

- > Multi-Channel Fraud Detection
- > Anti-Phishing
- > Anti-Malware / MITM / MITB
- > Multi-Factor Authentication
- > Real Time Anomaly Transaction Qualification

Exposé of a Credit Card Black Market

Slicker than Amazon

> **Executive Summary**

The massive Target credit card breach continues to make headlines as Target executives testify to Congress, and lawmakers try to (unsuccessfully) engineer legislation to prevent this sort of thing from happening again. However, what's been lost amidst the bluster is another important question: what exactly happened to those 40 million compromised credit cards? How do they get packaged up and sold? How sophisticated are these markets?

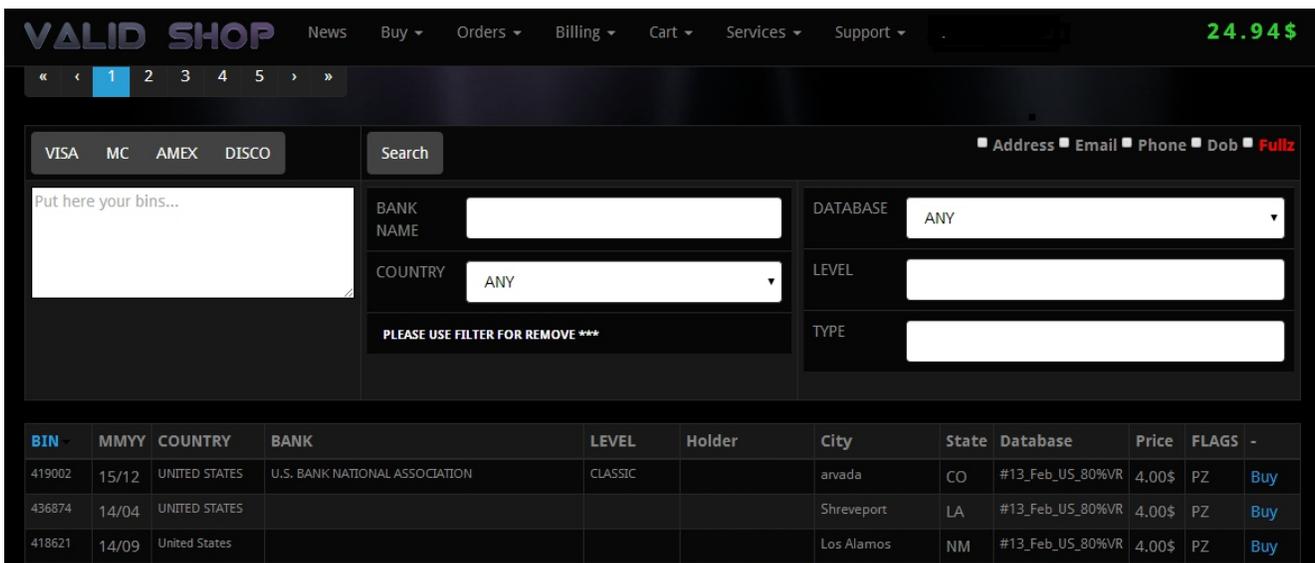
As part of the company's total fraud protection platform, Easy Solutions closely monitors these illicit marketplaces. To help raise industry awareness, this report provides a guided tour of the shadowy world of the black market credit card sites, and exposes one of these sites – **Valid Shop**. It demonstrates what it looks like when an individual's credit card information is made available, how criminal syndicates bundle and price stolen credit card data, and how surprisingly professional these sites can be. Now exposed, this black market will be no more, and criminals will move on to others out there.

> **Key Findings**

- Credit card black markets are now as, if not more, sophisticated than **Amazon.com**, offering support and services in addition to 'product'
- They harness the latest web development technologies, such as **Ajax**, to make searching for and buying specific cards incredibly easy
- **BitCoin** continues to be the preferred methods for transactions, though Perfect Money, and wire services (like Money Grant/Western Union) will also do
- Sophisticated markets even offer “**try on the fly**” service, to ensure the stolen card you've just purchased is valid and can still be used

> *Black Markets – As Sophisticated as Amazon.com*

New stolen cards are always showing up in the black markets, whether they come from a breach, an unencrypted transactional log file a piece of malware or simple a traditional skimmer device. Just like any other ecommerce site, Valid Shop and other black markets aim to provide a seamless buying experience for their end customers – the people purchasing these cards to then go out and use them. Many sites include functionality typically seen on an e-commerce site – product information, shopping carts, industry news, and even services and support offerings.



The screenshot shows the Valid Shop website interface. At the top, there is a navigation bar with links for News, Buy, Orders, Billing, Cart, Services, and Support. A price of 24.94\$ is displayed in the top right corner. Below the navigation bar is a search area with tabs for VISA, MC, AMEX, and DISCO. A search box contains the text "Put here your bins...". To the right of the search box are filters for BANK NAME, COUNTRY, DATABASE, LEVEL, and TYPE. Below the search area is a table of stolen cards with columns for BIN, MMY, COUNTRY, BANK, LEVEL, Holder, City, State, Database, Price, FLAGS, and a Buy button.

