Stolen Identity Valuation and Market Evolution on the Dark Web

Chad M.S. Steel[1]
George Mason University, United States of America

Abstract

This study explores the valuation of stolen identities available for retail sale on dark web marketplaces. All listings on the five major dark web marketplaces offering full stolen identities, of "fullz", were tabulated and manually coded. The research showed that targeted marketing and value-added services are being used by criminals to differentiate their offerings, with basic identity information becoming a commodity with pricing as low as 250 identities for $1. With the proliferation of data breaches, the concept of "first sale" for identities has evolved and is changing to a "first use for purpose" model. Traditional authentication mechanisms, such as social security number and mother's maiden name, are ineffective and no longer viable for most purposes. Enhanced authentication mechanisms to combat identity theft such as requiring scans of driver's licenses or passports or asking background questions from credit reports are becoming ineffective as new identities for sale offer these enhancements.

Keywords: Identity Theft, Dark Web, Fullz, Criminal Marketplace.

Introduction

The recent increase in data breaches has led to a market surplus in stolen identities. Normally, this would result in market saturation, but because the number of potential fraud schemes using stolen identities has continued to grow, older identities still have resale value. With the stolen data traded primarily over the Internet, these progressions have been reflected in changes to the online market for stolen identities.

The online market for stolen identities has evolved over the course of three generations. First generation data breaches were relatively small, with the early Internet used primarily to facilitate the acquisition as opposed to the sale of the identities. The second generation saw the development of an Internet-based wholesale marketplace and, with the advent of larger breaches, specialization appearing within the fraud cells. The third and current generation is showing further market maturity, with the differentiation of wholesale and retail markets. The dark web and cryptocurrencies have led to direct-to-

[1]Adjunct Professor, Digital Forensics and Cyber Analysis Program, Volgenau School of Engineering, George Mason University, Room No: 3300, Nguyen Engineering Building, Fairfax, VA 22030, USA. Email: csteel@gmu.edu

consumer sales of identities, which has had a significant impact on the marketing and pricing of stolen identities.

The purpose of the current study is to rigorously and comprehensively investigate the pricing of stolen identities on the dark web, identify value added services that impact pricing at the marketplace and the individual listing level, and evaluate the marketing utilized to sell stolen identities.

The generations identified are not discrete - there is overlap between them and there are features of the later generations present in small numbers during earlier periods, but they serve to provide a roadmap for the various evolution of behaviors exhibited by offenders. This is not the first paper to review identity theft - Anderson et al. chronicled the early rise of identity crimes (Anderson, Durbin, & Salinger, 2008), and Berghel (2000) differentiated the value of different components of identities. It is the first, however, to comprehensively look at the value of a stolen identity across all of the dark web markets, including a quantification of the components that make up that value.

First generation - Internet-facilitated theft and small scale breaches

In May 1998, the General Accounting Office (GAO) predicted an increase in identity theft cases with the then-recent explosive growth of the Internet (U.S. Government Accounting Office, 1998). At the time of their 1998 report, the GAO was unable to provide any reliable statistics on the number of victims of identity theft, but a follow-up report in 2002 used consumer credit reporting fraud alerts as a proxy, identifying 89,000, 29,593, and 92,000 cases from the three credit bureaus in the most recent twelve month period of data available (U.S. General Accounting Office, 2002).

The first generation of online identity theft cases were primarily perpetrated by individuals. While some fraud rings were present, they tended to be small and opportunistically formed. Exemplary of the first generation identity theft rings was the arrest of three individuals in Los Angeles for stealing the identities of 120 members of the Army Corps of Engineers, with the thieves using the identities to purchase approximately $700,000 in stolen goods. At the time, the group was identified as the then-second largest identity theft ring in the United States by valuation (Meyer & Martin, 2000; Stearns, 2001).

The first generation of Internet-enabled identity theft sales consisted of only a primary market with few inter-organizational transactions and mostly non-specialized players. The individuals stealing the identities were generally the same individuals that monetized the thefts. There were examples of intragroup specialization, but specialization did not appear to occur on a large scale between groups (Stearns, 2001).

Arguably the largest and most sophisticated of the first generation identity theft rings was the Campbell Organization, a group of fewer than twenty individuals responsible for $3 million in losses and the theft of approximately 150 identities in the Florida area (Stearns, 2001). The organization showed evidence of early intragroup specialization:

- The first group of individuals focused on stealing identities through "burglary, robbery, auto theft, postal theft" and the use of insiders at banks and credit card companies, in addition to general document theft.
- The second group collected the information and sold it, along with identity documents, to the third group.

