

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

I.C., a minor, by and through his natural parent, NASIM CHAUDHRI, on behalf of himself and all others similarly situated,

Plaintiff,

v.

STOCKX, INC.; and STOCKX, LLC,

Defendants.

Case No. _____

Hon. _____

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

I.C., a minor by and through his natural parent, Nasim Chaudhri, individually and on behalf of a Class defined below of similarly situated minor persons, alleges the following against Defendants StockX, Inc., and StockX, LLC (collectively “StockX”) based upon personal knowledge and on information and belief derived from, among other things, StockX’s August 8, 2019 “Notice of Data Breach,” investigation of counsel, and review of public documents as to all other matters.

NATURE OF COMPLAINT

1. Plaintiff brings this action against StockX for StockX’s failure to reasonably safeguard Plaintiff’s PII as defined herein, failure to reasonably provide timely notification that Plaintiff’s PII had been accessed and acquired by an

unauthorized third party, and for intentionally and unconscionably deceiving Plaintiff relating to the status, safety, location, access, and protection of Plaintiff's PII.

2. As a result of StockX's negligent, intentional, or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's PII was accessed, acquired, stolen, and re-sold by thieves for the express purpose of misusing Plaintiff's data and causing further irreparable harm to Plaintiff's personal, financial, reputational, and future well-being.

3. Plaintiff brings this lawsuit against StockX for statutory violations as well as common law tort claims under negligence, negligent misrepresentation, fraud and fraud through silence, negligence per se, unjust enrichment, violation of state data breach statutes, intrusion upon seclusion, and declaratory judgment.

4. As used throughout this Complaint, "Personally Identifiable Information" or "PII" is defined as all information exposed by the StockX data breach, includes all information so defined under individual states' statutes, and includes all or any part or combination of name, address, birth date, Social Security number, driver's license information (any part of license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, usernames, passwords, and log-in information that can be used to access a person's personal electronic content.

PARTIES

5. StockX, Inc. is a Delaware corporation with its principal place of business in Detroit, Michigan.

6. StockX, LLC, is a Michigan limited liability company with its principal place of business in Detroit, Michigan.

7. Plaintiff is an individual citizen of Kansas, who had a StockX account at the time of the incidents described herein and entrusted PII (as defined herein) to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

JURISDICTION AND VENUE

8. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, the number of class members exceeds 100, and StockX is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

9. This Court has personal jurisdiction over StockX because it is authorized to and regularly conducts business in Michigan and is headquartered in Detroit, Michigan.

10. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because StockX entered into terms of service and privacy agreements with Plaintiff in Kansas and Michigan, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in Kansas and Michigan.

GENERAL ALLEGATIONS

I. StockX – Background.

11. StockX is an ecommerce platform for luxury goods, fashion clothing, and accessories, with a particular emphasis on ultrarare, custom, vintage, and highly sought shoes for “sneakerheads,” including minors.

12. Under StockX's business model, products posted on its platform are treated similarly to the way in which stocks are traded on the market — i.e., each product is assigned a ticker symbol, sellers put out asking prices, and the products are then bid on by prospective purchasers. Users of StockX then see data such as price volatility, highs, and lows from across the internet, and once a bid matches with an

asking price, the sale occurs automatically.¹ StockX then takes a flat commission on each sale ranging from 8–9.5 percent.²

13. For example, in January of 2018, StockX sold limited-edition LeBron James shoes for an average of \$6,000 per pair—with approximately \$500 of each going directly to StockX. The shoes would then be “flipped” on the same StockX marketplace, with StockX, again, realizing its commission, without the purchaser ever taking actual physical possession of the shoes.³

14. Some sneakers on StockX have been sold for as high as \$30,000, and at one time, the site had sneakers with an asking price of \$850,000.⁴

15. StockX has grown rapidly since its inception in February 2016. As of mid-2018, StockX was conducting more than 10,000 transactions per day, had 370 employees, and more than \$700 million in sales.

¹ <https://www.nytimes.com/2018/07/06/business/smallbusiness/stockx-sneakerheads-luxury-goods.html?smid=nytcore-ios-share&module=inline> (Last visited, August 2019) (Exhibit 1).

² *Id.*

³ *Id.*

⁴ <https://www.sportswear-international.com/news/portrait/Marketplace-How-StockX-is-revolutionizing-the-sneaker-reseller-business-online-14099> (Last visited, August 2019) (Exhibit 2).

16. More recently, StockX reported sales of \$100 million per month, and in June 2019, StockX raised \$110 million in financing (on top of a previous \$60 million), valuing it at more than \$1 billion and in excess of 800 employees.⁵

II. StockX collects personally identifiable information from its users.

17. StockX requires all individuals who wish to use its platform to create a StockX user account, which requires the prospective user to submit certain information to StockX. The prospective user can create an account with StockX through the user's email address.

18. The information that StockX requires for prospective users to become active users initially includes the user's first name, last name, email address, a username, and a password. The user can then select one or more of four "vices": Sneakers, Streetwear, Bags & Accessories, or Watches. If "Sneakers" is one of the "vices" selected, StockX's sign-up form automatically prompts the prospective user to "Select U.S. Men's Size" by choosing from a drop-down box.

19. At the bottom of the Sign Up form, StockX includes a single-line checkbox advising prospective users that by signing up for their service they must agree to StockX's terms of service. The individual is also provided a link to StockX's

⁵ <https://www.freep.com/story/money/business/2019/06/26/stockx-valuation-ceo-scott-cutler/1569408001/> (Last visited, August 2019) (Exhibit 3).

Privacy Policy. If the user chooses, he or she can open the Privacy Policy or Terms of Service by clicking on green hyperlinks, which launch separate windows displaying those forms, comprised of many pages of fine print.

Sign Up

Login

Let's get started and create your account

f Sign Up With Facebook

t Sign Up with Twitter

Or with Email

First Name

Last Name

Username

Email Address

Password

You must use 8 or more characters with a mix of letters, numbers & symbols.

Choose your vice(s):

Sneakers

Streetwear

Bags & Accessories

Watches

Select U.S. Men's Size:

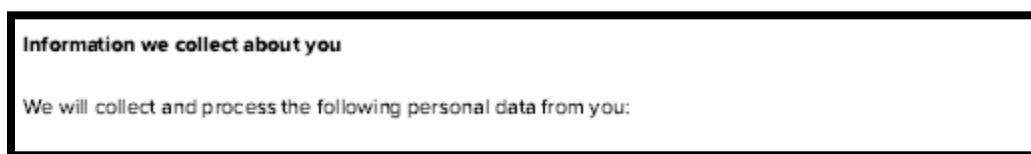
Please Select Size

☐ By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#).

20. Plaintiff, like all other members of the Class, created a user account on StockX's platform, and provided his first name, last name, username, email address, password, shoe size, and other information to StockX.

21. StockX's Privacy Policy is entitled "Your Privacy Rights." The current version of StockX's Privacy Policy as of the time of filing was last updated on October 9, 2018.

22. StockX fails to advise its users what information it does and will collect from them, even though it requires all prospective users to provide sensitive information at the very outset of their membership on the StockX platform. The first item listed in StockX's Privacy Policy purports to be information regarding "personal data" that StockX collects from its users; however, that section of the Privacy Policy is blank as shown in the below screen shot:



As a result, even if the prospective user reviewed StockX's Privacy Policy, the user would not have been fully informed regarding StockX's actual privacy policy and practices with respect to the "personal data" collected by StockX when the user created an account.

23. Nevertheless, in its Privacy Policy, StockX assures its users that it protects their information on “secure servers” and claims that “[o]nce we have received your information, we will use strict procedures and security features to try to prevent unauthorised [sic] access.”

III. StockX targets minors as part of its business model.

24. One of StockX’s principal targeted demographics includes pre-teen and early-teen minors.

25. It is well-known that a large segment of StockX’s user base is comprised of teenagers who have not yet reached the age of majority, and StockX has profited handsomely from their use of its services.⁶

26. The teenage demographic is a particularly active segment of StockX’s user population — as teenagers are disproportionately likely to be among those highly passionate about amassing and collecting custom-made, ultrarare, vintage, and fashionable sneakers — and one of the main reasons for StockX’s meteoric success.⁷

⁶ <https://www.businessinsider.com/teen-makes-money-selling-sneakers-stockx-2019-8> (“15-year-old Jake, whose last name has been omitted in order to protect his privacy, sells merchandise on the online sneaker resale marketplace StockX. Now a high school sophomore, he started reselling via Instagram when he was in eighth grade. Less than three years later, he says he's made over six figures.”) (Last visited, August 2019) (Exhibit 4).

⁷ <https://finance.yahoo.com/news/american-teens-are-increasingly-becoming-sneakerheads-145501328.html> (“American teenagers are embracing sneaker culture in significant numbers, according to Piper Jaffray’s spring 2019 ‘Taking

27. On June 26, 2019, the Wall Street Journal published an article describing StockX as the “Latest \$1 Billion Unicorn” and how StockX had “closed a round of venture funding that valued the startup at more than \$1 billion” by “riding the sneaker-reselling craze **fueled by teens.**”⁸ And in an April 2019 article, Vox observed that “StockX has benefited from the rising popularity of acquiring tough-to-buy sneakers, especially among millennial men and **teenage boys.**”⁹

28. According to a recent article in the New York Times, at the second annual “StockX Day” in April 2018, among the “rabid collectors” of StockX merchandise was “the 12-year-old son of a Venmo executive who had flown in for

Stock with Teens Survey.’ Thirty-one percent of male teens and 22% of female teens consider themselves sneakerheads (sneaker enthusiasts or collectors). Teens surveyed own eight pairs of sneakers on average, and at least 30% buy a new pair every month.”) (Last visited, August 2019) (Exhibit 5); <https://www.nytimes.com/2018/01/04/insider/peak-sneaker-inside-sneaker-con.html> (“[t]he heart and soul of the [Sneaker Con event sponsored by StockX] was the trading pit, an area in the back where a vibrant crowd of mostly teenage boys was talking and holding up sneakers, looking for buyers.”) (Last visited, August 2019) (Exhibit 6); <https://www.today.com/parents/sneakers-heart-sole-teen-boys-wbna36217370> (“What Imelda Marcos did with shoes, teenage boys do with sneakers.”) (Last visited, August 2019) (Exhibit 7).

⁸ <https://www.wsj.com/articles/stockx-hub-for-sneakerheads-is-latest-1-billion-unicorn-11561571959> (Last visited, August 2019) (emphasis added) (Exhibit 8).

⁹ <https://www.vox.com/2019/4/19/18486120/stockx-billion-valuation-funding-dst-ggv-sneakerhead> (Last visited, August 2019) (emphasis added) (Exhibit 9).

the event. To the crowd's delight, the 12-year-old scored an autographed LeBron James basketball jersey during a raffle."¹⁰

29. Indeed, Dan Gilbert, the billionaire founder of Quicken Loans, and co-founder of StockX, first began researching the business prospects of online sneaker culture and sales when he "noticed that his teenage son was flipping sneakers on eBay for profit."¹¹

30. Gilbert personally acknowledged the importance of the teenage market to StockX's business strategy in an interview with Sole Collector back in February 2016, shortly after StockX was formed: "The amount of interest and activity among my boys and their friends about sneakers was just crazy," Gilbert said. "Then I start asking other people that have teenage boys, and it's almost 90-95 percent of the people that I asked said the same thing."¹²

¹⁰ <https://www.nytimes.com/2018/07/06/business/smallbusiness/stockx-sneakerheads-luxury-goods.html?smid=nytcare-ios-share&module=inline> (Last visited, Aug. 6, 2019) (Exhibit 1).

