

BREACH OF TRUST:

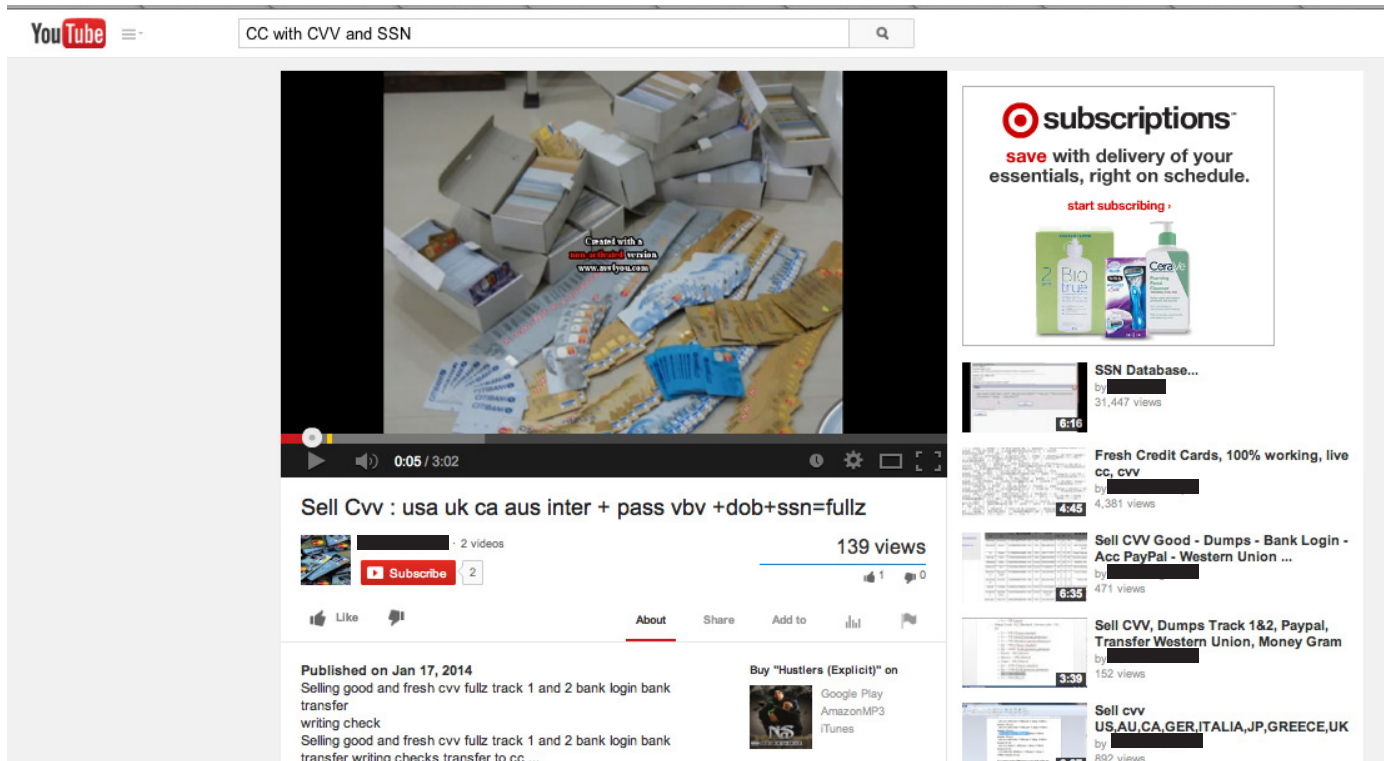
How the Online Market for Stolen and Bogus Credit Cards
is Eroding Confidence in the Internet



When Target acknowledged in January that a hacker had accessed credit card information for 70 million Americans, it created a firestorm of worry about the dangers of credit card theft, shaking consumer confidence and devastating Target's sales.

The fallout was remarkable: More than 80 lawsuits were filed against the company, Target's profit fell 46 percent as it spent over \$61 million to address the breach.

The credit card breach has done remarkable harm to what had been a strong, respected brand. So just imagine what Target executives and employees must think when they see this:



On June 2, Digital Citizens' researchers found this Target advertisement running alongside a video pushing credit cards, social security numbers, and bank logins on Youtube. When we clicked on the ad, we went directly to Target's website. At a time when the company is spending billions to regain trust, how does something like this undermine Target's investment?

Now here's the bad news - and it applies to all retailers as well as consumers.

This problem will continue - no matter how much retailers invest in security - as long as criminals can find a place they can easily sell their stolen credit cards.

The unholy alliance between hackers stealing credit card numbers and online markets advertising stolen and bogus credit cards has existed right under our noses. Hackers have been promoting the sale of stolen or bogus credit cards on online markets for years, including on some of our most popular online websites such as YouTube.