- The third group monetized the information by opening bank accounts, obtaining loans, purchasing goods, and even buying real estate using the stolen identities (Stearns, 2001).

The first generation saw an increase in regulation and enforcement in response to the burgeoning criminal marketplace, strengthening the penalties associated with online identity theft. In 1998, the Identity Theft and Assumption Deterrence Act was signed into law in the United States, which criminalized the act of identity theft at a federal level and resulted in sentences of up to 15 years in prison and compensation rights for victims (The Identity Theft and Assumption Deterrence Act: Report together with additional views (to accompany S. 512), 1998).

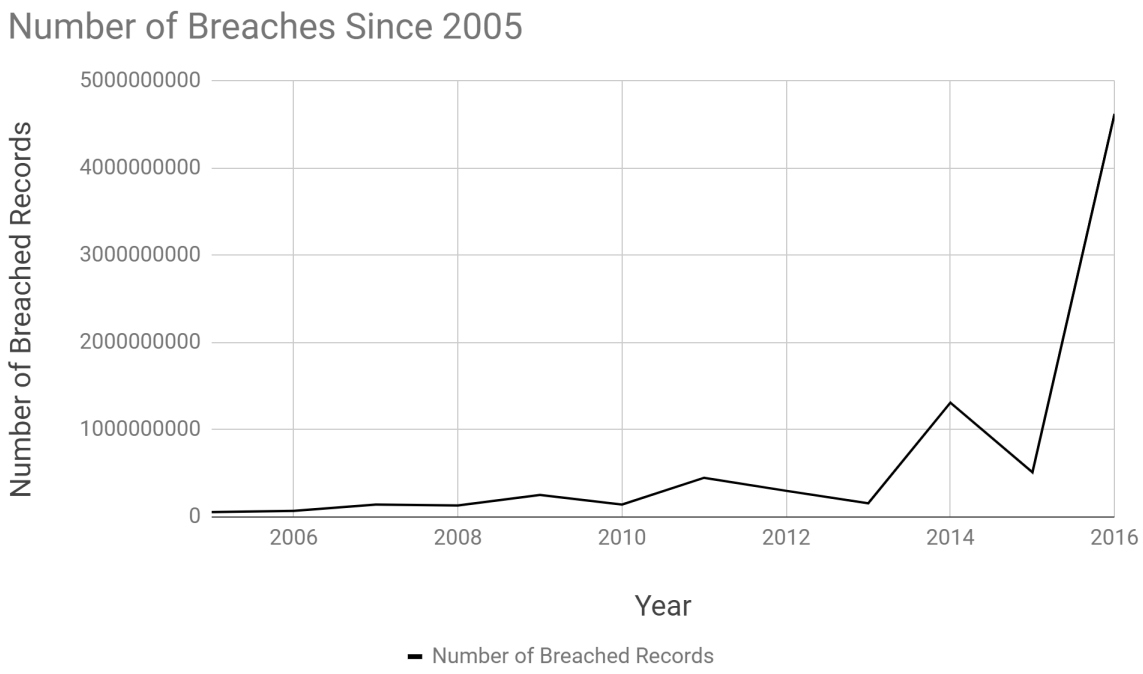
Because there was minimal resale of identities during the first generation, it is difficult to place a value on their possession. A cash-out value based on the total loss associated with a fraud could be obtained, but that is not necessarily reflective of the price a third party would pay for the identity itself. Despite not having a price associated with an identity, there was a definite focus on obtaining social security numbers specifically, which Berghel noted as the "Holy grail of identity thieves", and prophetically noted "Identity theft will be the undoing of the blissful ignorance we have maintained with respect to the misuse of SSNs" (Berghel, 2000).

Second generation - Internet auctions and large-scale breaches

The second generation of online identity theft was marked by large scale data breaches, increased specialization and segregation between the individuals obtaining the identities and those cashing in on them, and the creation of a free market economy for identities via Internet auctions. There was a continued focus on social security numbers, with a premium price put on "first sale" or newly stolen identities (Newman & Mcnally, 2005).