¹¹ <https://www.wsj.com/articles/this-website-is-the-stock-market-for-nikes-and-rolaxes-1543251772> (Last visited, August 2019) (Exhibit 10).

¹² <https://solecollector.com/news/2016/02/campless-stockx-dan-gilbert> (Last visited, August 2019) (Exhibit 11).

31. StockX has become a “leading gauge of market value in the sneaker world” and now sponsors large trade shows to which teenage, and pre-teenage, kids flock.¹³

32. StockX specifically targets investors with “cultural cachet” among its young audience, including Eminem and the actor Mark Wahlberg.¹⁴

33. StockX also contains a link to its terms of service on the new user registration page. Buried in those terms of service, among many other fine-print details, is a forced-arbitration clause and class-waiver provision.

34. Based on their status as minors, Plaintiff and the Class are not bound by StockX’s forced-arbitration and class-waiver provisions.

IV. Minors are a high-value target for cyber criminals and are particularly vulnerable to long-term identity theft and PII misuse.

35. According to numerous media reports and studies, stealing the identity of minors is especially attractive to cyber criminals for a host of reasons, including:

- (1) minors’ credit reports are clean, which makes them particularly valuable;
- (2) minors do not check their credit reports or review monthly bills the way adults do;
- (3) thieves are more likely to have unfettered access to minors’ identity and credit for

¹³ <https://www.freep.com/story/money/business/2018/07/09/detroit-stockx-sniffs-out-fake-sneakers/731070002/> (“Many in the crowd of buyers were teenage boys. Some looked no older than 12.”) (Last visited, August 2019) (Exhibit 12).

¹⁴ *Id.*

years or even decades; (4) it is often difficult or impossible to place a freeze on a minor's credit report—because they don't yet *have* credit; and (5) minors are less likely to receive notice, or to have an opportunity to take notice in the event that identity theft occurs or is ongoing, such as, e.g., if fraudulent accounts or charges occur under their names, if fake tax returns are filed in their names, if fraudulent health care is obtained under their identity, and if their information is fraudulently used in connection with employment.¹⁵

36. For these and other reasons, identity theft is a growing problem in the United States as it relates to our minor population. More than 1 million minors were victims of identity theft or fraud in 2017, totaling \$2.6 billion in fraudulent activity.¹⁶

37. In fact, in 2017, among notified breach victims, 39% of minors became victims of actual fraud (as opposed to 19% of adults).¹⁷

38. According to a report on child identity theft published by Carnegie Mellon, a study based on identity protection scans of 40,000 U.S. children, the risk

¹⁵ <https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html> (Last visited, August 2019) (Exhibit 13).

¹⁶ <https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html> (Last visited, August 2019) (Exhibit 14). *See also* <https://www.nbcnews.com/business/consumer/more-1-million-children-were-victims-id-theft-last-year-n885351> (Last visited, August 2019) (Exhibit 15).

¹⁷ <https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html> (Last visited, August 2019) (Exhibit 15).

that someone was using their social security number was 51 times higher than the rate for adults in the same population, with the largest fraud being against a 16-year-old girl for \$725,000.¹⁸

39. The Carnegie Mellon report continues: “[t]he potential impact [of identity theft] on the child’s future is profound; it could destroy or damage a child’s ability to win approval on student loans, acquire a mobile phone, obtain a job, or secure a place to live.”¹⁹

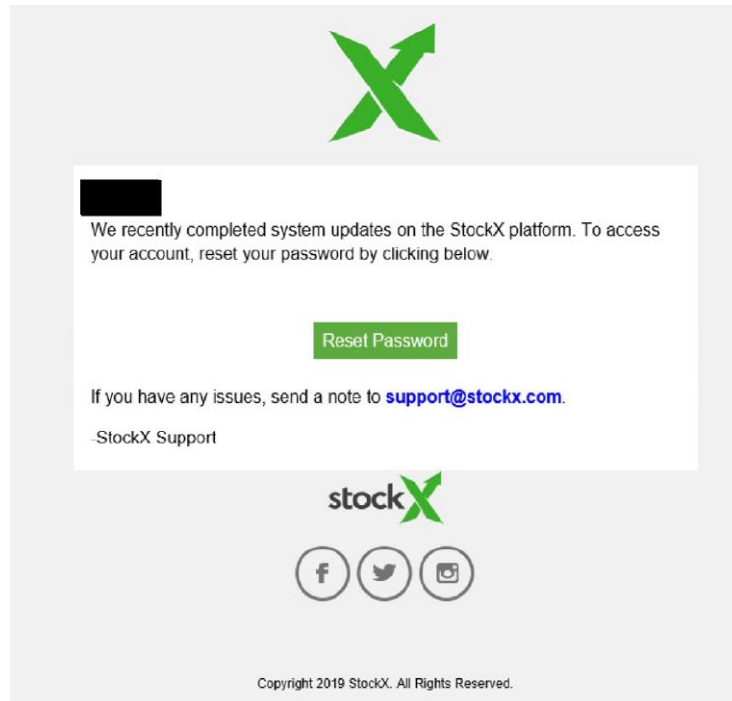
40. Based on StockX’s laser-focus on its young teenage demographic, StockX was well aware of the economic and reputational value of exploiting that market for its own monetary gain, and it should have been equally concerned with protecting the PII entrusted to it by that valuable and relatively defenseless group.

V. The data breach and StockX’s attempted cover-up

41. On August 1, 2019, StockX sent its users, including Plaintiff and the Class, an email notification advising that StockX had “recently completed system updates on the StockX platform” and requiring them to reset their passwords.

¹⁸ https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf, at PDF p. 4 (Last visited, August 2019) (Exhibit 16).

¹⁹ https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf, at PDF p. 3 (Last visited, August 2019) (Exhibit 16).



42. This notification was based on a deception. In reality, StockX’s password-reset notification was not a result of “system updates,” as StockX falsely claimed; rather, StockX had experienced a data breach several months before the notification.

43. According to several news stories published on August 3, 2019—several days after StockX’s fake “system updates” email—more than 6.8 million user accounts were stolen from StockX by a hacker in May 2019, who then listed the stolen data on the “dark web,” an encrypted online area not indexed by conventional search engines that functions, in part, as a marketplace for thieves to buy and sell stolen PII.²⁰

²⁰ See <https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/> (Last accessed, August 2019) (Exhibit 17).

44. Information relating to this data breach was provided to TechCrunch, a media outlet emphasizing technology and cyber news, by an “unnamed data breached seller,” who advised that the data was for sale on the dark web and provided TechCrunch with a sample of 1,000 records. Tech Crunch confirmed this information by contacting customers and providing them information from the stolen records that only the actual customers would know.²¹

45. Following publication of the news stories relating to the data breach, StockX sent a second email to its user base, acknowledging the data breach and admitting that the data breach was the real reason StockX had issued the previous password-reset email.

46. StockX further advised its users, including Plaintiff and the Class, that, according to then-known information, an unknown third-party had been able to gain access to certain customer data, including customer name, email address, shipping address, username, password, and purchase history.

47. On August 8, 2019, StockX sent another email to its users titled “Notice of Data Breach,” stating that it was alerted to “suspicious activity potentially

²¹ <https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/> (Last visited, August 2019) (Exhibit 17).

involving customer data” on July 26, 2019—6 days before their false “system updates” email and 8 days before StockX apprised its users that it had been hacked.

48. The PII stolen from StockX constitutes “personal identifying information,” which qualifies as “identity theft” when used to defraud or otherwise misrepresent with the intent of harming the owner of the information. Identity theft can occur by using (with the intent to defraud) information such as: name, birth date, address, telephone number, passwords, usernames, or other log-in information that can be used to access a person’s electronic content, including content stored on a social networking site.²²

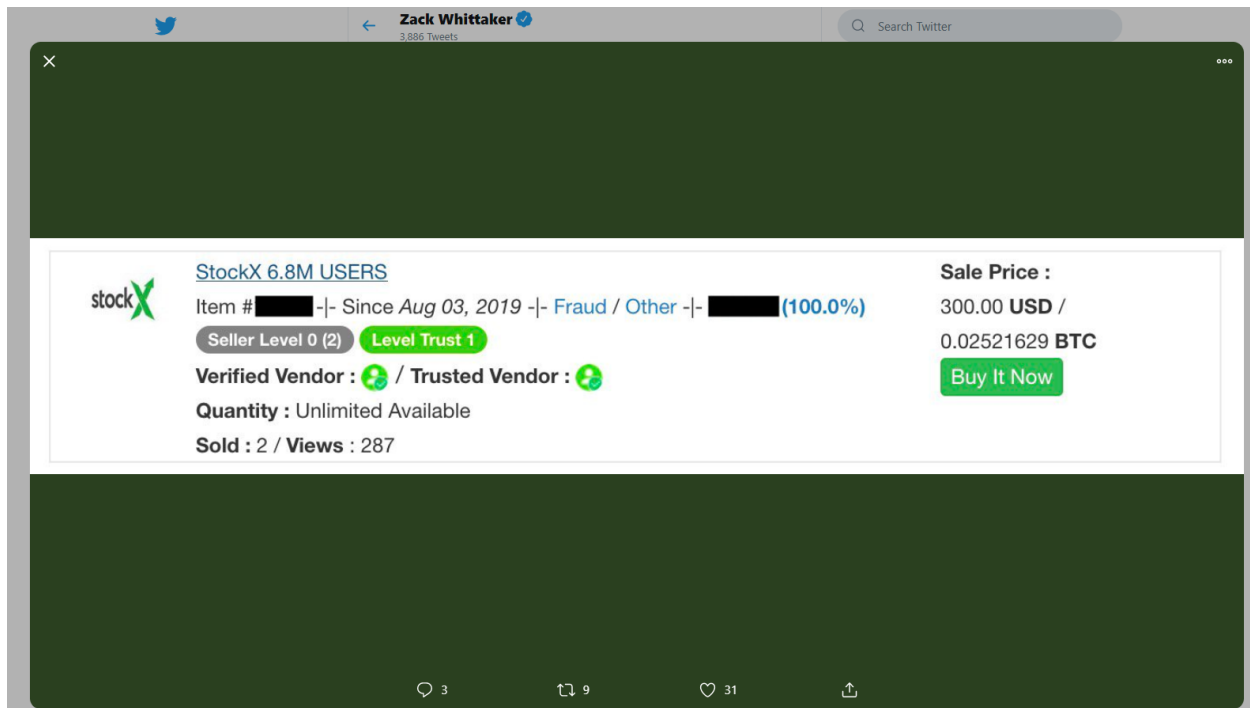
49. The information stolen from StockX included usernames and passwords—PII that is highly valued amongst cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for \$15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay (\$12), Amazon (\leq \$10), and Walmart (\leq \$10) are not far behind.²³ In fact, there is a well-

²² See K.S.A. 21-6107(2).

²³ <https://fortune.com/2018/03/07/apple-id-dark-web-cost/> (Last visited, August 2019) (Exhibit 18). See also <https://www.npr.org/2018/02/22/588069886/take-a-peek-inside-the-market-for-stolen-usernames-and-passwords> (Last visited, August 2019) (Exhibit 19).

established market for stolen account credentials on the Dark Web, including StockX credentials.²⁴

50. In early reports, prior to StockX notifying Plaintiff and the Class that their PII had been stolen, the StockX data had already been sold at least twice for \$300 on the dark web.