BIN	MMYY	COUNTRY	BANK	LEVEL	Holder	City	State	Database	Price	FLAGS	-
419002	15/12	UNITED STATES	U.S. BANK NATIONAL ASSOCIATION	CLASSIC		arvada	CO	#13_Feb_US_80%VR	4.00\$	PZ	Buy
436874	14/04	UNITED STATES				Shreveport	LA	#13_Feb_US_80%VR	4.00\$	PZ	Buy
418621	14/09	United States				Los Alamos	NM	#13_Feb_US_80%VR	4.00\$	PZ	Buy

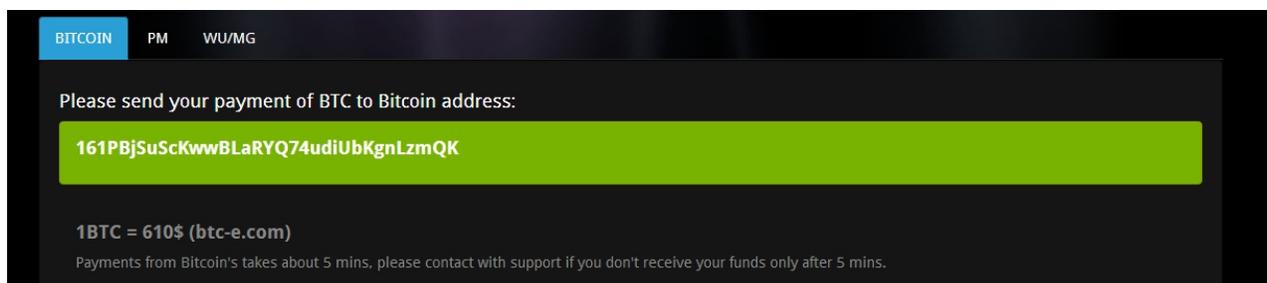
Leveraging the latest web development technologies, such as Ajax, the interfaces for these black markets have become richer and richer. They provide highly “user-friendly” functionality that allows a buyer to search for their target in two or fewer clicks. For example, buyers can search for target by type of card, bank, geographic location, or even the original card owner's name.

Sophisticated criminals can very granularly purchase cards, based on many criteria, including:

- The country of origin
- The BIN
- The type of card (VISA vs AMEX, depending on your expertise/prior success rate)
- Quality of cards (Standard, Platinum, Black, etc)
- The reputation of an specific stolen list (Target, Neiman Marcus, etc)
- Issuing bank (especially useful if the criminal knows a specific bank is not using various protections)

> *BitCoin Continues To Be Preferred Payment Method*

Bitcoin continues to be the preferred method of payment for these black markets, and is the default payment method (first tab) for Valid Shop. Once the buyer clicks to pay, a unique “non-traceable” Bitcoin address is created, waiting for money to be deposited.

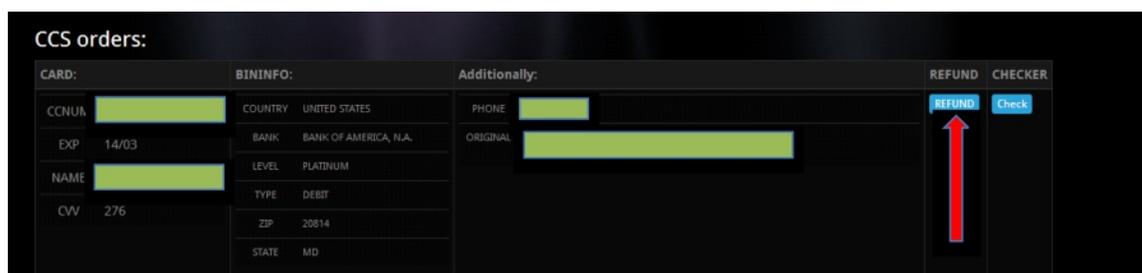


Perfect Money is also accepted in some forums, as are wire services such as Money Grant or Western Union (and in some countries, this is the only option). While these services typically require physically going in to a retail store, criminals have also found creative ways to avoid exposing themselves to cameras when they make that transaction. In other words, the payment methods for purchasing stolen credit cards remain virtually untraceable, and continue to grow more sophisticated every day.

> *“One-click” buying, easy checkout, and money-back guarantees!*

Like any other good e-commerce provider, Valid Shop and other credit card black markets make it as easy as possible to purchase your desired products. Just like Amazon, Valid Shop offers “one-click” purchasing options, to fill all of your impulse credit card purchase needs.

In addition (and currently not offered by Amazon!), Valid Shop offers customers the ability to try the product you have selected on the fly, and make sure that stolen card you just bought is valid and accepted online (at least). In addition, the site provides a “money-back guarantee”. With Valid Shop, you can ask for an instant refund. Other sites automatically refund your purchase price if the card is instantly declined.



> **Conclusion**

Web technologies have enabled all types of commerce sites, including those dedicated to selling illegally-obtained credit card numbers, to improve their searchability, order processing, and overall customer service. Criminals will continue to improve the quality of these sites, making it ever easier for the end-buyers to target their usage of these cards.

Banks and other financial institutions are fighting an asymmetrical war against these highly-organized, well-run markets. Compromise of these cards is inevitable. In understanding these black markets, our hope is that providing organizations the ability to rapidly identify which cards are compromised, and reducing the time to containment/replacement, organizations will be able to better protect themselves and their end customers from increasingly sophisticated fraud.

> **About Easy Solutions**

Easy Solutions delivers Total Fraud Protection to over 200 clients with more than 50 million end users. The company's products protect against phishing, pharming, malware, Man-in-the-Middle and Man-in-the-Browser attacks, and deliver multifactor authentication and transaction anomaly detection. The company witnessed 80% subscription revenue growth in 2013, marking the best year-over-year growth rate since the company was founded. Easy Solutions is projecting another year of rapid growth with internal forecasts calling for 150% growth in 2014 as the company further expands in the North America and EMEA markets.

For more information, visit <http://www.easysol.net>, or follow us on Twitter [@goeasysol](https://twitter.com/goeasysol).