In 2000, the largest confirmed breach of social security numbers to-date was by a hacker at the University of Washington Medical Center, who stole 5,000 records (Tehan, 2008). In 2017, an Equifax breach resulted in the theft of the social security numbers (and substantially more sensitive personally identifiable information) on 143 million individuals in the United States ("Nearly half of US citizens hit by massive Equifax breach," 2017). Since 2005, the first year for which the Privacy Rights Clearinghouse began tracking reliable statistics, the number of records breached has grown exponentially as shown in Figure 1 ("Privacy rights clearinghouse - Data breaches by year," 2017). As the number of records being breached increased, the ability for a single individual or group of individuals to cash out became increasingly difficult, resulting in a differentiation between the individuals stealing the identities and the individuals operationalizing fraud schemes based on the stolen identities. This culminated in the formation of Internet auctions specifically targeted at identity theft information, colloquially referred to as "fullz".

Figure 1. Records breached by year
("Privacy rights clearinghouse - Data breaches by year," 2017)



In 2003, the concept of purchasing lists of social security numbers in an Internet auction began to gain prevalence (Huse, 2003). Identity theft rings became substantially more sophisticated as well. As an example, Shadowcrew, a criminal organization with approximately 4,000 members that operated between 2002 and 2004 stealing credit card and identity information, had a sophisticated, hierarchical organization (Hilley, 2006). The organization was described by Peretti as having a segregated and differentiated functional composition as follows:

- a small group of "administrators" who served as a governing council of the criminal organization;
- "moderators" who oversaw and administered one or more subject-matter-specific forums on the website that was either within an area of their expertise or dealt with their geographic location;
- "reviewers" who examined and/or tested products and services that members of the criminal organizations desired to advertise and sell;
- "vendors" who advertised and sold products and services to members of the criminal organizations via the website after the product or service had obtained a position written review from a reviewer; and
- "general members" who used the web sites to gather and provide information about perpetrating criminal activity and facilitate their purchases of credit card numbers, false identification documents and other contraband (Peretti, 2008).

Shadowcrew and other identity theft enterprises began providing sophisticated e-commerce platforms in a wholesale model to sell bulk dumps from breaches by both members and non-members. These locations included a platform for the sale of stolen identities, forums to discuss identity theft techniques, how-to guides on committing identity fraud and taking precautionary measures, and the purchase of supplemental documentation (e.g. fake drivers' licenses) to facilitate cashing out on stolen identities (Peretti, 2008).

The initial auctions were one-stage economic transactions, which eventually differentiated into wholesale and retail marketplaces. Auctions continued to be popular on the wholesale side, while smaller groupings of identities became available for sale on dedicated forums for smaller criminal enterprises and individuals to purchase. During this period, a secondary market for "used" or "dead" identities also began, allowing previously stolen information to be repurposed for other criminal activity.

Thirdgeneration - specialization, targeting, and value-added services

The third generation can be characterized by what Camp et al. (Camp, Johnson, & Schwartz, 2012) described as ubiquitous identity theft. The Identity Theft Resource Center ("Identity theft resource center," 2018) reported 1.077 billion identity records have been stolen as of 2018 in data breaches. The stealing of identities has become pervasive to the point that, as a mean based on the above figures, each adult in the United States has had their identity stolen approximately 4.4 times.

Due to the ubiquity of identity theft, the economics have shifted for identity sales, creating a tiered marketplace and an opportunity for value-added services. At the same time, two primary technological changes, Tor ("The Onion Router") and digital currencies, have altered the risk/benefit ratio of identity fraud. The interaction of these two competing forces changed the economics of identity theft in unforeseen ways.

The primary technology behind most current identity theft marketplaces is Tor (Jardine, 2015). Tor allows users to connect in a largely anonymous fashion to sites that are hosted at anonymous locations (Dingledine, Mathewson, & Syverson, 2004), collectively known as the dark web, which has facilitated the growth of numerous online illicit activities. With a reduced risk of discovery, criminal marketplaces have become overt and more sophisticated, selling everything from identities to hacking exploits to child exploitation material directly to end consumers. The sites that sell stolen identities have begun to resemble full e-commerce marketplaces, complete with shopping carts, reviewer feedback, and customization of purchases. Likewise, with the increased anonymity afforded by Tor, they have become more widely accessible and consumer-friendly (Christin, 2013).

The second barrier that was overcome in the third generation is one of payment transactions. The rise of Bitcoin and similar blockchain-based currencies allows for the digital equivalent of the anonymity offered through cash transactions (Chen, 2011; Hurlburt & Bojanova, 2014). Coupled with the dark web, these currencies reduced the risks for both buyers and sellers, increasing the number of individuals participating in the overall underground economy present in these markets. With the reduced risk, individuals who would otherwise have been disinclined to commit identity theft now have greater incentive to do so (Kethineni, Cao, & Dodge, 2017).