51. Unsurprisingly, some users appear to have already been defrauded in the time between StockX's deceptive August 1 "system update" email and the August 3 email acknowledging that StockX had been hacked. One such user posted on Twitter

²⁴ <https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/> (Last visited, August 2019) (Exhibit 20); <https://www.techradar.com/news/nearly-620-million-stolen-accounts-for-sale-on-dark-web> (Last visited, August 2019) (Exhibit 21).

posted a screenshot of an allegedly fraudulent purchase for a Jordan 1 sneaker for more than \$23,000 that occurred between the August 1 and August 3 emails from StockX.

52. On information and belief, it is not difficult to perceive one way in which criminals could leverage the stolen StockX data for a highly profitable enterprise. The criminals purchase the StockX data and thereby obtain Plaintiff's and the Class's stolen PII, including email address, usernames, passwords, shipping addresses, etc.; StockX sends its users a password-reset email based on its fake "system update" notice; the criminals trigger a password-reset through StockX's system and intercept the confirmation email by logging in to the user's email using the stolen StockX PII; and the criminal updates the StockX password and initiates fraudulent purchases redirecting either the funds, the merchandise, or both. This is but one example of many ways in which the stolen PII belonging to Plaintiff and the Class could be misused now and into the future.

53. The PII that Plaintiff and the Class entrusted to StockX has been stolen, sold, and purchased by criminals who will seek and have already sought to misuse it.

54. According to more recent reporting, bad actors “have already begun to decrypt the stolen passwords and it is expected for this information to be used in future attacks.”²⁵

55. The stolen information has also been added to the data breach monitoring website, “Have I Been Pwned,”²⁶ which added the StockX database to their website so users can check to see if their email was included in the breach. As shown in the below screenshot from “Have I Been Pwned,” 6,840,399 accounts were stolen from StockX.



²⁵ <https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/> (Last visited, August 2019) (Exhibit 22).

²⁶ <https://haveibeenpwned.com/> (pronounced “poned”) (Last visited, August 2019) (Front page of website attached as Exhibit 23, reference to StockX breach on PDF page 2).

56. A search of “Have I Been Pwned” confirms that Plaintiff’s information was exposed as a result of the StockX data breach.²⁷

57. Though originally being sold for \$300, as referenced above, the username and password combinations are now being distributed on underground hacker forums for as little as \$2.15, which virtually guarantees that it will be widely distributed. And for those cybercriminals who do not want to go through the trouble of decrypting the user accounts, they can purchase up to 367,000 decrypted accounts (of the more than 6.8 million stolen accounts) for \$400.²⁸

58. Now that the stolen data is available for a minimal sum, the credentials will be used in “credential stuffing” attacks, which involve thieves compiling and using usernames and passwords that were leaked from different data breaches to try and gain access to accounts at other sites.²⁹

59. The founder of Rendition Infosec, a cybersecurity firm staffed by former NSA, DoD, and US Cyber Command Operators stated that StockX’s misleading

²⁷ <https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/> (Last visited, August 2019) (Exhibit 23).

²⁸ *Id.*

²⁹ <https://www.wired.com/story/what-is-credential-stuffing/> (Last visited, August 2019) (Exhibit 24); <https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/> (Last visited, August 2019) (Exhibit 23).

conduct “robbed their users of the chance to evaluate their exposure” by not informing its users of the breach when it happened.³⁰

60. Plaintiff’s and the Class’s PII was among the confidential information compromised in the StockX data breach, causing Plaintiff and the Class to suffer injury and damages, including but not limited to the improper disclosure of the PII, the loss of the value of the PII, ongoing disclosures and dissemination of the PII, the imminent threat of identity theft and other fraud against Plaintiff and the Class, the loss of Plaintiff’s and the Class’s privacy, and out-of-pocket expenses and time devoted to mitigating the effects of the data breach and ascertaining the extent of Plaintiff’s and the Class’s losses and exposure.

61. Plaintiff and the Class would never have provided their PII to StockX if it was known the security provided by StockX was not reasonable security or that StockX was not providing the security that StockX represented it would provide, as was revealed by the data breach described by media outlets following StockX’s false “system updates” email.

³⁰ <https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/> (Last visited, August 2019) (Exhibit 17).

62. Plaintiff and the Class would further never have provided their PII to StockX if they had known that StockX would seek to deceive Plaintiff and the Class in the event that StockX was subject to a data breach.

63. Plaintiff and the Class would never have provided their PII to StockX if StockX had disclosed that it lacked adequate security measures and data security practices, as was revealed by the media reports.

64. Plaintiff and the Class have been damaged in that Plaintiff and the Class spent time and will spend additional time in the future speaking with representatives; researching and monitoring accounts; researching and monitoring credit history; responding to identity theft incidents; purchasing identity protection; and suffering annoyance, interference, and inconvenience, as a result of the data breach.

65. StockX's actions and failures to act when required have caused Plaintiff and the Class to suffer harm and face the significant and imminent risk of future harm, including:

- theft of their PII;
- costs associated with researching the scope and nature of the breach and of responding to the data breach and attendant risks and harm in light of StockX's misinformation campaign;

- costs associated with the detection and prevention of identity theft and unauthorized use of their PII;
- unauthorized access to and misuse of their online accounts;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the StockX data breach—including finding fraudulent charges and enrolling in and purchasing credit monitoring and identity theft protection services;
- the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals;
- damages to and diminution in value of their PII entrusted, directly or indirectly, to StockX with the mutual understanding that StockX would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and
- continued risk of exposure to hackers and thieves of their PII, which remains in StockX possession and is subject to further breaches so long

as StockX fails to undertake appropriate and adequate measures to protect Plaintiff and the Class.

66. Consequently, Plaintiff and the Class are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the data breach and StockX's deceptive and unconscionable conduct.

CLASS ALLEGATIONS

67. Plaintiff brings this action on behalf of Plaintiff and those minors similarly situated both across the United States and within their State or Territory of residence.

68. Class certification is appropriate under Fed. R. Civ. P. 23(a) and (b)(1), (b)(2), and/or (b)(3).

69. **Nationwide Class:** All minor individuals in the United States whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach described herein.

70. **Numerosity (FRCP 23(a)(1)):** The class satisfies the numerosity requirement because it is composed of millions of persons, in numerous locations. The number of class members is so large that joinder of all its members is impracticable.

71. Commonality and Predominance (FRCP 23(a)(2) and 23(b)(3)):

There are questions of law and fact common to the Class, and these questions predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to:

- whether the data breach constitutes a breach of the data-security commitments and obligations to protect and safeguard PII made to the Class by StockX in its privacy policy;
- whether StockX acted with intent or reckless indifference with respect to the Class and the safety, value, and security of the Class's PII when it falsely advised the Class that a password reset was required because of a "system update," not a data breach, which StockX knew to be the case at the time of its statements;
- whether StockX was negligent in its representations to the Class concerning its security protocols;
- whether StockX's conduct and practices described herein amount to acts of intrusion upon seclusion under the laws of the "Intrusion Upon Seclusion States" defined below;
- whether StockX was negligent in making misrepresentations to the Class when it falsely advised the Class that a password reset was

required because of a “system update,” not a data breach, which StockX knew to be the case at the time of its statements;

- whether StockX was negligent in establishing, implementing, and following security protocols;
- whether StockX failed to abide by all applicable legal requirements (including relevant state law requirements) and industry standards concerning the privacy and confidentiality of the Class members’ PII;
- whether the Class members’ PII was compromised and exposed as a result of the data breach and the extent of that compromise and exposure;
- whether the Class members are entitled to compensatory damages; and
- whether the Class members are entitled to punitive damages.

72. **Typicality (FRCP 23(a)(3)):** Plaintiff’s claims are typical of the claims of the members of the Class because Plaintiff’s claims, and the claims of all Class members, arise out of the same conduct, policies, and practices of StockX, as alleged herein, and all members of the Class are similarly affected by StockX’s wrongful conduct and the data breach described herein.

73. **Adequacy of Representation (FRCP 23(a)(4)):** Plaintiff will fairly and adequately represent the Class and have retained counsel competent in the

prosecution of class action litigation; data breach litigation; data privacy and cybersecurity law; and technical I.T. concepts, practices, and theory. Plaintiff has no interests antagonistic to those of other members of the Class. Plaintiff is committed to the vigorous prosecution of this action and anticipates no difficulty in the management of this litigation as a class action.

74. Class action status in this action is warranted under Rule 23(b)(1)(A) because prosecution of separate actions by the members of the Class would create a risk of establishing incompatible standards of conduct for Defendants. Class action status is also warranted under Rule 23(b)(1)(B) because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

75. In the alternative, certification under Rule 23(b)(2) is warranted because Defendants acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive, declaratory, or other appropriate equitable relief with respect to the Class as a whole.

76. In the alternative, certification under Rule 23(b)(3) is appropriate because questions of law or fact common to members of the Class predominate over

any questions affecting only individual members, and class action treatment is superior to the other available methods for the fair and efficient adjudication of this controversy.

CAUSES OF ACTION AND CLAIMS FOR RELIEF

COUNT I — Negligence (On behalf of Plaintiff and the Class)

77. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

78. StockX owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that StockX collected.

79. StockX owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII that StockX collected.

80. StockX owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the Class of a data breach as soon as possible after it is discovered.

81. StockX owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

82. StockX solicited, gathered, and stored the PII provided by Plaintiff and the Class.

83. StockX knew or should have known it inadequately safeguarded this information.

84. StockX knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and the Class, and StockX was therefore charged with a duty to adequately protect this critically sensitive information.

85. StockX had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's willingness to entrust StockX with their PII was predicated on the understanding that StockX would take adequate security precautions. Moreover, only StockX had the ability to protect its systems and the PII it stored on them from attack.

86. StockX's own conduct also created a foreseeable risk of harm to Plaintiff and the Class and their financial information. StockX's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

87. StockX breached its duties to Plaintiff and the Class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the financial information of Plaintiff and the Class.

88. StockX breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

89. StockX breached the duties it owed to Plaintiff and the Class by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

90. StockX breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose that Plaintiff's and the Class members' PII had been improperly acquired or accessed.

91. The law further imposes an affirmative duty on StockX to timely disclose the unauthorized access and theft of the financial information to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial information.

92. StockX breached its duty to notify Plaintiff and the Class by failing to provide Plaintiff and the Class information regarding the breach until August 3, 2019. To date, StockX has not provided sufficient information to Plaintiff and the Class

regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

93. As a direct and proximate result of StockX's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT II – Negligent Misrepresentation
(On behalf of Plaintiff and the Class)**

94. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

95. Through its Privacy Policy and other actions and representations, StockX held itself out to Plaintiff and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the PII belonging to Plaintiff and the Class.

96. StockX knew or should have known that it was not in compliance with the representations made in its Privacy Policy.

97. StockX knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to Plaintiff and the Class.

98. Neither Plaintiff nor the Class could have known or discovered the material weaknesses in StockX's data security practices.

99. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiff and the Class.

100. StockX also failed to exercise reasonable care when it falsely conveyed information to Plaintiff and the Class on August 1, 2019, relating to the underlying need for Plaintiff and the Class to reset their passwords, which misrepresentation failed to sufficiently convey the facts underlying the actual need for a password reset; failed to instill the urgency of the need to reset their passwords immediately; provided the thieves of the stolen information with additional time and cover to further purloin and re-sell the stolen PII belonging to Plaintiff and the Class; provided the thieves and the purchasers of the stolen information with an opportunity to directly defraud Plaintiff and the Class; and failed to adequately apprise Plaintiff and the Class of the fact that their PII was compromised and in imminent jeopardy of falling further into the hands of cyber criminals.

101. StockX also failed to exercise reasonable care when it failed to timely communicate information concerning the data breach that it knew, or should have known, compromised PII of Plaintiff and the Class.