Now here's the worse news.

When someone stumbles onto videos marketing stolen credit cards, as well as other stolen and illegal items displayed on YouTube, the site's parent company, Google, makes money. After seeing in previous Digital Citizens Alliance reports ads running next to videos pushing rogue online pharmacies, performance enhancing drugs, fake passports, and various other items, reporters and law enforcement tried to get answers from Google about this activity.

Harvard Business School Professor Ben Edelman estimates that Google's revenue from the illegal activities of others exceeds \$1 billion dollars.¹ This has gotten the attention of state attorneys general (AGs), which have asked how much money Google makes from illegal activities. Last year, Google responded to a request from AGs by saying it was "burdensome" to provide a "complete answer" on how much the company makes from illegal activity on YouTube.²

But one thing is clear: there is a supply and demand for stolen and bogus credit cards that poses a threat to American consumers. It goes beyond Target, because the problem existed long before security expert and blogger Brian Krebs exposed the Target breach. It has existed for years, right in front of us, and is getting worse, not better.

And perhaps most troubling, it's starting to have an impact on how Americans view online shopping. According to a recent Zogby Analytics survey commissioned by the Digital Citizens Alliance, Americans are worried about whether online shopping is becoming too risky:

- 84 percent of Americans called the issue of thieves hacking into retailers to steal card numbers or stolen credit card numbers showing up online a "serious" issue, with 58 percent calling it "very serious."
- 37 percent of Americans report that they have had their credit card stolen or compromised. Nearly half of those said they never an explanation for or discovered the cause of the theft or compromise.
- Nearly half of all Americans – 48 percent – say that the prospect of credit card theft or fraud has made them more reluctant to make an online purchase.

ANATOMY OF A HACK/CARD GENERATOR

Once hackers get credit card information, they can clone the information onto a new physical card and use it in stores to buy electronics, clothes, etc. that they can then easily resell for cash.

Krebs detailed that "crooks often use stolen dumps to purchase high-priced items such as Xbox consoles and high-dollar amount gift cards, goods that can be fenced, auctioned or otherwise offloaded quickly and easily for cash."

Or, they can simply use the information online to make the same purchases without having to create physical cards and exposing themselves and go directly to ATM's and pull out as much cash as possible using the stolen debit or credit information.

In other cases, credit card numbers are generated to create numbers that mimic real credit cards in order to fool validation algorithms on websites that require you to enter a CC number to join, but that don't charge you. They are used to avoid giving out their real information.

They are not tied to an actual credit or bank account so they cannot be used for real purchases. In the majority of these cases this service is free. When you have to pay for it is when you should be careful.

SILK ROAD - OR YOUTUBE?

These revelations are troubling because our society is invested in the Internet for our future, with much of our economic growth - which means jobs and a solid future for the next generation - tied to the success or failure of our trust with doing things online.

But Americans also expect one more thing: 69 percent surveyed said that websites such as YouTube "should not be in the business of advertising or promoting stolen or fraudulent credit cards."

¹ <http://www.forbes.com/sites/petercohan/2013/11/08/harvard-professor-sees-googles-illegal-revenue-over-1-billion/>

² <http://newsok.com/google-claims-it-makes-little-money-from-videos-with-illegal-or-objectionable-content/article/3873056>

But, unfortunately, they are. YouTube is infested with videos promoting the sale of credit cards. YouTube is one of the most popular websites in the world³ and the most popular amongst teens.⁴ Many marketers of all types see YouTube as a virtual mall where you can not only sell products, but also demonstrate to “shoppers” how those products can be used. That makes it that much more troubling that it is so easy to find and buy credit card numbers on YouTube.

Below are the terms that we searched and the results:

“how to get credit card numbers that work 2014”	15,900 Results
“CC info with CVV”	8,820 Results
“Buy cc numbers”	4,850 Results
“CC number with CVV⁵”	4,160 Results
“CC Fullz⁶”	2,030 Results
“CC Fullz and bank login”	1,790 Results
“CC with CVV and SSN⁷”	785 Results

And many of these videos are embedded with advertisements, which means that Google is effectively in business with crooks peddling stolen or bogus credit cards.