The introduction of the dark web and Tor changed the marketplace from a primarily one-tier to a primarily two-tier model. Originally, online identities were sold in bulk on private channels through Internet Relay Chat (IRC) or through private forums. Identity thieves would advertise recent thefts and sell lots of 10,000 or more identities negotiated through private interactions (Holt, Smirnova, Chua, & Copes, 2015; Wehinger, 2011). The wholesale market remains a mostly private channel enterprise, but a retail market arose that allowed for direct-to-consumer sales of smaller lots of identities, with lots as small as one (Ablon, Libicki, & Golay, 2014; Holt et al., 2015). These markets began competing, driving down pricing and offering value added services to differentiate themselves.

The primary value-added services in the third generation were related to risk reduction for buyers and sellers, principally rating/review and escrow services. The Silk Road marketplace was the largest initial service to offer both. Their reviewing services allowed consumers to rate vendors and provide direct feedback on purchases, similar to Amazon seller ratings, which provided greater assurances to other consumers (Lacson & Jones, 2016). Additionally, the inclusion of an escrow service allowed the marketplace to safely monetize based on transaction volumes and amounts while providing both buyers and sellers greater guarantees of payment and delivery (Lacey & Salmon, 2015).

Further opening up the marketplace, many of the online vendors began offering end user-focused tutorials (as opposed to the insider tutorials in the second generation), including step-by-step guides to cashing in on stolen identities. These ranged from PDFs containing instructions on using stolen identities safely to Youtube video tutorials detailing how to commit specific frauds (Hutchings & Holt, 2016). This had the net effect of increasing the number of individuals exploiting identities at a low level and not as part of an organized group by disintermediating and empowering "mules" and allowing them to act independently of a hierarchy (Ablon, 2018).

Additional value-added services were identified in the current generation, as noted below, which allowed for greater differentiation in an increasingly commoditized marketplace. These differentiators provided pricing power to sellers and convenience services to buyers, with the marketplaces themselves receiving increased revenue as a result.

Historical pricing

While there have been no comprehensive reviews of identity costs and associated services in the prior art, there have been commercial reviews that have documented historical trends. A review of the literature identified ten prior reviews of historical prices for an identity is noted in Table 1.

Current study

The current study seeks to evaluate, both quantitatively and qualitatively, the pricing and the factors influencing pricing for stolen identities online. Because there has been no prior comprehensive review of the dark web identity markets, this research will serve as a baseline for future trend analysis. Based on the current state of identity theft markets, it is hypothesized that:

- H1: The current increase in supply of identities from breaches has driven prices downward.

- H2: Because of a lack of consumer market maturity and stability, price fluctuations will be large.
- H3: Pricing will be strongly dependent on value-added features.

Table 1. Historical pricing for full identities

Year	*Study*	*Low*	*High*
2007	(Symantec, 2008)	$10	$150
2008	(Symantec, 2009)	$0.70	$60
2009	(Symantec, 2010)	$0.70	$20
2013	(SecureWorks, 2016)	$0.25	$25
2014	(SecureWorks, 2016)	$30	$30
2015	(Collins, 2015)	<$1.00	$454.05
2016	(SecureWorks, 2016)	$15	$65
2016	(Symantec, 2017)	$0.10	$1.50

Methodology

The current study reviewed the major dark web marketplaces selling stolen identities in November and December 2017. All of the major marketplaces that were extant and available and advertised stolen identities were analyzed. Each of the marketplaces was reviewed for marketplace-wide value-added features as well as policies related to transactions. Five marketplaces were identified as meeting the above criteria and all listings on each of the marketplaces were reviewed for the sale of stolen identities. The marketplaces identified were as follows:

- Berlusconi
- Dream Market
- RSClub
- T*chka
- Wall Street

Because of inconsistent availability on the sites, the collection and review of listings spanned two months. The listings collected were limited to those selling identity information on individuals within the United States to ensure that comparisons were not influenced by differing values of an identity in other countries. Only listings that offered a stolen identity with non-public information that could be used to obtain something of value while impersonating another individual were included. Listings that were comprised of screen scrapes of names/phones/addresses/email addresses which were sold for mass marketing or phishing/spam purposes were not included. Finally, any listings that included a stolen credit card with the identity were excluded to avoid the confound of the value of the card as opposed to the identity itself.

