**Fraud Trade on dark web –**

“The dark web, often inaccurately portrayed as a playground for hitmen and human traffickers, is a place where fraudsters leverage tools, tactics, and technology to build scalable business models, collect and co-opt sensitive data, and exploit organizations around the clock.”

### **Dark web fraud trade**

Previously, dark web transactions relied on payment processors like PayPal and Western Union to pay for goods and services. Those services required a certain level of user information to transact, and law enforcement leveraged those user details to arrest buyers and vendors. This isn’t a sustainable system for building a large-scale criminal economy. Cryptocurrency changed everything.

Within the criminal communities on the dark web, fraudsters have built entire e-commerce platforms designed to trade in illicit goods and services. The infamous Silk Road marketplace, launched in 2011, was the first market to combine the anonymizing dark web technology with the power of anonymous cryptocurrency transactions.

Silk Road became a model for all future dark web marketplaces. At any given time, a handful of large-scale criminal marketplaces operate on the dark web, each with thousands to tens of thousands of listings for illicit goods and services. These marketplaces use familiar site structures, akin to the user experience of browsing on Amazon or eBay. On these markets, users can browse listings by category, navigate vendor advertisements, filter their search options by price, location or vendor reviews, and message the vendors or market administrators with questions.

These marketplaces — like Empire and Berlusconi — rely on mutual anonymity and reputation. Vendors encourage positive reviews for their products and prioritize customer service, offering to troubleshoot software or to replace defunct digital goods. In exchange for these efforts, vendors receive reviews and “vendor trust level” rankings, which helps them capture more market share for their particular good or service.

Established platforms allow vendors — particularly fraud vendors dealing in digital goods — to automate and scale their operations. Many fraud vendors use an auto-delivery mechanism for their listings, which ensures buyers receive the volume of data purchased immediately after checkout. In this way, vendors can continue to turn profits and move inventory around the clock.

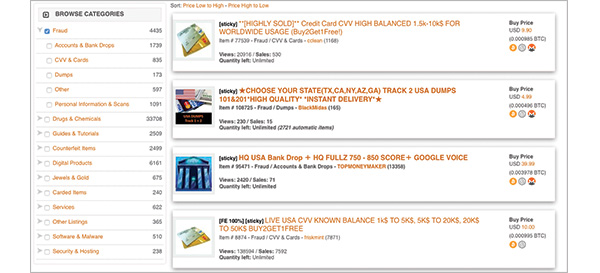
Additionally, criminals have created a wide range of fraud forums and independent shops. Many independent fraud shops are dedicated entirely to the sale of compromised payment cards (like the [famous release of payment cards](http://tinyurl.com/puft5hr) from the Target breach). Buyers can filter listings on a range of card-specific attributes (e.g., issuing bank, expiration date) and receive discounts for buying data in wholesale quantities. Forums provide a marketing and networking platform where vendors can promote links to their goods and services, and interface with customers. Forums also give fraudsters a platform to request specific goods and services, whether they’re seeking access to specific types of financial data or are looking for partners to assist in money laundering.

The dark web fraud economy follows the same economic patterns as traditional commerce: New vendors enter the scene promising differentiated value from their competitors, established shops announce holiday sales and new inventory, and buyers — determined to destroy the reputation of the responsible vendors — take to the platform expounding negative experiences and scams.

These established platforms and economic flows speak to the maturity and resilience of the dark web fraud economy. Media often paints dark web interactions as code-based interfaces in darkened rooms where transactions occur through the digital equivalent of back-alley trades. However, the reality is far more mundane and familiar — and all the more concerning for its practicality.

### **What are criminals buying?**

After drugs, fraud materials are the most popular listings on dark web markets. Fraud materials fall into five main categories: personal data, financial data, guides and templates, software and fraud services.



*An example of fraud listings on a major dark web market.*

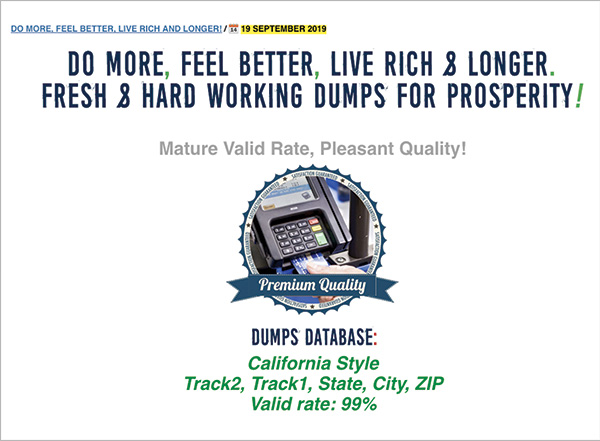
**Personal data**

The dark web fraud economy is built on compromised data, and the steady stream of breaches and exposures have contributed to the proliferation of personal data on the markets. Vendors sell everything from music-streaming accounts to credit reports, health records to full identity kits containing complete sets of personal and financial information.