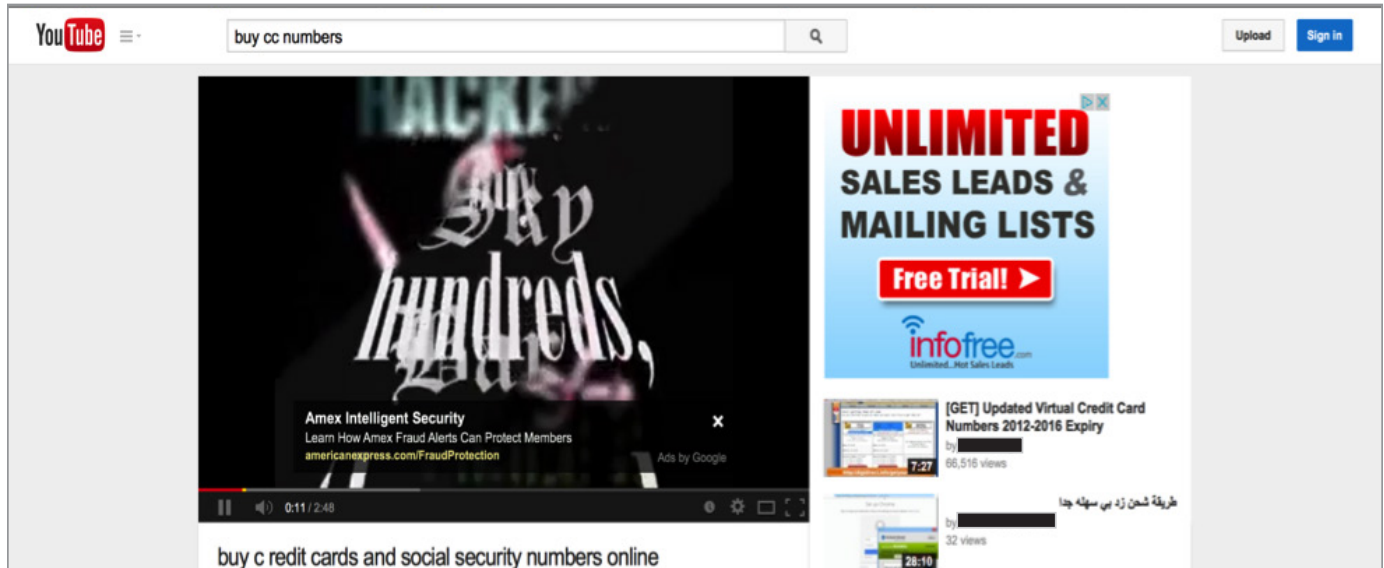
³ <http://www.alexa.com/topsites>
⁴ <http://www.thedrum.com/news/2013/11/06/youtube-more-popular-among-teenagers-facebook>
⁵ CVV = Card Verification Value
⁶ According to creditcards.com, Fullz is “a slang term used by hackers meaning full packages of individuals’ identifying information.”
⁷ SSN = Social Security Number

HOW?

[Google's business is built on ads](#), and YouTube is just one platform that contributes to the \$55 billion in annual sales. YouTube receives more than a billion unique visitors each month. Google makes money by selling ads – to a search term, or a video. Think about when you click on a YouTube video. Sometimes you have to watch an ad before it will run, sometimes there is a banner ad that shows up on the bottom during the video, and other times there are ads that run around the video.

If enough viewers click on those ads, Google will split the ad revenue with the video producer – in this case the crooks that are peddling credit cards.

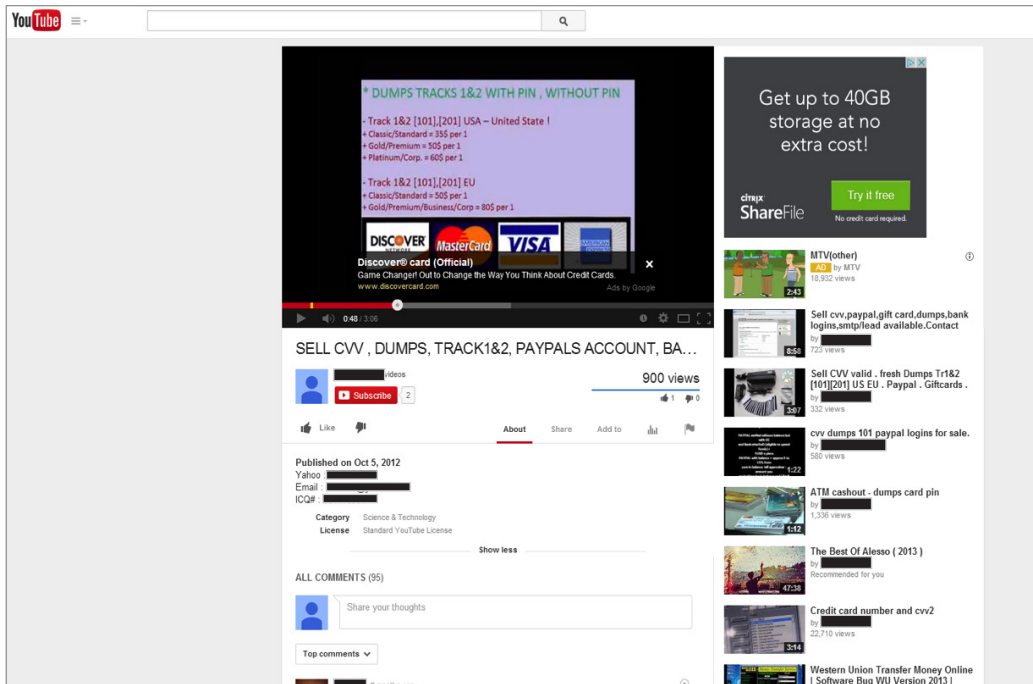
Here is an example:

A screenshot of a YouTube search results page for the query "buy cc numbers". The search bar at the top contains the text "buy cc numbers". The main video player shows a video titled "buy c redit cards and social security numbers online" with a thumbnail featuring the text "HACKED" and "buy hundreds, thousands". Below the video player, there is an advertisement for "Amex Intelligent Security" with the text "Learn How Amex Fraud Alerts Can Protect Members" and the URL "americanexpress.com/FraudProtection". To the right of the video player, there is a large advertisement for "UNLIMITED SALES LEADS & MAILING LISTS" with a "Free Trial!" button and the logo for "infofree.com". Below this, there are two smaller video thumbnails. The first is titled "[GET] Updated Virtual Credit Card Numbers 2012-2016 Expiry" with 66,516 views. The second is titled "طريقة شحن زد بي سهله جدا" with 32 views.

In this screen shot, the search term is “buy cc numbers.” The video producer’s video is entitled “buy credit cards and social security numbers online” and has been up on YouTube since December 2013. The advertising is on the right and embedded in the video.

Look at the ad embedded in the video. It’s for American Express. That means Amex is paying Google to advertise on a YouTube video promoting the illegal sale of credit cards. It is fair to assume that Amex didn’t think that’s where its advertising dollars would go.

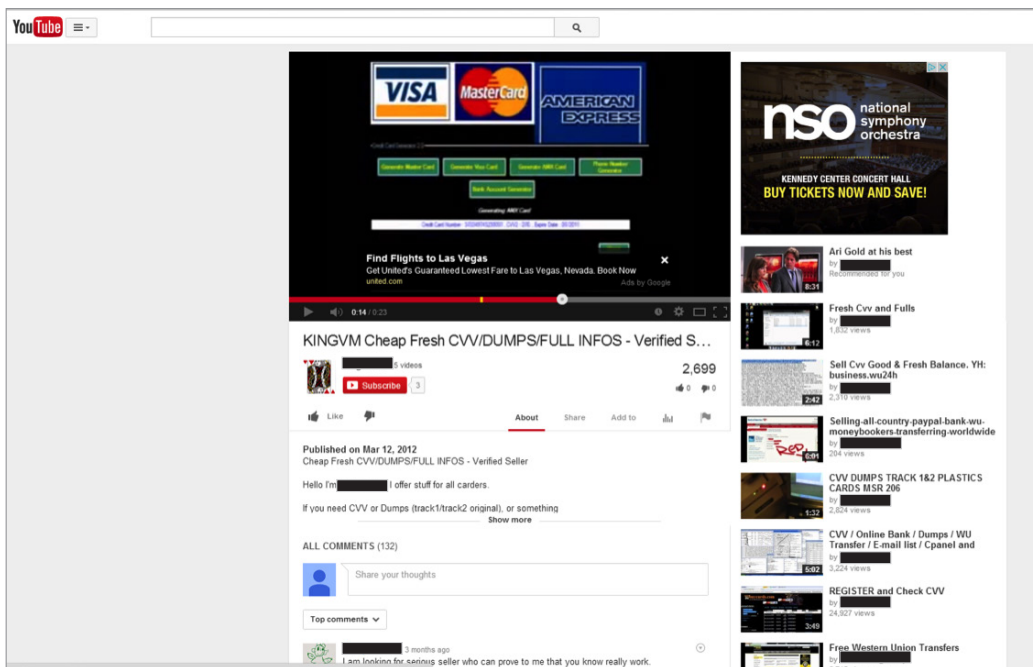
But this isn’t the only video peddling credit cards, and Amex isn’t the only credit card issuer to be associated with it.



The video below shows an ad for the Discover Card embedded in the video.