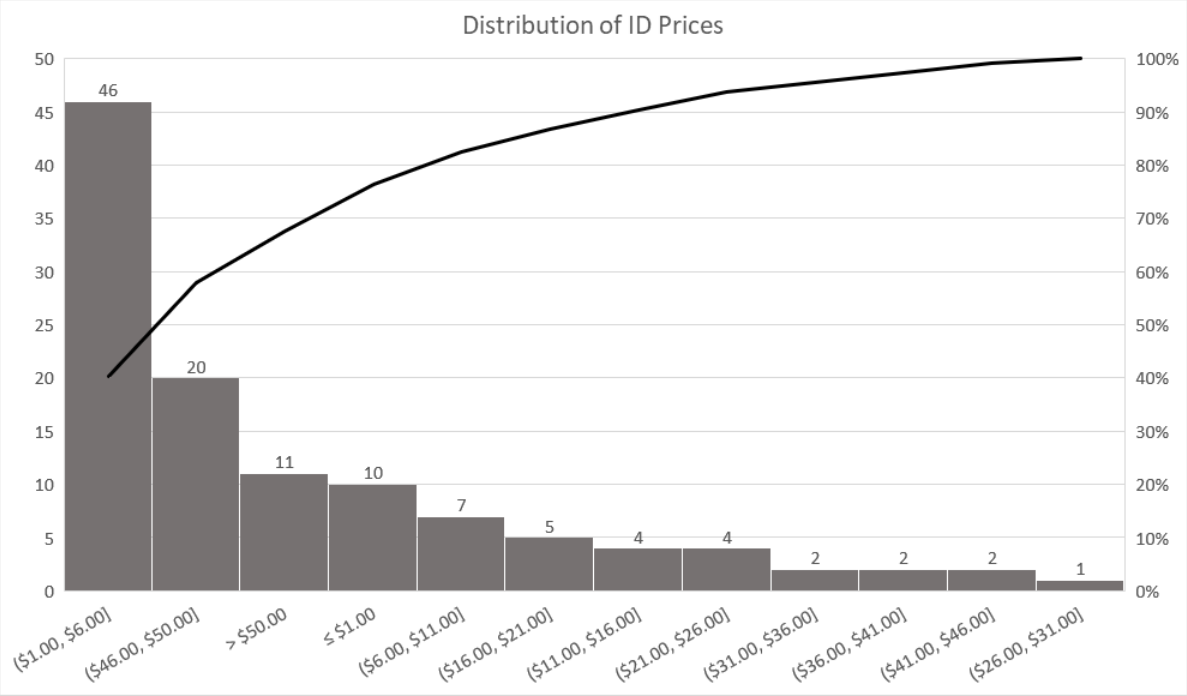
For each listing collected (n=115), which represented the total number of listings available across the marketplaces at the time of the study, the details of the offerings were manually coded based on the types of personally identifiable information offered, the quantity of identities offered, and the cost per identity. Any value-added services or targeted offerings that were made as part of the listing were also noted.

The price range for identities were tabulated and the features associated with each price identified. For each of the value-added features, a conjoint analysis was performed against the price of the offerings to determine what, if any, pricing power those features had.

Results

A total of n=115 sellers providing "fullz" were identified. The majority of the sales were for single identities (n=87, 76%), with an unspecified maximum number of identities available. The prices ranged from $.004009 (n=1) to over $200 per identity, with a mean cost of $23.94. The price distribution is shown in Figure 2.

Figure 2. Price distribution of identities



The minimum prices varied by marketplace, with high deviations both within and between marketplaces. The mean price correlated inversely with the size of the market (r=-.551), with larger markets having lower mean pricing. The overall results are shown in Table 2.

Table 2. Listings by marketplace

Marketplace	*n*	*Min Price*	*Max Price*	*Mean Price*	*Standard Deviation*
Berlusconi	23	0.004	489.350	62.759	137.079
Dream Market	57	0.010	200.000	18.155	31.871
RSClub	10	2.500	70.000	28.900	24.507
T⋆chka	1	50	50	50	50
Wall Street	24	0.580	100.000	35.626	25.511

The majority of identities for sale included a social security number (n=112, 98%) and a date of birth (n=109, 96%). Many of the listings advertised biographical information, with past address information (n=73, 64%) available more frequently than current address information (n=35, 31%), likely due to the age of the identity information. A few sellers offered scans of a passport (n=2, 2%) and driver's license (n=8, 7%) associated with the identities, however the validity of the pictures provided could not be verified. The distribution of products offering each element are shown in Table 3.

