucial for long-term impact. As experts explain, "[t]aking down accounts 'here and there' does raise the cost structure for [merchants], but ultimately it takes focus to convince such operators to close up shop."[31]

  This type of coordinated approach would require extensive network mapping and enhanced intelligence. G2 is one entity that may be capable of providing such assistance, but in order to have maximum impact, it would need to be offered as part of the standard Portal Program (as opposed to just as an enhanced service). This would result in a significant increase to the cost of the program, which many participating rights-holders would not be willing to sustain.

- Additional Program Partners
  In order for the program to evolve with payment processing trends, the IACC needs to secure the partnership of Western Union. As explained above, and as confirmed by external research,[32] it has become increasingly common for merchants faced with Card Network terminations to rely on Western Union payments for continued sales. The IACC has participated in discussions with Western Union regarding its potential partnership in the program; however, these discussions up to this point have been

[29] Attach. 1, at 11.
[30] *Id.* at 9.
[31] *Id.* at 11.
[32] *See id.* at 11.

unproductive, as Western Union insists that the program is not conducive to its business model.

Beyond Western Union, the IACC would like to expand the breadth of the program to include other third-party entities, such as DNS providers, ad networks, ISPs, search engines, and shipping service providers whose logos are also commonly used by rogue websites.

- Continued Participation in Payment Industry Trainings
  The IACC intends to continue participation in Card Network-hosted training events for acquiring banks, PSPs, and Card Network staff, to the extent possible. This may require an increase in program funds to account for travel-related expenses.

- Additional Financial Resources
  Several of the recommendations outlined above require additional financial investment by the IACC. Unfortunately, the IACC is currently running the Portal Program at a significant loss to the organization. The IACC must seek out alternative funding options toward this end.