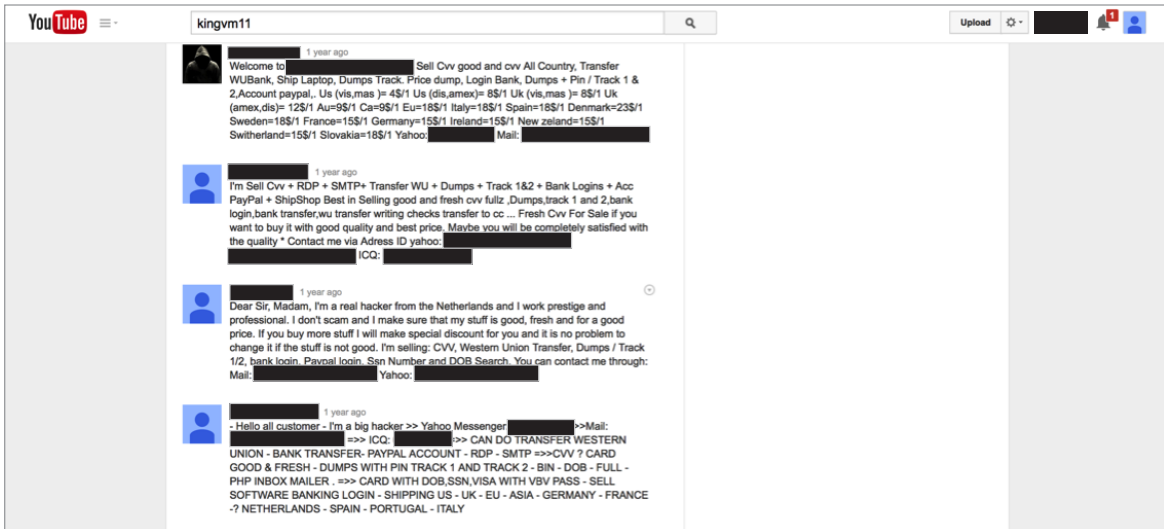
Note that the video has been up on YouTube since October 2012.

This next video below promoting credit cards for sale includes ads for both United Airlines and the Kennedy Center. In both cases, the advertiser is seeking online sales, but presumably not from the stolen or bogus credit cards that are being peddled on this video.

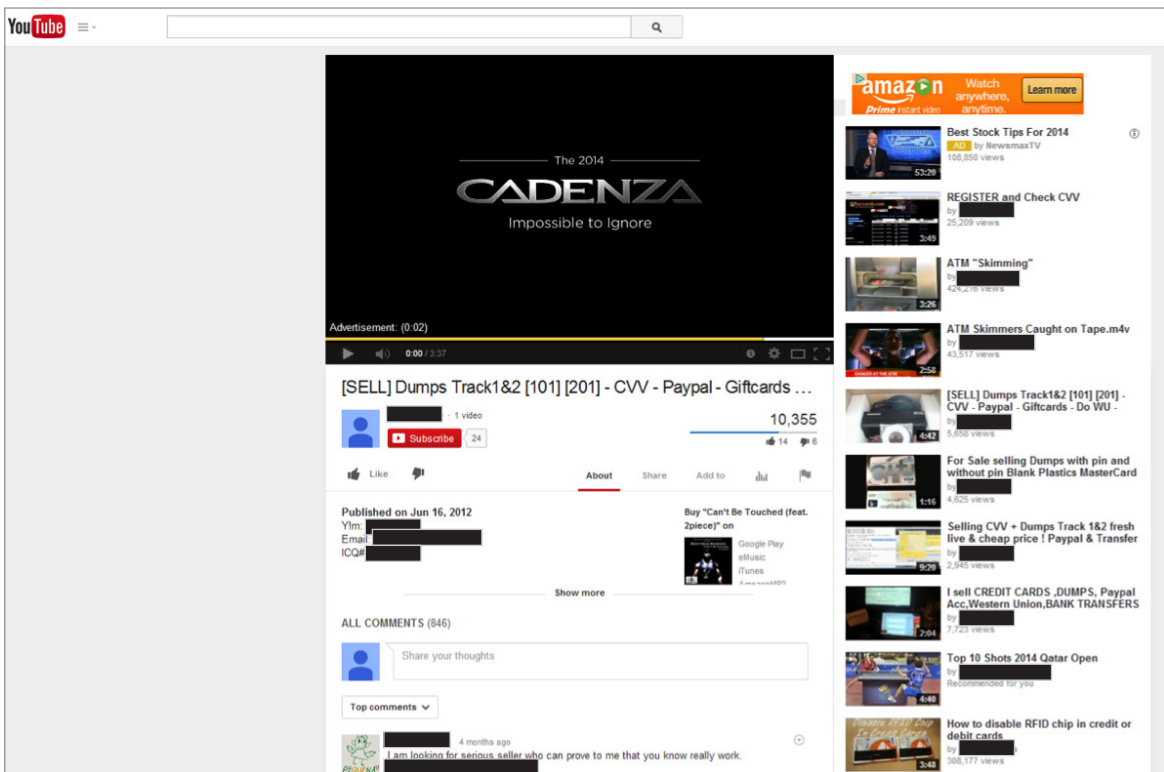


Note that the prior video has been on YouTube since March 2012 and had nearly 2,700 views in that time.