Table 3. Elements included in sale

Element	*Fullz Advertising That Element*
Name	1.00
SSN	0.98
DOB	0.96
Past Address	0.64
Employer	0.45
Income	0.43
Phone	0.40
Education	0.37
MMN	0.37
Current Address	0.31
Bank Account Number	0.22
Email	0.17
Passport Photo	0.08
DL Number	0.07
Credit Score	0.03
DL Photo	0.02

There was no observed difference in the reviews of the sellers offering higher priced identities versus those offering lower priced identities. To determine the if there was a pricing bias based on the presence of a particular element, a conjoint analysis was performed on the dataset. Of particular note, most sellers advertised the availability of mother's maiden name (MMN) in their product titles, indicating a belief by sellers in the value of that element. When analyzed, however, mother's maiden named showed no

predictive power on pricing. The only two elements that showed a high predictive power with a statistically significant p-value ($p<.01$) were the presence of a bank account number (coefficient=34.4, p=.0009) and a credit score (coefficient=30.6, p=.0006).

Value-added services

Value-added services were identified at both the marketplace and seller level. Marketplace value-added services provided features that benefited both the seller and the buyer, while seller value-added services were advertised to allow the consumer to differentiation between similar sellers.

For the storefronts, all five marketplaces offered blockchain based currency options and escrow services. The fees for escrow ranged from 3.5% for Wall Street transactions to 6.5% for Berlusconi transactions. All of the providers accepted Bitcoins, with Wall Street also accepting Monero. All of the providers listed their transactions in the local currency (US Dollars) or in Bitcoins.

Several marketplaces offered two additional value-added escrow enhancements, Finalize Early (FE) and MultiSig. FE is a service that is of primary benefit to the seller in that escrowed funds are released early without full contract completion. FE was introduced to protect sellers as well as to allow the marketplace to collect revenue on a stable basis. FE is used to reduce seller risk from Bitcoin price fluctuations and was provided in response to dramatic shifts in Bitcoin valuations.

Multiple Signature, or Multisig, relies on public key cryptographic algorithms and requires that multiple parties agree before funds transfers can be finalized. Multisig enables FE (the seller and escrow agent can agree to finalize the transaction) and can be used independently of it (all three signatures can be required for the transfer of Bitcoins). T★chka and RSClub offered both FE and Multisig, while Wall Street only supported MultiSig and Dream Market only supported FE.

As a risk reduction service, T★chka, RSClub, and Wall Street offered Pretty Good Privacy (PGP) encryption of all transaction records. While there was no direct way to verify compliance, encrypting the transactions provides both the buyer and the seller an additional degree of security in the event that the marketplace records are seized by law enforcement. While the other services did not advertise encryption, they may be doing so on the backend to obfuscate their own activities in the event of a seizure.

A number of sellers (n=13, 11%) advertised the ability to target individual states, and particular zip codes within a state, specifically highlighting the ability to obtain Florida identities to obtain benefits following hurricanes Harvey and Irma. As a more general value-added service, approximately one third of sellers (n=42, 37%) offered buyers the ability to select specific credit score ranges for their purchases.

Discussion

As the third generation of online identity theft evolves, there have been fundamental shifts in the economics of stolen identities that are only now being reflected in the pricing. The large disparity in prices despite few differentiators is indicative of an immature market (and may be partially based on rapid, large Bitcoin valuation changes), but there is a steady downward trend for the minimum price on a stolen identity. The lowest price available at retail at the time of the study, $.004, reflects an all-time low. Because most adults in the United States have had their identities stolen and sold multiple times based on large scale breaches, the value of "zero day" or "first sale" identities has become negligible. The focus

on timely benefits fraud exhibited by the targeted sale of Florida identities shows that thieves are now seeking to be the first to exploit an identity for a particular fraud. While any specific identity has likely been previously sold, it may not have been used for the fraud intended by the purchaser. As such, there is a value for timely exploitation on new frauds (e.g. disaster benefits fraud), while longer term frauds (e.g. fraudulent IRS filings) are likely to diminish as fewer unexploited identities are on the market and there is no current way of knowing a priori which have been previously exploited in a particular scheme.

What remains to be seen on the supply side is the impact of a now-nominal value for a stolen identity and the ubiquity of credit monitoring and credit freeze services that individuals have signed up for as a result of prior breaches. The lowered retail cost of an identity should devalue and therefore reduce the number (and impact) of general breaches, but it may also result in more targeted breaches directed at more valuable and exploitable identity information.

Based on the qualitative information obtained in the study, there are several findings that directly impact the design of authentication mechanisms to prevent targeted identity theft. Additionally, the findings have implications for the future of the market pricing and makeup.