102. Plaintiff and the Class relied on Capital One's representations, or lack thereof, when they provided their PII to StockX.

103. As a direct and proximate result of StockX's negligent misrepresentations by omission, Plaintiff and the Class have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

**COUNT III – Fraud and fraud through silence
(On behalf of Plaintiff and the Class)**

104. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

105. StockX knew that data belonging to Plaintiff and the Class had been stolen prior to its false “system update” email on August 1, 2019. This knowledge was of material importance relating to the safety, value, and security of the PII belonging to Plaintiff and the Class.

106. Plaintiff and the Class did not know about the theft of their PII from StockX, nor could they have discovered such information by exercise of reasonable diligence.

107. StockX was under an obligation to forthrightly and promptly communicate the pertinent facts relating to the data breach to Plaintiff and the Class to permit them to undertake appropriate protective measures to mitigate the harm caused by StockX's failure to adequately protect the data and to reasonably safeguard their identities, livelihood, and safety.

108. Despite its knowledge of the data breach and the imminent danger the PII theft posed, StockX failed to timely and forthrightly advise Plaintiff and the Class of the breach; instead, StockX falsely advised Plaintiff and the Class that a password reset was necessary because of “system upgrades.”

109. In conjunction, and simultaneous with its misrepresentations relating to the need for Plaintiff and the Class to reset their passwords, StockX intentionally failed to communicate to Plaintiff and the class material facts relating to the data breach, the theft of their PII, the urgency with which Plaintiff and the Class needed to update their passwords, the concurrent and urgent need for Plaintiff and the Class to protect and safeguard their data, and other measures needed in light of the data breach.

110. Plaintiff and the Class justifiably relied on StockX’s misrepresentations and StockX’s intentional withholding of material facts, suffered injuries as a result, and were damaged as discussed herein and as will be proven at trial.

111. As a direct result of StockX’s fraud and fraud by silence, Plaintiff and the Class have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

**COUNT IV – Negligence Per Se – FTC Act
(On behalf of Plaintiff and the Class)**

112. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

113. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair...practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as StockX of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Equifax’s duty.

114. StockX violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII; by failing to comply with applicable industry standards; by falsely representing to its users and the public the nature and scope of the data breach and the need for password resets; and by unduly delaying reasonable notice of the actual breach. StockX’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a data breach, and the foreseeable consequences of misleading its users and the public.

115. StockX’s violation of Section 5 of the FTC Act constitutes negligence per se.

116. Plaintiff and the Class are within the category of persons the FTC Act was intended to protect.

117. The harm that occurred as a result of the data breach described herein and in the various media reports detailing StockX's deception relating to the data breach is the type of harm the FTC Act was intended to guard against.

118. As a direct and proximate result of StockX's negligence per se, Plaintiff and the Class have suffered injury, have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in StockX's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT V – Unjust Enrichment
(On behalf of Plaintiff and the Class)**

119. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

120. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was collected and maintained by StockX. This PII was conferred on StockX directly by Plaintiff and the Class themselves.

121. StockX was benefitted by the conferral upon it of the PII pertaining to Plaintiff and the Class and by its ability to retain and use that information. StockX understood that it was in fact so benefitted.

122. StockX also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon StockX maintaining the privacy and confidentiality of that PII.

123. But for StockX's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and the Class would not have transferred PII to StockX or entrusted their PII to StockX, and StockX would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers and users of its platform, gaining the reputational advantages conferred upon it by Plaintiff and the Class, collecting excessive sales commissions as described herein, raising investment capital as described herein, and realizing excessive profits.

124. As a result of StockX's wrongful conduct as alleged in this Complaint (including, among other things, its deception of Plaintiff, the Class, its users in general, and the public relating to the nature and scope of the data breach; its utter failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiff and the Class without having adequate data security measures; and its other conduct facilitating the theft of that PII) StockX has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

125. StockX's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

126. Under the common law doctrine of unjust enrichment, it is inequitable for StockX to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. StockX's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

127. The benefit conferred upon, received, and enjoyed by StockX was not conferred officiously or gratuitously, and it would be inequitable and unjust for StockX to retain the benefit.

128. StockX is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on StockX as a result of its wrongful conduct, including specifically the value to StockX of the PII that was stolen in the StockX data breach and the profits StockX is receiving from the use and sale of that information.

**COUNT VI – Violation of State Data Breach Statutes
(On behalf of Plaintiff and all members of the Class residing in states
with applicable data breach statutes)**

129. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

130. StockX is in possession of PII belonging to Plaintiff and the Class and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

131. StockX failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by the laws of the State of Kansas, Michigan, and all other applicable State laws.

132. StockX further failed to provide reasonable and timely notice of the data breach to Plaintiff and the Class as required by the various state data breach notification statutes, including, without limitation, K.S.A. 50-7a01, *et seq.*

133. As a result of StockX's failure to reasonably safeguard the PII belonging to Plaintiff and the Class, and StockX's failure to provide reasonable and timely notice of the data breach to Plaintiff and the Class, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in StockX's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT VII – Intrusion Upon Seclusion
(On behalf of Plaintiff and all members of the Class
who reside in Intrusion Upon Seclusion States)**

134. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

135. Plaintiff brings this claim on behalf of persons who reside in the following states: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia (the “Intrusion Upon Seclusion States”).

136. Plaintiff had a reasonable expectation of privacy in the PII Defendant mishandled.

137. By failing to keep Plaintiff’s Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Plaintiff’s privacy by:

- Intruding into Plaintiff’s private affairs in a manner that would be highly offensive to a reasonable person; and

- Publicizing private facts about the Plaintiffs, which is highly offensive to a reasonable person.

138. StockX knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider StockX's actions highly offensive.

139. StockX invaded Plaintiff's right to privacy and intruded into Plaintiff's private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

140. As a proximate result of such misuse and disclosures, Plaintiff's reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. StockX's conduct amounted to a serious invasion of Plaintiff's protected privacy interests.

141. In failing to protect Plaintiff's Private Information, and in misusing and/or disclosing their Private Information, StockX has acted with malice and oppression and in conscious disregard of Plaintiff's and the Class Members' rights to have such information kept confidential and private. The Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

**COUNT VIII – Declaratory Judgment
(On behalf of Plaintiff and the Class)**

142. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

143. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

144. An actual controversy has arisen in the wake of the StockX data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether StockX is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII. Plaintiff allege that StockX's data security measures remain inadequate.

145. Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

146. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that StockX continues to owe a legal duty to secure

consumers' PII and to timely notify consumers of any data breach and that StockX is required to establish and implement data security measures that are adequate to secure consumers' PII.

147. The Court also should issue corresponding prospective injunctive relief requiring StockX to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

148. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury, and Plaintiffs and the Class lack an adequate legal remedy. The threat of another StockX data breach is real, immediate, and substantial. If another breach at StockX occurs, Plaintiff will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

149. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to StockX if an injunction is issued. Among other things, if another massive data breach occurs at StockX, Plaintiff will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to StockX of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and StockX has a pre-existing legal obligation to employ such measures.

150. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at StockX, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of members of the Class, as applicable, respectfully requests that the Court enter judgment in their favor and against StockX, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;
2. That Plaintiff be granted the declaratory relief sought herein;
3. That the Court grant permanent injunctive relief to prohibit StockX from continuing to engage in the unlawful acts, omissions, and practices described herein;
4. That the Court award Plaintiff and Class and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

7. That the Court award pre- and post-judgment interest at the maximum legal rate; and

8. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution.

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demand a jury trial on all claims so triable.

Dated: August 19, 2019

Respectfully submitted,

/s/ E. Powell Miller

E. Powell Miller (P39487)

Sharon S. Almonrode (P33938)

William Kalas (P82113)

THE MILLER LAW FIRM, P.C.

950 W. University Dr., Suite 300

Rochester, Michigan 48307

Telephone: (248) 841-2200

Fax: (248) 652-2852

epm@millerlawpc.com

ssa@millerlawpc.com

wk@millerlawpc.com

FOULSTON SIEFKIN LLP

Scott C. Nehrbass

Daniel J. Buller

32 Corporate Woods, Suite 600

9225 Indian Creek Parkway

Overland Park, KS 66210-2000

Tel: (913) 253-2144

Fax: (866) 347-1472

snehrbass@foulston.com

dbuller@foulston.com

FOULSTON SIEFKIN LLP

Boyd A. Byers

1551 N. Waterfront Parkway, Suite 100

Wichita, Kansas 67206-4466

Tel: (316) 291-9796

Fax: (866) 559-6541

bbyers@foulston.com

*ATTORNEYS FOR PLAINTIFF AND THE
PROPOSED CLASS*

INDEX OF EXHIBITS

<i>EXHIBIT</i>	<i>DESCRIPTION</i>
Exhibit 1	07.06.18 NY Times- <i>StockX Aims to Tame 'Chaos'</i>
Exhibit 2	05.15.18 Marketplace- <i>How StockX is Revolutionizing the Sneaker Reseller Business Online</i>
Exhibit 3	06.26.19 Detroit Free Press- <i>Detroit Startup StockX</i>
Exhibit 4	08.02.19-Business Insider- <i>Meet the 15-Year Old Who Has Made 6 Figures</i>
Exhibit 5	04.11.19Yahoo Finance- <i>American Teens Becoming Sneakerheads</i>
Exhibit 6	01.04.18 NY Times- <i>Inside Sneaker Con</i>
Exhibit 7	04.07.10 Associated Press- <i>Sneakers: Heart and Sole</i>
Exhibit 8	06.26.19 Wall Street Journal- <u><i>StockX Hub for Sneakerheads</i></u>
Exhibit 9	04.19.19 Vox- <i>A Giant New Investment</i>
Exhibit 10	11.26.18 Wall Street Journal- <i>Website is Stock Market for Nikes and Rolexes</i>
Exhibit 11	02.08.16 Sole Collector- <i>Dan Gilbert is Investing</i>
Exhibit 12	07.09.18 Detroit Free Press- <i>Fast-Growing Detroit Startup</i>
Exhibit 13	04.17.15 NY Times- <i>Identity Theft Poses Trouble</i>
Exhibit 14	04.24.18 CNBC- <i>Kids are Victims too</i>
Exhibit 15	06.21.18 NBCNews- <i>1 Million Children Were Victims</i>
Exhibit 16	Child Identity Theft

Exhibit 17	08.03.19 Techcrunch- <i>StockX was Hacked</i>
Exhibit 18	03.07.18 Fortune- <i>Stolen Apple ID</i>
Exhibit 19	02.22.18 NPR- <i>Take a Peek Inside</i>
Exhibit 20	12.2017 Krebs on Security- <i>Market for Stolen Account Credentials</i>
Exhibit 21	02.12.19 Techradar- <i>Stolen Accounts for Sale on Dark Web</i>
Exhibit 22	08.11.19 Bleepingcomputer- <i>Database from StockX Sold Online</i>
Exhibit 23	<i>Check if you have an account that has been compromised in a data breach</i>
Exhibit 24	02.17.19 Wired- <i>What is Credential Stuffing?</i>

Exhibit 1

The New York Times

A Nasdaq for Sneakerheads? StockX Aims to Tame 'Chaos' of Luxury Market

By Dan Hyman

July 6, 2018

The Times reports from 140+ countries.

When a story starts with a city, it means we were there to report it.

[Don't show me messages like this](#)

DETROIT — Standing among more than 350 pairs of sneakers in his converted attic, Josh Luber, a self-proclaimed “sneakerhead,” held a pair of nearly identical Nike Air Jordan IVs in each hand. He eyed them as if they were rare biological specimens.