Once the video is on YouTube, other credit card peddlers (or scammers) flood the comment section trying to promote their “businesses.” Here are some comments from the prior video.



Amazon is the world's largest online retailer, selling nearly \$70 billion in goods and services a year. Given their reliance on online commerce, it's unlikely they'd appreciate their advertising showing up on video offering the illegal sale of credit cards, as occurs in the video below.



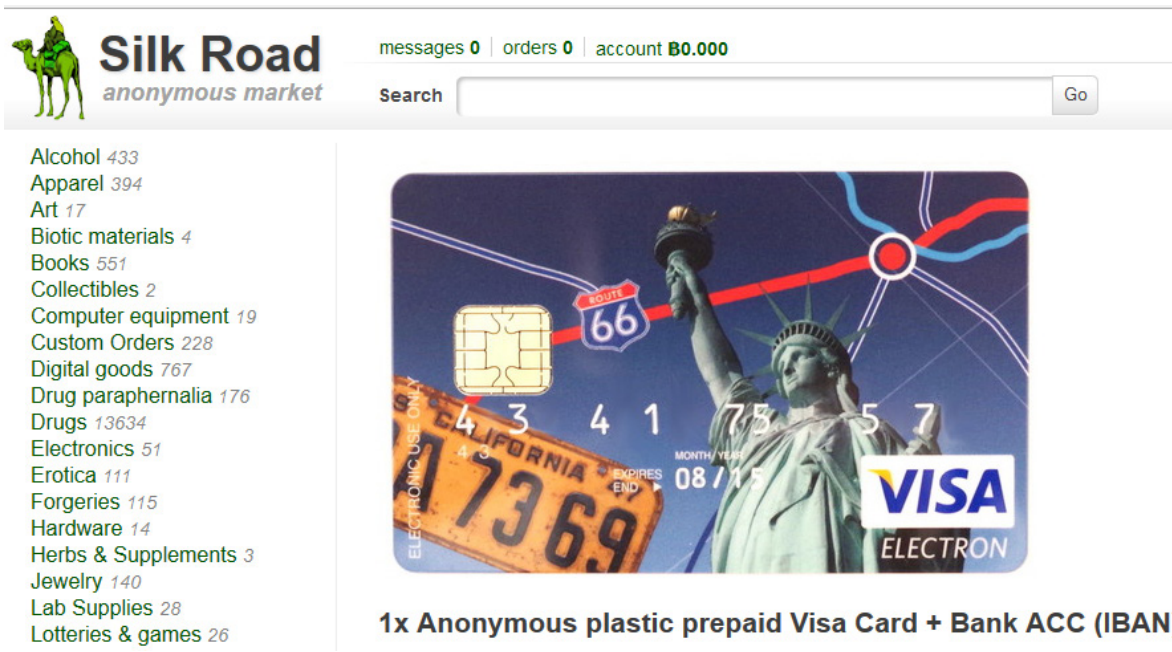
Note that this video has been on YouTube since June 2012, and the video producer's email is "h4ckercc@yahoo.com."

Numerous other brands show up on videos peddling illegal credit cards, from KPMG to Google itself, as shown in the screenshot below. Google should know when its ads show up on its own platform.



Note the Google AdWords video embedded in the video and that while the video has only been up since January 2014, it already has more than 23,000 views.

In some ways, YouTube is mimicking essentially the types of illegal goods associated with “darknet” sites such as Silk Road.



Over the past year, Digital Citizens has raised issues around what is sold on the Internet, from the obscure “darknet” sites such as Silk Road to mainstream sites such as YouTube. Whether mysterious or popular, they seem to have one thing in common: a desire to make money, regardless of the consequences or criticism.

WHAT'S TO BE DONE?

Silk Road was raided by the FBI, only to resurface stronger than ever.

In Google's case, in each instance when the company has been confronted with examples of illegal or dangerous goods and services being sold on YouTube – whether prescription painkillers, steroids, fake passports, forged documents, escort services, or counterfeit – Google's response has been the same:

- First, scrub YouTube to remove controversial videos to stop the criticism and scrutiny. Ultimately, the videos make their way back onto YouTube in ensuing months.
- Second, put out a statement trumpeting all the company is doing to make YouTube safe.

Here's the statement they'll put out after this report is published:

“We take user safety seriously and have [Guidelines](#) that prohibit any content encouraging dangerous, illegal activities...This includes content promoting the sale of drugs. YouTube's review teams respond to videos flagged for our attention around the clock, removing millions of videos each year that violate our policies. We also have stringent advertising guidelines, and work to prevent ads appearing against any video, channel or page once we determine that the content is not appropriate for our advertising partners.”⁸

That's an excellent statement, with just one problem: if Google was actually doing all it could these videos wouldn't exist on YouTube. Once again, Google has to start treating this less like a PR problem to be managed, and more like an Internet safety problem that poses risks and dangers to its users.