Some fraudsters also openly leak PII — free for anyone to use or exploit. Long lists of usernames and passwords, email addresses or contact information float freely around the dark web. Users repackage and remarket data from different sources over time; fraudsters might sell or leak the same data set hundreds of times over, and each new leak or sale increases the risk to the individuals or organizations involved.

**Financial data**

Financial data on the dark web typically appears as payment card information, banking information or payment processor accounts. Unlike personal data, financial details aren’t leaked quite as frequently. PII allows fraudsters to carry out a wider range of fraud schemes over time, but financial information offers immediate cash-out opportunities — financial accounts are typically shut down as soon as an unauthorized transaction takes place. Vendors typically safeguard full card numbers until after buyers make a purchase, and any fraudster in possession of financial data would extract all monetary value from the accounts before sharing remaining details with the broader fraud community.



*An example of an advertisement from a carding market on the dark web.*

Payment processor accounts and other financial data, like gift cards or money orders, allow fraudsters to launder money and pay mules through alternative networks.

**Guides and templates**

Dark web markets go beyond simply offering personal and financial details for sale. Vendors also offer guides and templates to better facilitate fraudulent activity. Guides contain detailed instructional kits for fraudsters that offer step-by-step tutorials on popular fraud schemes, including phishing, account takeover, business email compromise, tax fraud and how to cash out on stolen payment cards.

These guides are effectively recipes for the fraud community that provide lists of raw materials, sets of instructions and authors’ guidance for specific tips and tricks to achieve the best possible results. Some guides offer exclusively technical information, but many also provide recommendations for the social engineering aspects of fraud, such as how to speak to customer service representatives, managers, bank tellers and other associates they might need to interact with over the course of their fraud scheme.

Guides range from general information on how to execute fraud schemes to specific, targeted recommendations on how to defraud a given financial institution, retailer or other organization. These guides represent institutional knowledge developed within the fraud community over the last several decades. They’re  another example of the maturity and development of the digital fraud economy. Schemes have become so practiced and sufficiently standardized that vendors can record their tactics and profit from the sale of that knowledge.

**Software and fraud service**

Vendors also offer software and fraud services on the dark web. Software can be legal, mass-market tools (like Adobe Photoshop, which is used to edit or manufacture fraudulent documentation) to makeshift programs or custom scripts from vendors.

Phishing schemers buy pre-made scam pages to convince users they’re visiting a legitimate website. These scam pages come loaded with the technology needed to capture account details when unsuspecting users interact with the page.

Some vendors offer fraud services as a compliment to their existing data listings. One vendor selling PII offered an additional look-up service, for a fee, if users wanted to track down the drivers’ license numbers for stolen identities they’d purchased. These value-add services expand a vendor’s potential profit.

Other vendors offer unrelated services, including one-off fraud services or physical documentation copies — most users purchasing fraudulent documentation seek out digital versions, but some vendors still process the traditional forgeries.

**Data valuation**

All goods and services traded on these criminal platforms reinforce the growth and stability of the dark web fraud economy. The fraud economy runs on compromised data, and these compromised data sets are raw materials to cybercriminals. Treating compromised information like raw materials changes the way fraudsters view and value data. Fraudsters value data based on its potential for monetization, whether because of intrinsic value (like a payment card) or its ubiquity across multiple platforms or targets (like a Social Security number), which allow fraudsters to carry out a wide range of schemes with a single data point.

Organizations typically worry about securing financial projections, research and development details, or merger and acquisition activity, but fraudsters work most effectively with the standard data types that an organization has amassed over time — employee details, customer information, executive profiles and financial accounts.

## ****The Mammoth Dark Web Fraud Trade****

Dark web e-commerce platforms or marketplaces have been developed by criminal communities to facilitate the trade of illicit goods and services. The article talks of the success of these marketplaces, their evolution, and takes a detailed look at the most popular listings across these platforms. Drugs are #1, but information to assist in fraudulent activity is #2.

**Marketplace Structures**

In 2011, the now-infamous Silk Road Marketplace launched – becoming the first market to combine privacy, ensuring dark web technology and transactions utilizing anonymous cryptocurrency. Silk Road, in its success, became the model for “all future marketplaces,” employing familiar site structures for users. Users on Silk Road would have a similar experience to those purchasing goods and services on legitimate and legal platforms like eBay or Amazon. When it comes to fulfillment, dark web vendors – particularly those involved in the trade of fraud, use auto-delivery mechanisms to ensure delivery of stolen information to buyers, 24 hours a day. There are also independent shops – many of which are dedicated entirely to the sale of stolen payment card data. These independent shops offer volume discounts for their customers and allow buyers to filter offerings based on criteria like an expiration date.