One was a standard model of the shoe that typically sells on secondary markets for \$160; the other was an ultrarare model designed by the rapper Eminem that can fetch more than \$20,000.

“This is the sneaker industry right here,” he said, referring to how brands use scarcity and buzz to drive up prices in secondary markets and create brand cachet.

EXHIBIT 1



The StockX office features a replica of the Quicken Loans Arena basketball court, home of the Cleveland Cavaliers. Dan Gilbert, a StockX co-founder, is the majority owner of the Cavaliers.

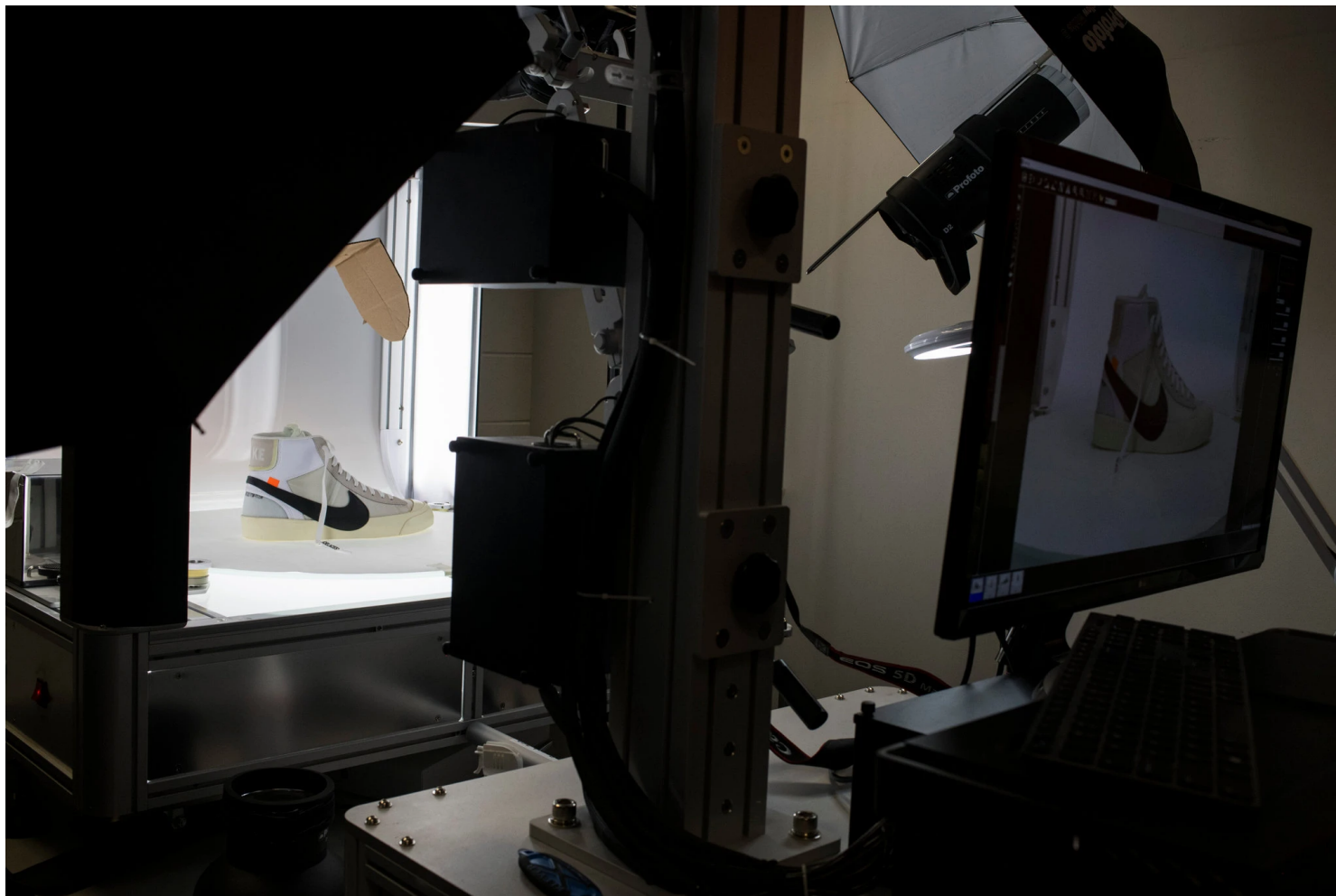
Brittany Greeson/The New York Times

That price volatility helped inspire Mr. Lubner to found StockX, an e-commerce platform for luxury goods. The familiar model of buying and selling high-end shoes “leads to chaos,” Mr. Lubner argued. When limited-edition sneakers are released, people camp in line for days to get their hands on a pair, and the opportunity to make a quick profit can lead some to bribe store workers. It can even turn to violence: In 2015, a Brooklyn teenager was shot in his foot for cutting in line.

So Mr. Lubner, the company’s chief executive, and his co-founders, including Dan Gilbert, the billionaire founder of Quicken Loans, came up with what they believe to be an elegant solution to determine the value of high-end goods: Treat them as if they were stocks.

You have 5 free articles remaining.
Subscribe to The Times

On StockX, products, which include streetwear, handbags and watches in addition to sneakers, are assigned ticker symbols. Sellers put out asking prices, and buyers bid. Users can see data like recent sale figures from across the internet, price volatility, and 52-week highs and lows. Once a bid and an ask coincide, the sale is automatically made.



A Nike shoe is photographed at the StockX offices for customers to view online in 360 degrees.
Brittany Greeson/The New York Times

Niche marketplaces for high-end goods are not new: Before sneakerheads connected on the internet, there were consignment shops reselling shoes and stores that specialized in just one brand of watches. But when people have access to hard data on how a product is selling across the market, they can best understand its true value, which has the potential to bring down prices, Mr. Luber argued.

His goal is to work directly with retailers and have products open on StockX in an initial public offering of sorts. He said that this would provide more pricing stability, and that allowing average consumers access when new products were released could help brands expand their customer bases.

“Brands love the fact that, ‘Oh, yeah, people waited three days outside of the store to get my product,’” Mr. Luber said of traditional product releases. “Our whole idea is, ‘Look, there’s just a different way to benefit from that that adds order to it.’”

In April, 150 of StockX’s most loyal buyers and sellers — sneakerheads and small-business owners — gathered in Detroit for StockX Day. Brittany Greeson/The New York Times

In April, 150 of StockX's most loyal buyers and sellers, selected from more than 5,000 applicants, gathered in Detroit for the second StockX Day. Some attendees treated Mr. Lubber as if he were a celebrity. During a question-and-answer portion, a 24-year-old woman from New York told him that his 2015 TED Talk on the sneaker industry had inspired her to become an entrepreneur.

"You are why we exist!" Mr. Lubber, wearing a pair of Air Jordan I sneakers customized for StockX by Jake Ferrato, a shoemaker in Cleveland, told the crowd. The attendees included employees from Nike and Complex, owners of resale businesses, and rabid collectors, including the 12-year-old son of a Venmo executive who had flown in for the event. To the crowd's delight, the 12-year-old scored an autographed LeBron James basketball jersey during a raffle.

Onstage, Mr. Lubber, 40, teased the 56-year-old Mr. Gilbert, wearing a pair of brown hiking boots, like a son poking fun at his decidedly unhip father. Three years as business partners, "and I still can't get you to wear a pair of sneakers," Mr. Lubber said.

More than 5,000 people applied to attend StockX Day, which included a tour of the company's offices.
Brittany Greeson/The New York Times

Mr. Luber, who, like many sneakerheads, speaks of his footwear collection as if it were an ever-expanding portfolio, started collecting at age 10. In 2012, while an analyst at IBM, he founded Campless, a website he described as the Kelley Blue Book for sneakers. When he met with brand representatives, he would describe his dream of a marketplace that treated sneakers as if they were assets. Companies were interested in his data but uninterested in overhauling their sale process.

In April 2015, Mr. Luber was summoned to a meeting with Mr. Gilbert, who had started an in-house incubator and was exploring new business ideas. Mr. Gilbert was intrigued by the idea of a stock-market model for e-commerce and, as the father of a teenage sneakerhead, was convinced that sneakers were a perfect starting point to test the concept.

To protect against knockoffs, sellers ship purchased products to StockX, which authenticates the items and sends them to buyers by day's end, similar to services provided by other high-end marketplaces. StockX takes a 9.5 percent commission on each sale.

StockX's offices occupy almost an entire floor of the One Campus Martius building in Detroit, where Quicken Loans is also headquartered. Brittany Greeson/The New York Times

Since starting in February 2016, StockX has grown to more than 10,000 transactions per day. It has added nearly 170 of its more than 370 employees since the end of April.

“We’ve gone from zero to \$700 million in sales in two years, and most of the world doesn’t even know this exists,” said Greg Schwartz, 37, a co-founder and now the company’s chief operating officer.

As a test of the model of an initial offering, StockX teamed up with Nike in January to release limited-edition LeBron James shoes, with the prices determined by an open auction. The sneakers sold for an average of \$6,000 per pair. Winning buyers could resell the shoes on the platform without ever taking physical ownership of them.

A StockX staff member checking a pair of shoes sold through the site for authenticity.
Brittany Greeson/The New York Times

“This then becomes true commodities trading,” Mr. Luber said. It’s not dissimilar from trading oil futures, he said. In fact, because the items were resold without physically changing hands, StockX worried the shoes might be considered futures and “spent a lot of time talking to lawyers making sure we weren’t running afoul of any securities laws,” Mr. Luber said.

With a billionaire co-founder, capital has not been an issue, but StockX has still sought out investors who Mr. Schwartz said “provide outside value” or cultural cachet: Eminem and his manager, Paul Rosenberg; the actor Mark Wahlberg; Scooter Braun, Justin Bieber’s manager; and Steve Case and Tim Armstrong, former chief executives of AOL.

Noting that AOL aimed to give more Americans access to the internet, Mr. Case said StockX was similarly centered on giving average consumers access to scarce luxury goods, which are often scooped up by insiders. There’s no guarantee those consumers will be able to afford the items, but the prices will at least be fairer, he said.

With StockX, Mr. Luber hopes to make the process of buying high-end goods, such as rare sneakers, more equitable. Brittany Greeson/The New York Times

Outside of capital investment, Mr. Gilbert's involvement has been a major boon to StockX. The company had access to Quicken's resources and employee benefits and to cross-promotional marketing opportunities, such as a Super Bowl ad this year for Rocket Mortgage featuring a teenager wearing a StockX baseball cap. StockX's offices occupy almost an entire floor of Detroit's towering One Campus Martius building, where Quicken has its headquarters.

StockX has two authentication centers and more than 100 authenticators, who go through a 90-day training course. As the authenticators receive items, the details of the product and the sale are available on a computer screen at their station. Once they have performed all the steps in the authentication — which can include smelling the shoe — a shipping label is printed and the seller is automatically paid.

When StockX started, Mr. Luber personally authenticated sneakers in a room of the office before taking them downstairs to be shipped. “And then if the freight elevator would break down for the day, we’d be like, ‘Oh, our whole business is done,’” Mr. Schwartz recalled with a laugh.

But Mr. Luber said the business wasn’t just an excuse to play with sneakers.

“Everyone feels like it’s impossible to get a pair of Off-White Jordans for retail” unless you have insider connections, Mr. Luber said, adding: “There was a reason the Foot Locker manager’s brother won the raffle every time.”