Asking Google to stop posting – and profiting – from YouTube videos promoting illegal and dangerous activities seems pointless at this time since they have ignored previous calls to action.

The next stage then seems to be outreach to the brands who certainly don't want to be featured on YouTube videos promoting credit card theft and fraud, illegal drug sales, steroids, escorts or counterfeits.

Our next step as Digital Citizens is to start working with the brands, raising their awareness to the problem and hopefully convincing them to urge Google to step up and take responsibility.

Digital Citizens knows that Google faces a tough job.

Millions of hours of video are downloaded each day onto YouTube. But it's frankly a cop-out for Google to say they can do nothing. Simply flagging videos with search terms such as “buy stolen credit cards,” “buy fake passports,” and “buy prescription drugs without a prescription” for closer review before they are uploaded would make a dent in the problem. But it appears Google would rather take a hands-off approach, perhaps out of fear that taking some responsibility will lead to a slippery slope of more responsibility.

After authorities challenged Google to crackdown on rogue online pharmacies, the company had to shell out \$500 million dollars. That's when Google says it cracked down on such ads. It claims in 2010, ads from unlicensed pharmacies have dropped by 99.9 percent.⁹ When Google decides that a crime is serious, like illegal pharmacies and child pornography, it takes action. Isn't it time that Google stops judging which crimes are serious enough for action and which are tolerable consequences? And just as importantly, isn't it time that they stop profiting from it?

⁸ <http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/10/need-drugs-or-a-fake-id-try-youtube/>

Also:

- <http://abcnews.go.com/blogs/health/2013/10/03/group-probes-ease-and-danger-of-buying-steroids-online/>;
- http://www.washingtonpost.com/business/technology/the-circuit-sprint-and-softbank-deal-said-nearing-fcc-approval-state-ags-eye-youtube-reddit-users-skew-young-male/2013/07/03/f366526e-e3f9-11e2-a11e-c2ea876a8f30_story.html;
- <http://www.cbs58.com/news/local-news/Google-under-fire-over-illegal-prescription-meds-210933101.html?m=y&smobile=y>;
- <http://www.usatoday.com/story/money/2013/06/06/google-profits-on-drug-dealers/2396439/>

⁹ http://www.washingtonpost.com/politics/google-faces-new-pressure-from-states-to-crack-down-on-illegal-online-drug-sales/2014/04/15/6dfc61fa-be6d-11e3-b195dd0c1174052c_story.html

APPENDIX

One conversation comes from a credit card seller found on Silk Road, widely regarded as the world's leading online illegal Darknet Marketplace. The other conversation started after finding a vendor promising credit card numbers to interested shoppers searching YouTube, the world's third most visited website. Can you tell the difference?

IS IT SILK ROAD OR YOUTUBE? YOU BE THE JUDGE....

Digital Citizens Researcher: I am looking to buy some actual fullz and dumps on here. Do you sell that type of info or know any other vendors on here that do that won't scam me?

Appreciate any info you can give me.

Vendor: I just have cvv/cvv2 info. You can usually find all the info you could ever need on the cardholder if they are in the US on intelius.com. 5 for \$95.

Digital Citizens Researcher: So I'm kind of a newb on here to the carding game...what do I get with that? I get the name and the card number and cvv/cvv2 or what?

Just want to be sure we are on the same page before I move forward.

Thanks

Vendor: Card number, type, cvv/cvv2, expiry date, name, address, sometimes phone/email. Have just about any country, lots of US.

Digital Citizens Researcher: Yo man I saw your vid on YouTube. Lookin to get some fullz off you if you're still active.

Get back to me with the cost and what you have available if you're still around.

Vendor: what u need?

Digital Citizens Researcher: Looking for 50-100 Fullz depending on your pricing. What kind of cost am I lookin at?

Vendor: country u want?

Digital Citizens Researcher: U.S.

Vendor: USA:

- Visa Card = 4\$
- Master Card = 4\$
- American Express = 9\$
- Discover Card = 9\$
- DOB = 12\$

SEE ANSWER ON THE NEXT PAGE

Digital Citizens Researcher:

Awesome thanks for the clarification...If I needed cards from specific states to try and stay under the radar a bit longer do you do that? Would that cost me extra?