Basic authentication mechanisms need to evolve. The use of social security number, date of birth, and mother's maiden name as a means of identity verification are no longer feasible. These identifiers should be considered compromised for all individuals in the United States and provide minimal incremental value in establishing identity.

Enhanced authentication mechanisms need to increase the attacker cost. The requirement that individuals provide a digital copy of common photo-based identification represents a negligible additional cost to the attacker in terms of cash outlay and time required. The additional cost of uncommon knowledge-based credit and background-based challenges is higher. An unintended consequence of legislation designed to protect consumers, the Fair Credit Reporting Act, is that it allows attackers that have obtained identity information to obtain zero cost credit reports by impersonating the subject and the decentralization of the credit bureaus provides additional opportunities for compromise. While the Equifax breach received substantial news coverage, its data represented a negligible decrease in attacker cost. Background check information, including relatives, employment history, education, past addresses and similar details are available through open source collection (which requires substantial time investment) or through cash outlay (individual reports cost as little as $7.95 from online brokers like Intelius and are readily available to the attacker). These are all considered static authenticators – the historical details do not change over time and once compromised remain compromised. The use of these same background identifiers also invalidates many security challenge questions. In particular, a few of the entries advertised the availability of security challenge questions and answers for their victims as part of their package. Exemplary of these was a listing offering answers to the following additional information for a small premium per identity:

> Security Question 1 : In what city did you attend high school?
> Security Question 2 : What is your father\'s middle name?
> Security Question 3 : What is your mother\'s middle name?
> Security Question 4 : In what year (YYYY) did you graduate from high school?

Security Question 5 : In what city was your father born?
Security Question 6 : In what city did you attend high school?

Attackers are adopting price discrimination and targeted marketing tactics. Identities are no longer purchased as massive lists of unrelated entries. They can be bought as targeted market lists, with everything from credit score to age to zip code tailored to a particular identity fraud. Atherton, California had the highest value homes of any United States zip code in 2017, with a median home value of $9,686,154 (Sharf, 2017). Identities from this location may generate a premium for fraudsters targeting the opening of lines of credit, however they may not be effective in a fraud scheme targeting Housing and Urban Development (HUD) section 8 benefits fraud. Likewise, identities of older individuals may be more viable for social security fraud, and areas of recent hurricanes targeted for disaster aid fraud. As seen in the study, Florida identities were advertised as a premium feature to support benefits fraud as a result of recent natural disasters. This shows that the consumer is aware of the need for tailored identities, and that the market has already responded. If this trend continues through the fraud chain, we may begin to see targeted breaches-on-demand in response to a market need for specific identity information.

The concept of "dead" identities is no longer valid. Because identity theft is so widespread, it is generally assumed that any identities used are secondary or tertiary sales (and uses) of the same information. The market has already responded by offering new information on the same identities that can expand the fraudulent utility of that identity. There is also no such thing as a "dead" identity any longer. A particular identity is only usable or not usable for a particular scheme. The value of an identity may fluctuate higher as new schemes are conceived of that take advantage of identities already on the market and lower as a result of flooding from new breaches.

Conclusion

The increase in data breaches has driven the price of a stolen identity to an all-time low. The market for stolen identities has shifted from small groups of individuals stealing limited numbers of identities and exploiting them directly to large scale data breaches with both wholesale and retail markets. As we transition to a world where everyone's basic identity information has been compromised at one point or another, the concept of a first sale for fresh identities has been relegated to the past, while new value-added services continue to be included to increase the sale price of identities and to stay ahead of the changes in authentication enhancements made as a result of past breaches.

Limitations

This study was the first comprehensive look at the identities available on the dark web from a cost perspective. There are limitations inherent in the study, due primarily to the nature of the dark web marketplaces. First, the marketplaces and the individual vendors on those marketplaces are relatively transient. If a marketplace grows to large, it becomes a target for law enforcement efforts to take it down, making things like vendor reputations time-limited. Second, the quality of the identities and whether or not they actually matched the advertised content could not be determined without violating the law. Third, the study focused on consumer-oriented identities. The wholesale market of bulk identities sold in private forums was not examined but represents an integral part of the stolen identity economy.

References

Ablon, L. (2018). *Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data*. Rand Corporation.

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Rand Corporation.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity Theft. *The Journal of Economic Perspectives: A Journal of the American Economic Association*, *22*(2), 171–192.

Berghel, H. (2000). Identity theft, social security numbers, and the Web. *Communications of the ACM*, *43*(2), 17–21.