A version of this article appears in print on July 6, 2018, Section B, Page 3 of the New York edition with the headline: A Nasdaq for Sneakerheads? A Way to Tame the High-End Market

Exhibit 2



CEO, Co-Founder and avid sneaker collector Josh Lubber

[HOME \(/\)](#) / [NEWS \(/NEWS\)](#)
/ [PORTRAIT \(/NEWS/PORTRAIT\)](#)

MARKETPLACE

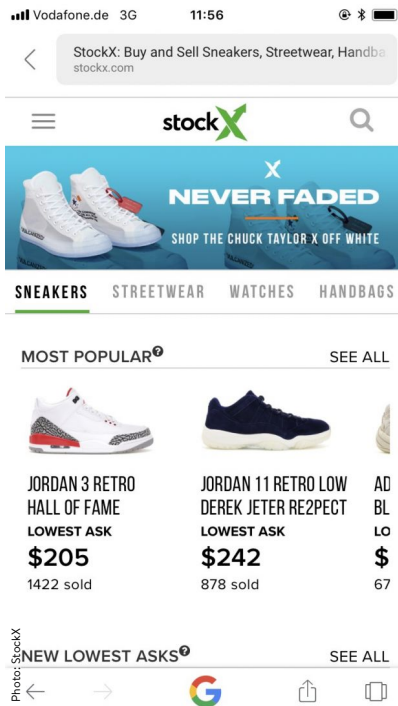
How StockX is revolutionizing the sneaker reseller business online

by **Rebecca Cringean** — May 15, 2018

StockX is the marketplace of things to buy authenticated deadstock sneakers, luxury handbags, watches and now streetwear, too!

In the past, sneakerheads had to buy their retro deadstock sneakers on eBay and eBay clones, taking their chances with authenticity and iffy sellers. Same is true for fans of luxury handbags, watches and other accessories. And don't forget lovers of hot streetwear items. The craze is just as real as what sneakerheads face. Auction sites try their best to make sure there are no imitations but it's still rampant, even, surprisingly, on non-auction sites like Amazon.

EXHIBIT 2



StockX website

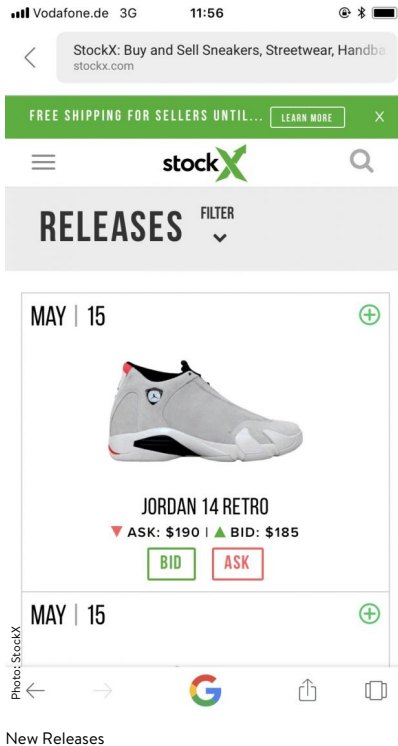
StockX was conceived to eliminate the risk and bring together buyers and sellers, playing middleman to make everyone comfortable and to keep things real. StockX bills itself as “The Stock Market of Things where you can buy and sell deadstock Adidas Yeezy, NMD or Retro Jordans, Supreme Streetwear, luxury handbags, and watches in excellent condition.” Potential buyers float what they’re willing to offer for a product. A seller of that product can accept the price. The folks at StockX then receive the product, authenticate it, release the buyer’s money to the seller and then, as the StockX site says, “You sip a daiquiri, knowing you will never get a fake.” With the addition of streetwear like Bape and Supreme, StockX is cornering the market on deadstock auctions.

We had a chat with CEO, Co-Founder and avid sneaker collector, Josh Luber (who, it should be noted, delivered the world’s first TED talk about the resell sneaker industry) to find out more on the internet’s newest luxury goods hotspot.

Tell us about the premise for StockX.

StockX was originally launched as a partnership between myself, Greg Schwartz (COO) and Dan Gilbert. Greg

had experience launching previous tech companies, so brought past knowledge and experience to the table. Dan took care of the finances and myself, the sneaker expertise. I had previously founded the company Campless, which was basically a sneaker price guide or KBB for sneakers. This site worked by pulling analytics from eBay to track trends in sneaker purchases and sales. The data provided by Campless was used to develop the framework for the launch of StockX.



How is the secondary sneaker market doing in your opinion?

We value the sneaker secondary market at \$6B globally. With the boom in social media, it has become easier for sneakerheads to find, trade and flip shoes from their collections. This has also made the market more mainstream, which adds to the success of brands such as Kanye West's Yeezy lineup. With this growing market, it became harder for people to find reliable outlets to purchase and sell authentic sneakers. This is where StockX comes in. We provide a simple platform that provides full transparency on the value of goods, while guaranteeing authenticity.

Marketplace: How StockX is revolutionizing the sneaker reseller business online

Vodafone.de 3G 11:57

StockX: Buy and Sell Sneakers, Streetwear, Handbags
stockx.com

FREE SHIPPING FOR SELLERS UNTIL... [LEARN MORE](#) X

stockX

PORTFOLIOS [+ PORTFOLIO](#)







USER	ITEMS	VALUE
 kabeshyt...	1201	\$577,874
 Luluskix	1421	\$540,593
 stayfresh	2229	\$456,466
 kyleemm...	766	\$360,582
 Foriegnb...	1116	\$342,826
 Anita_ch...	1135	\$324,792

Photo: StockX

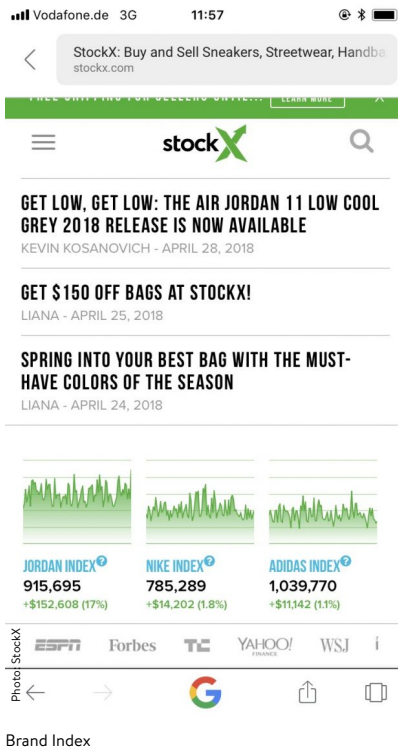
StockX user portfolios

Tell us about the addition of brands like Bape and Supreme.

Streetwear was the perfect next step for StockX. The streetwear and sneaker demographics are quite similar, so we already had a strong base built from our sneaker vertical. Once we were able to find brand experts to lead our authentication teams, the actual launch was easy. We currently offer Supreme, Bape, Palace and Kith.

What new brands can we expect in the near future?

We are focusing on growing our current verticals, which include streetwear, sneakers, watches and handbags. As we continue to grow, we plan to add additional authentication centers around the globe to expedite the shipping and authentication processes and fill more than 50 open positions.



What is currently the hottest StockX item/ask/sell?

Our most popular sneaker is the adidas Yeezy (Kanye's line). The most expensive sneaker that we have seen come across our platform is the Nike Air MAG 'Back to the Future', which sold for more than \$30,000. We currently have a Patek Philippe Sky Moon 5002P watch listed on the site with an ask of \$850,000. That's pretty huge.

Anything else our readers should know?

We really do see StockX as the future of e-commerce -- a transformative platform that harnesses the power of stock market mechanics to allow for efficient pricing and seamless, transparent, and anonymous transactions. We're seeing that user-focused strategy pay off in our growth -- in just two years, we've grown from 20 employees to more than 200 and we continue to hire for open positions as we build.

Read also:



REPORT

Young and brand-obsessed: The

teenage streetwear files

Read more →

(/news/stories/Report-Young-and-brand-obsessed-The-teenage-streetwear-files-13770)



RETAILER TO WATCH

How The Place wants to attract customers with reselling in store

Read more →

(/news/retailertowatch/Retailer-to-watch-How-The-Place-wants-to-attract-customer-with-reselling-in-store-14098)

TOPICS

sneakers (/search/topics/sneakers)

streetwear (/search/topics/streetwear)

eBay (/search/topics/eBay)

Josh Luber (/search/topics/Josh+Luber)

Yeezy (/search/topics/Yeezy)

Bape (/search/topics/Bape)

Stockx (/search/topics/Stockx)

SHARE THIS ARTICLE

(https://www.facebook.com/sharer/sharer.php?

furl=https%3A%2F%2Fwww.sportswear-international.com%2Fnews%2Fp%2F14099)



(https://twitter.com/share?

url=https%3A%2F%2Fwww.sportswear-international.com%2Fnews%2Fp%2F14099&text=Mark How StockX is revolutionizing the sneaker reseller business online)

DISCUSS ABOUT THIS ARTICLE

Exhibit 3

Detroit startup StockX now worth \$1B: How it got rare status

JC Reindl, Detroit Free Press Published 11:11 a.m. ET June 26, 2019 | Updated 5:33 p.m. ET June 26, 2019

Detroit-based StockX, an online resale marketplace for unworn merchandise — particularly sneakers — has achieved rare "unicorn" status for a Michigan company with a new \$1 billion-plus valuation.

StockX also announced Wednesday that it has hired a former eBay and StubHub executive as its new CEO, replacing hardcore sneaker collector Josh Lubner, who will remain on the three-year-old company's executive leadership team and board of directors.



Calais Sewell, 27, of Detroit prepares authenticated goods for shipping at the new Stock X operations center on Tuesday, July 3, 2018. (Photo: Kimberly P. Mitchell, Detroit Free Press)

More: [Fast-growing Detroit startup StockX sniffs out fake sneakers \(/story/money/business/2018/07/09/detroit-stockx-sniffs-out-fake-sneakers/731070002/\)](https://www.freepress.com/story/money/business/2018/07/09/detroit-stockx-sniffs-out-fake-sneakers/731070002/)

More: [Dan Gilbert's Detroit startup has no profits. But it could be worth \\$1B \(/story/money/business/john-gallagher/2019/04/25/stockx-startup-dan-gilbert-nears-1-b-valuation/3554179002/\)](https://www.freepress.com/story/money/business/john-gallagher/2019/04/25/stockx-startup-dan-gilbert-nears-1-b-valuation/3554179002/)

The company received its \$1 billion-plus valuation through a new \$110 million Series C funding round from investment firms DST Global, General Atlantic and GGV Capital.

StockX calls itself the world's first "stock market of things" and was co-founded in early 2016 by Luber, Detroit businessman Dan Gilbert and the company's now-Chief Operations Officer Greg Schwartz.

Headquartered at One Campus Martius in downtown Detroit, StockX is one of three southeast Michigan-based startup firms in recent years to become a so-called "unicorn." The others firm were Duo Security in Ann Arbor, which sells digital security systems, and OneStream Software, a Rochester-based firm that sells financial management software to major corporations.

StockX said in a news release (<https://www.prnewswire.com/news-releases/detroit-based-stockx-closes-110m-series-c-led-by-dst-global-general-atlantic-and-ggv-capital-names-e-commerce-veteran-scott-cutler-ceo-300875188.html>) that it plans to use the new investment money to fuel its international growth, with a focus on Europe and Asia. It also hopes to have more new products directly released on StockX.

The company says it has more than 800 employees.

StockX gives consumers a platform to buy and sell like-new merchandise in four categories: sneakers, watches, handbags and street wear. Similar to what Kelley Blue Book is for used cars, StockX is now the leading gauge of market value in the sneaker resale world.

The company earns revenue through a flat transaction fee and by taking a percentage of each sale.