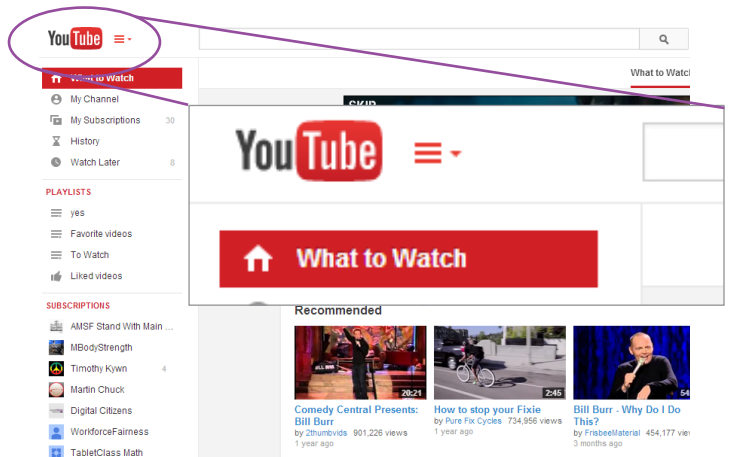
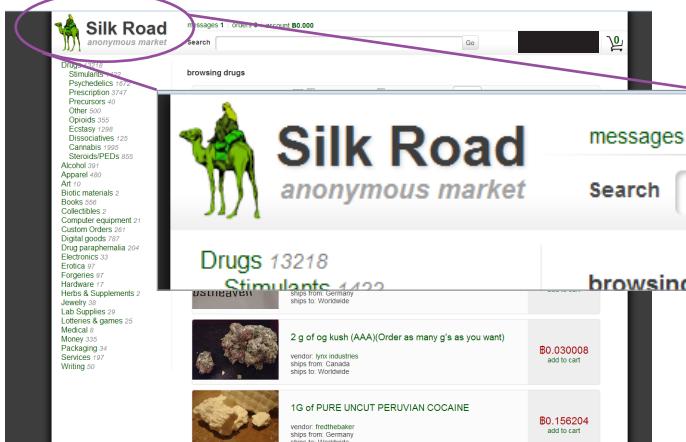
Also, do you have Visa, Mastercard, AmEx? same 5 for 95 for each?

Vendor: I have everything. Add \$4 for each amex you want, no charge for specific state.

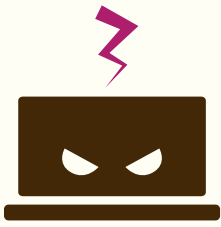
Digital Citizens Researcher: Alright and does price come down if I order in large volume say 100 or so? do you have different thresholds or the same price no matter what?

Vendor: Yes, I can do volume discounts. Once you make a purchase tell me how many you want of which and from where and I will give you a nice price.

- Pass VBV = 10\$
- BIN = 12\$
- Fullz = 20\$



Digital Citizens Alliance found another vendor promising to sell credit cards on YouTube and eventually got him to speak on the phone. That conversation can be found on the [Digital Citizens Alliance website](#).



5 THINGS

Consumers Should Know About the Recent Cyber Attacks on America's Retailers

Recent revelations that several of America's retailers were victims of a malicious data breach sent millions of consumers reeling as they realized their personal information was at risk. Here at Digital Citizens, we want to make sure you are aware of the resources available to you during this difficult situation regarding your online personal information.

1 FREE CREDIT MONITORING



Target, for instance, is offering one year of free credit monitoring to all victims of this attack.

2 MONITOR YOUR BANK STATEMENTS

Financial institutions have issued new credit and debit cards to affected consumers. If you see suspicious activity on your bank statements, call your institution immediately.



3 BUSINESSES ARE INVESTING RESOURCES TO EDUCATE CONSUMERS

Millions of dollars have been committed to help educate consumers on the threats of online scams.



4 YOUR SOCIAL SECURITY NUMBERS ARE SAFE



The recent credit card hacks did not compromise individual social security numbers.

5 YOU ARE NOT RESPONSIBLE FOR FRAUDULENT CHARGES

Either your bank or the retailer has that responsibility.



What should you do? Take the following steps to protect your online financial information:

- ✓ Change the passwords to your online financial digital properties frequently.
- ✓ Review your digital banking statements in detail.
- ✓ Never give your credit card or bank information online to a website you are unsure is legitimate.

If some of the largest retailers in America can be a victim, you can too.

PROTECT YOURSELF ONLINE.

ABOUT DIGITAL CITIZENS

This report was created by the Digital Citizens Alliance, a nonprofit 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet and the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place.

While all Digital Citizens hold themselves personally responsible to do all they can to protect themselves and their families, we are also concerned that technologies, standards, and practices are in place that will help keep all of us safe as a community. The industry has a critical role to play in ensuring those safeguards are established and updated as needed to address the continually evolving challenges we face online.

We have much work to do, but we can't do it effectively without understanding the problems we face.

That is why the Digital Citizens Alliance investigates issues such as those detailed in this report. By sharing our findings with consumers, we hope all Digital Citizens will engage in discussions about these issues.