Camp, L. J., Johnson, M., & Schwartz, A. (2012). Scenario IV: Ubiquitous identity theft. In *The economics of financial and medical identity theft* (pp. 147–153).

Chen, H. (2011). Dark web: Exploring and mining the dark side of the web. *2011 European Intelligence and Security Informatics Conference*. doi: 10.1109/eisic.2011.78

Christin, N. (2013). Traveling the silk road: A measurement of a large anonymous online marketplace. *Proceedings of the 22nd International Conference on World Wide Web*. Presented at the 22nd international conference on World Wide Web. https://doi.org/10.21236/ada579383

Collins, K. (2015, July 23). Here's what your stolen identity goes for on the internet's black market. Retrieved from https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. *Proceedings of the 13th Conference on USENIX Security*. Presented at the 13th conference on USENIX Security . https://doi.org/10.21236/ada465464

Hilley, S. (2006). Case analysis of the Shadowcrew carding gang. *Computer Fraud & Security*, *2006*(2), 5.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103.

Hurlburt, G. F., & Bojanova, I. (2014). Bitcoin: Benefit or curse? *IT Professional*, *16*(3), 10–15.

Huse, J. G., Jr. (2003, July). *Prepared Statement*. Presented at the Hearing Before the Subcommittee on Social Security of the Committee on Ways and Means U.S. House of Representatives.

Hutchings, A., & Holt, T. J. (2016). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11–30.

Identity theft resource center. (2018). Retrieved April 24, 2018, from Identity Theft Resource Center website: https://www.idtheftcenter.org

Jardine, E. (2015). The dark web dilemma: Tor, anonymity and online policing. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2667711

Kethineni, S., Cao, Y., & Dodge, C. (2017). Use of Bitcoin in darknet markets: Examining facilitative factors on Bitcoin-related crimes. *American Journal of Criminal Justice: AJCJ*. https://doi.org/10.1007/s12103-017-9394-6

Lacey, D., & Salmon, P. M. (2015). It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums. In *Lecture Notes in Computer Science* (pp. 117–128).

Lacson, W., & Jones, B. (2016). The 21st century darknet market: Lessons from the fall of silk road. *International Journal of Cyber Criminology*, *10*(1).

Meyer, J., & Martin, H. (2000, August 31). 2 Held in raid on identity theft ring. *Los Angeles Times*.

Nearly half of US citizens hit by massive Equifax breach. (2017). *Computer Fraud & Security*, *2017*(9), 1–3.

Newman, G., & Mcnally, M. (2005). *Identity theft literature review*. United States Department of Justice.

Peretti, K. (2008). Data breaches: What the underground world of carding reveals. *Santa Clara Computer & High Technology Law Journal*, *25*(2).

Privacy rights clearinghouse - Data breaches by year. (2017). Retrieved December 30, 2017, from https://www.privacyrights.org/data-breaches

SecureWorks. (2016). *Underground hacker markets*. SecureWorks.

Sharf, S. (2017, November 28). Full list: America's most expensive ZIP codes 2017. *Forbes*.

Stearns, C. (2001). *Protecting privacy and preventing the misuse of social security numbers*. Presented at the Hearing before the Subcommittee on Social Security of the Committee on Ways and Means, House of Representatives, One Hundred Seventh Congress, First Session, May 22, 2001. Retrieved from https://books.google.com/books/about/Protecting_Privacy_and_Preventing_the_Mi.html?hl=&id=XM84nQAACAAJ

Symantec. (2008). *2007 Internet Security Threat Report (ISTR)*. Symantec.

Symantec. (2009). *2008 Internet Security Threat Report (ISTR)*. Symantec.

Symantec. (2010). *2009 Internet Security Threat Report (ISTR)*. Symantec.

Symantec. (2017). *2017 Internet Security Threat Report (ISTR)*. Symantec.

Tehan, R. (2008). *Data security breaches: Context and incident summaries* (No. RL33199). Congressional Research Service.

The Identity Theft and Assumption Deterrence Act: Report together with additional views (to accompany S. 512). , (1998).

U.S. General Accounting Office. (2002). *Identity theft: Prevalence and cost appear to be growing* (No. GAO-02-363).

U.S. Government Accounting Office. (1998). *Identity fraud: Information on prevalence, cost, and Internet impact is limited* (No. GAO/GGD-98-100BR).

Wehinger, F. (2011). The dark net: Self-regulation dynamics of illegal online markets for identities and related services. *2011 European Intelligence and Security Informatics Conference*. https://doi.org/10.1109/eisic.2011.54