The newly named CEO is Scott Cutler, who most recently worked as a senior vice president at eBay and, from 2015 to 2017, was president of StubHub. He previously was an executive vice president at the New York Stock Exchange.

Luber, who owns a personal collection of over 350 pairs of sneakers, founded a Philadelphia-based company called Campless that was a first-of-its-kind price guide for sneakers.

Gilbert purchased that company, bringing Luber to Detroit to help him start StockX.

"Scott and I met just two days after StockX went live," Luber said in a statement. "His extraordinary background — a unique mix of experience working in the stock market, eCommerce, marketplace, retail and resale — mirrors the unique business model we've built here at StockX.

"As a result, Scott understood the power of the 'stock market of things' perhaps more so than any non-founder, and he quickly became a friend and trusted advisor. Over the next three years, as StockX grew, we always had this idea that Scott might one day be the perfect CEO to take us to the next level."

Other high-profile StockX investors include Eminem, Mark Wahlberg, streetwear designer Don C and model Karlie Kloss.

Contact JC Reindlat 313-222-6631 or jcreindl@freepress.com (<mailto:jcreindl@freepress.com>). Follow him on Twitter@[jcreindl](https://twitter.com/jcreindl) (<https://twitter.com/jcreindl>). Read more on [business](https://www.freep.com/business/) (<https://www.freep.com/business/>) and sign up for our [business newsletter](https://profile.freep.com/newsletters/business-headlines/) (<https://profile.freep.com/newsletters/business-headlines/>).

Read or Share this story: <https://www.freep.com/story/money/business/2019/06/26/stockx-valuation-ceo-scott-cutler/1569408001/>

Exhibit 4

Meet the 15-year-old who has made 6 figures reselling sneakers

Shoshy Ciment Aug. 2, 2019, 1:11 PM



StockX is a top sneaker resale marketplace. Matt Marzahl

Exhibit 4



- **Sneaker resale** has never been hotter.

- One 15-year-old, Jake, told Business Insider he has made six figures reselling sneakers. He says many of the sellers he meets are between the ages of 17 and 20.

- The global sneaker resale market could be worth **\$6 billion by 2025**, a recent Cowen & Co. analysis estimated. Sneakers on resale marketplaces like **StockX** and **Stadium Goods** have gone for as high as **\$20,000**.

- Visit **Business Insider's** homepage for more stories.

Forget about a college degree. This teen has made six figures reselling sneakers — and he doesn't even have a high school diploma.

15-year-old Jake, whose last name has been omitted in order to protect his privacy, sells merchandise on the online sneaker resale marketplace StockX. Now a high school sophomore, he started reselling via Instagram when he was in eighth grade. Less than three years later, he says he's made over six figures.

"It's just supply and demand," Jake told Business Insider when asked for his thoughts on the booming sneaker market.

His first turnaround earned him a \$250 profit.

Read more: *These were the most iconic sneakers the year you were born, according to sneaker historians*

"And then I just did that every week and it escalated from there," he said.



Kanye West's Yeezys can go for thousands of dollars on the resale market. Mike Lawrie/Getty Images

In the early days, Jake was selling merchandise via Instagram. He was mostly buying and selling Supreme and Yeezy, Kanye West's collaboration with Adidas. Eventually, Jake got connected with similar entrepreneurs and started selling sneakers through StockX.

During the school year, Jake spends four to five hours a day working on the business, in addition to eight hours of school, plus homework. He quit sports to have more time to work, and he often stays up all night when a new pair drops.

Read more: *These are the 10 best-selling sneakers of the year so far*

But this teen has no regrets. Financial gains aside, Jake has made valuable connections in the growing industry and has picked up some friends along the way as well. Most of the people he works with are between the ages of 17 and 20, he said.

His most expensive shoes sold for \$7,000 — they were the 2011 Nike Mags based on the pair worn by Marty McFly in "Back To the Future Part II." To get them, Jake traded 18 pairs of Yeezys, worth an approximate value of \$3,800.



A new version of the Nike Mag was released in 2016 and included an automatic-lacing feature. Reuters/Danny Moloshok

This year alone, Jake has sold thousands of pairs. He once had a buyer drop nearly \$120,000 with him in one night. However, his personal collection isn't overwhelming, totaling no more than about 15 pairs. Jake prefers to reinvest everything he earns into his business with hopes to gain enough capital to move into the real-estate sector.



The teen might be making bank for now, but to Jake, this whole venture has essentially been a labor of love.

"I really can't describe it," Jake said, referring to the way he feels when he makes a sale or nabs an exclusive drop.

"Everything pays off at that point," he said. "And that's only the beginning."

Exhibit 5

Home Mail News Finance Sports Entertainment Search Mobile More

Search for news, symbols or companies

Sign in



Finance Home Watchlists My Portfolio Screeners Premium Markets Industries Videos

Premium - Try it free

S&P 500

2,927.29

+38.61 (+1.34%)



Dow 30

26,165.15

+279.14 (+1.08%)



Nasdaq

8,018.77

+122.78 (+1.55%)



Russell 2000

1,514.64

+21.00 (+1.41%)



U.S. Markets close in 2 hrs 2 mins

Crude Oil

55.94

+1.07 (+1.95%)



Open an account.
E*TRADE

Because of
where you work

Get up to
\$200 + **\$20**/mo.
via Prepaid Mastercard® Uber credits

Switch now
Restrictions Apply



merican teens are increasingly becoming sneakerheads



Reggie Wade
Writer

Yahoo Finance April 11, 2019

Follow



Quote Lookup

Recently Viewed >

Your list is empty.

EXHIBIT 5

[Sign in](#)[Finance Home](#)[Watchlists](#)[My Portfolio](#)[Screeners](#)[Premium](#) [Markets](#)[Industries](#)[Videos](#)[Premium - Try it free](#)

teens consider themselves sneakerheads (sneaker enthusiasts or collectors). Teens surveyed own eight pairs of sneakers on average, and at least 30% buy a new pair every month.

When it comes to American teens' footwear preference, Nike is GenZ's brand of choice. According to those surveyed, 41% said that Nike was their favorite footwear brand. Vans came in second at 20%, and Adidas came in at No. 3 with 13%. The three brands have taken the top 3 spots since spring 2017 and are the brands of choice for 74% of all teens surveyed.

Nike has also made great strides among teens with its SNKRS mobile app. According to the survey, the average male teen shops on the app 39 times per year, while their female peers shop on the app an average of 19 times a year.

[Gatorade](#)[None of the above](#)**verizon**
media[Next](#)[What to Read Next](#)[3 Marijuana Stocks You Should Buy, According to This 124-Year-Old Wall Street Firm](#)[Motley Fool](#)

[Home](#) [Mail](#) [News](#) [Finance](#) [Sports](#) [Entertainment](#) [Search](#) [Mobile](#) [More](#)[Sign in](#)[Finance Home](#)[Watchlists](#)[My Portfolio](#)[Screeners](#)[Premium](#) [Markets](#)[Industries](#)[Videos](#)[Premium - Try it free](#)

Piper Jaffray analyst Erinn Murphy says Nike is in “a very strong eight-and-a-half year long athletic cycle” in which Nike has risen in popularity among teens and millennials to become top brand across apparel and footwear.

Murphy also points out that the athletic footwear landscape has changed over the last 3 years. “[It’s] gotten a lot cleaner, and it’s not as promotional as it used to be. Sneaker brands like Nike, Jordan and Adidas’s Yeezy have become social currency.”

Better Buy: Aurora Cannabis vs. Cronos Gro

Motley Fool

Piper Jaffray Companies (NYSE:PJC)'s Could Be A Buy For Its Upcoming Dividend

Simply Wall St.

[Home](#) [Mail](#) [News](#) [Finance](#) [Sports](#) [Entertainment](#) [Search](#) [Mobile](#) [More](#)

[Sign in](#)

[Finance Home](#) [Watchlists](#) [My Portfolio](#) [Screeners](#) [Premium](#) [Markets](#) [Industries](#) [Videos](#)
[Premium - Try it free](#)

U.S. teens also have strong preferences when it comes to buying and selling sneakers on the secondary market. Sixty-seven percent of surveyed teens use StockX as their secondary marketplace of choice while 27% prefer to use GOAT Group, which includes [Flight Club](#).

“I think big picture there is a tremendous opportunity,” Murphy said. “Fashion and athletic brands have become a way of life. It is being used not just for sports but everyday wear — 72% of females named an athletic brand as their favorite brand. Going back to our survey 10 years ago, that number was in the low 20% range. The rise of athletic in the primary market shows a long proxy of what the secondary market can do over time.”

Reggie Wade is a writer for Yahoo Finance. Follow him on Twitter at [@ReggieWade](#)

Follow Yahoo Finance on [Twitter](#), [Facebook](#), [Instagram](#), [Flipboard](#), [LinkedIn](#), and [reddit](#).

More from Reggie:

[Nike is trading like Zion Williamson’s shoe never exploded](#)

[In-N-Out Burger is suing Puma](#)

[Foot Locker makes \\$100M bet on popular online sneaker marketplace GOAT](#)

[The top 5 bestselling retro sneakers according to GOAT](#)

Wichita,KS: Notice For Cars Used Less Than Miles A Day

EverQuote Sponsored

The Week Ahead: Nordstrom, Foot Locker Report Earnings + Puma Hits Fifth Avenue

Footwear News

Search for news, symbols or companies

Sign in



Finance Home

Watchlists

My Portfolio

Screeners

Premium

Markets

Industries

Videos

Premium - Try it free

\$ 25,000

Location

Wichita, KS

Account Type

Savings & MM...

Citi - Savings

2.36%\$0

2.36% APY & no minimum deposit. Offer available in select markets.
Rate: 2.33% • Fees: N/A • FDIC Insured

Capital One - 360 Money Market

2.00%\$10,000

One of the Nation's Top Savings Rates - No Fees
Rate: 1.98% • Fees: N/A • FDIC Insured

TIAA Bank - Money Market

2.15%\$1

APY shown is 1-year introductory APY on balances up to \$250k for 1st time Yield Pledge Money Market account holders. \$5k minimum to open

Ad Disclosure

Millions of Americans with employer health c
are still spending a fortune

Yahoo Finance

Stephen Ross isn't Trump's only supporter —
Here are other business leaders who have
backed Trump

Yahoo Finance

[Sign in to post a message.](#)

HURRY UP & SAVE
SALES EVENT



**SOME THINGS ARE
TOO GOOD TO LAST**

*Offer disclosure
2019 F-15
XLT SuperCrew

ESTIM
SA

EARN COMPL
THROUGH

MSRP BEFORE D
CASH BACK + PK
FORD CREDIT BC
NAT. AVG. DEAL

TOTAL EST SAVIN

1

SEA

Your M

Home Mail News Finance Sports Entertainment Search Mobile More

Search for news, symbols or companies

Sign in



Mail

Finance Home Watchlists My Portfolio Screeners Premium Markets Industries Videos

Premium - Try it free

Exhibit 6

The New York Times

Peak Sneaker: Inside Sneaker Con

By Joanna Nikas

Jan. 4, 2018

As a Styles editor, I try to keep up with the latest sneaker drops, but it feels as if I am always playing catch-up.

Sure, trends change in clothing from season to season, but the pace and variety of the sneaker economy is out of the ordinary. And “keeping them fresh” is a large part of keeping up. There seems to be a never-ending barrage of new shoes coming out, and it’s nearly impossible to walk through downtown Manhattan without passing groups of boys lining up to get them.

Yeezy Waverunners! Nike Air Max 97s! OFF-WHITE x Air Jordan 1s! With each drop more pressing than the last, sneaker culture might have hit a peak in 2017.

Sneaker Con, a gathering of shoe fanatics founded by Yu Ming Wu, has been taking place for nine years. This year, the organizers moved it to an expanded space at the Jacob K. Javits Convention Center and expected nearly 20,000 people, a huge increase from the 600 people who attended it the first year. My experience with covering events like this is that, although we can add analysis, reporting and insight into the event, most of the “kids” will follow it on Instagram and YouTube, so by Monday morning, it’s old news. I wanted to find a new way to cover it that helped non sneaker heads, like myself, get a grasp on the culture. So I thought of the idea to solicit the experts for their various sneaker tips. I pitched it to my editor, Chore Sicha, on Slack.

Joanna Nikas 5:31 p.m.: “Story idea headline From the Sneaker Heads at Sneaker Con: Tips on Care, Tricks on Copping and Choosing Their All-Time Favorites.”

Chore Sicha 5:32 p.m.: “omg SOLD.”

EXHIBIT 6

In hindsight, I didn't know what I was in for (it was my first Sneaker Con). I arrived at the convention center around noon on Saturday, the first day of the event, and the line was already two blocks long. I was wearing a pair of Nike Air Max 90 sneakerboots, which didn't seem to impress anyone.

You have 5 free articles remaining.
Subscribe to The Times

In the brightly lit center, there were nearly 500 official vendors set up spanning almost every inch of the 160,000-square-foot partitioned space. But the heart and soul of the event was the trading pit, an area in the back where a vibrant crowd of mostly teenage boys was talking and holding up sneakers, looking for buyers.

"Who is this guy," asked a very confused parent as she pointed to Giancarlo Purchia, known as Blazendary to his 800,000 vlog subscribers. A 17-year-old internet star known for his YouTube commentary on sneakers and streetwear trends, he had set up a step-and-repeat to greet and take photos with his fans. He was wearing a jacket from the coveted Supreme and Louis Vuitton collaboration, a Goyard bag and Nike Mag sneakers, a look that cost over \$60,000, he boasted online.

Across the space, Benjamin Kickz, a 16-year-old reseller to celebrities like DJ Khaled, was giving tips to kids who had gathered around him to take selfies. "You go to events like Sneaker Con and make a bunch of connections, and you just text them," he said. "You say: 'Yo, how much is this? How much is this?' You just eventually get all of it."

As a woman, I stuck out like a sore thumb. The event was very male-focused, so my eye was out for female sneaker heads.

I came across Ariana Peters, a founder of The Chicks With Kicks, which she started with her sisters after her father handed over his 6,000-pair sneaker collection, assembled over more than 25 years. But she was one of the very few. "We have not seen another female-run booth," she said. "So you have to break down that barrier. Even when we started our Instagram account, we got comments saying, 'You are girls, you don't know anything about the sneaker world.' We try to make that a point to show up early and be in the front, since it is a first-come, first-served basis, we don't want to get lost in the crowd."

I had been to vintage conventions and fashion week shows, but even the most hyped events lacked the organic energy of this one. From early 1985 Air Jordans to Converse Chuck Taylors to Adidas Superstars, there is a deep-rooted history embedded in sneaker culture that allows people to connect to excellence and their idols, whether they are sports icons like LeBron James or cultural stars like Kanye West.

So what did I learn?

- 1) Store your sneakers in a dark space, because light can cause yellowing, which devalues your shoes.
- 2) Become friends with people who work at sneaker shops.
- 3) Always check details like font and stitching when verifying real versus fake sneakers.
- 4) Ask your elders for their old clothes and sneakers. Chances are they will eventually come back in style.
- 5) Wash your insoles for, well, obvious reasons.

A version of this article appears in print on Jan. 3, 2018, Section A, Page 2 of the New York edition with the headline: Inside the Sneaker World

Exhibit 7

[PARENTS](#)

Sneakers: Heart and sole to teen boys

April 7, 2010, 10:34 AM CDT / Source: The Associated Press

What Imelda Marcos did with shoes, teenage boys do with sneakers.

They hoard them and display them. They have sneakers for every occasion. They buy them when they don't need them, hold on to them after outgrowing them, and even save the boxes.

As an outsider to this culture of sneaker obsession, I've made some dreadful mistakes.

I've been yelled at for throwing away old sneakers with holes in them, not realizing they were collectibles. I've packed cupcakes for bake sales in sneaker boxes with plastic see-through tops, not realizing I had sullied a display case.

And I've been mocked for owning just one pair of nondescript sneakers myself, proudly purchased for \$29 at an outlet store back in 2001 and still worn, much to the embarrassment of my offspring.

In contrast to my lonely set of sneaks, my 12-year-old's collection includes five pair, each with a different purpose. He has red sneakers with black stripes for playing basketball indoors. Black sneakers with yellow stripes for playing basketball outside. High-tops with thick soles to wear in the rain, a beat-up pair of Nikes for every day to school, and pristine white Jordans for weddings and bar mitzvahs. (I have to admit, they look darn cute with a pinstriped suit.)

Yvette Quiazon, an ethnographer who has studied sneaker culture for companies like Nike and Adidas, wasn't surprised to hear that my son has dress-up sneakers. After all, she said, celebrities wear sneakers with suits to awards shows.

"It trickled down from celebrities and made a suit look cool," she said. "I don't think they'll stop wanting to wear the sneakers with the suits. I see that going into adulthood. Sneakers are shoes to them."

While I've grudgingly accepted kids wearing sneakers to formal occasions, I still have a hard time with sneaker prices. When my 12-year-old and his big brother were small, I got away with the cheapest sneakers I could find – two pair for \$20 at the discount store.

EXHIBIT 7

But that ended when my older son got to middle school. He told me that having cool sneakers was a safety issue: He'd get beat up if he looked like a dork.

And here I had been under the impression that cool sneakers make you a target for thieves!

I slowly came to understand that cool sneakers get you off the hit list, not on it. But I still didn't want to pay for them. Eventually I put the kids on a sneaker budget, and that has worked well in our family.

I pitch in what I deem a reasonable sum – say \$50, twice a year. If they want to spend more than that, they use their allowance or money they've earned, or they trade in the right to all other birthday presents in order to obtain the sneakers of their dreams.

Dan Cherry, who heads the Converse sneaker account at the New York ad agency Anomaly and in the past has also worked on campaigns for Jordan and Nike, says "today's kids are experts in sneaker culture."

He added that "sneaker heritage" dates back decades with iconic brands named for basketball legends like Chuck Taylor and Michael Jordan. Kids way too young to have seen these athletes play know the brands and their stories.

Cherry understood why I was scolded for throwing away old sneakers. "If you had a vintage dress, you'd scream if your boyfriend or husband threw it out," he said.

And he explained why my son was upset when I packed cupcakes in a sneaker box: "That box was an authentic part of an heirloom sneaker collection."

While sneaker culture started with basketball stars, it also has roots in the skateboard world, hip-hop and rock culture. Not only can every kid find a style to relate to, but over time, says Quiazon, the ethnographer, the styles have blended.

Quiazon is hired by companies to go into homes and kids' closets to see what they own and wear. Tweens and teens she's interviewed own an average of five to 10 pairs of sneakers, but she said the recession has slowed the trend, with kids "simplifying" their collections rather than adding to them.

"The idea is to understand an average teen who uses their product," she said. "I'll take pictures, I'll ask a ton of questions – who you are as a kid, what's important to you. Describe yourself. Pull out outfits for me. Say you're going out Saturday with your friends. What are you doing, what are you wearing and why."

Quiazon says it's not unusual for kids to decide what sneakers they are wearing that day, and then "build the outfit from the sneaker going upwards."



 [22 photos](#)



Slideshow

The American teen

From a California punk to a drag queen in Georgia, photojournalist Robin Bowman captures the passion, pride and conflict of a young generation coming of age.

Being trendy is important, of course, with moms telling Quiazon they sometimes postpone back-to-school shopping until after school starts so their kids can figure out what's hot before buying. But Quiazon says kids also want to be unique.

That may be one reason customization is so popular, with teens buying made-to-order sneakers online for \$100 or so. They can choose colors, patterns and fabric, and can even print a name or slogan on the back.

Also notable in the world of sneaker obsessions: limited edition releases, reissues of classic models, used sneaker and sneaker-swap stores and sites like FlightClubNY.com, and boutiques where sneakers are put on a pedestal and presented "in a way that is beautiful, like a Manolo Blahnik shoe," as Quiazon put it.

Cherry said sneaker collectors are no different from people who collect wine, classic cars or vintage fashion. Some adult connoisseurs have vintage sneaker collections worth hundreds, even thousands, of dollars, he said.

Cherry was also able to explain one other incident that had puzzled me. Recently, my son was invited to a birthday party. Instead of giving the usual gift card to our local video game store, my son and a few other kids chipped in \$20 apiece, asked the birthday boy his shoe size, and bought him a carefully chosen pair of sneakers.

Cherry assured me this made perfect sense in the universe of sneaker collecting: "It's like buying the right bottle of wine for a dinner party."

[ABOUT](#)[CAREERS](#)[ADCHOICES](#)[VISIT](#)[PRIVACY POLICY](#)[TODAY STORE](#)[TERMS OF SERVICE](#)[TODAY APPS](#)[CLOSED CAPTIONING](#)[COUPONS](#)[SITEMAP](#)[CONTACT](#)[ADVERTISE](#)



Exhibit 8

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/stockx-hub-for-sneakerheads-is-latest-1-billion-unicorn-11561571959>

BUSINESS

StockX, Hub for Sneakerheads, Is Latest \$1 Billion Unicorn

Online marketplace lets people trade shoes like stocks, riding boom in teen selling



Antonio Gray looks over a pair of Jordans sneakers at StockX's authentication center in Detroit. The company is on the path to sell merchandise valued at more than \$1 billion this year. PHOTO: KIMBERLY P. MITCHELL/DETROIT FREE PRESS/ASSOCIATED PRESS

By Khadeeja Safdar

Updated June 26, 2019 3:04 pm ET

StockX, an online marketplace that lets individuals trade sneakers like stocks, closed a round of venture funding that valued the startup at more than \$1 billion, riding the sneaker-reselling craze fueled by teens.

Founded in 2016, the Detroit company started as a website for sneakerheads, or sneaker fanatics who buy and sell rare shoe models.

It has now evolved into a broader marketplace for streetwear, handbags, watches and other goods and is on the path to sell merchandise valued at more than \$1 billion this year.

StockX said Wednesday it closed on a \$110 million funding round from DST Global, General Atlantic and GGV Capital.

Sneakers have emerged as an alternative asset class among young shoppers, who collect rare shoe models and sell them for higher prices online.

The resale market for sneakers and streetwear is more than \$2 billion in North America and growing by more than 10% annually, according to Cowen, an investment bank. StockX said it has the potential to reach more than \$6 billion in sales by 2025.

In the past year, investments have flowed into sneaker-reselling sites and shops.

In February, Foot Locker Inc. said it was investing \$100 million in Goat Group, an online reselling platform for sneakers.

In December, Farfetch Ltd. , a luxury-fashion site, said it was acquiring Stadium Goods, a sneaker-reselling store, for \$250 million.

Some streetwear and rare sneaker models are commanding higher price tags than products from storied luxury brands. A Supreme hoodie, which retailed for \$168, was last sold on StockX for \$678. A pair of Nike Pigeon Dunks, which once had a retail price of \$200, were last sold for \$12,000.

Part of what is fueling the resale economy is that shoppers no longer attach a stigma to preowned goods the way they used to.

The RealReal Inc., a marketplace for preowned luxury goods, has filed to go public this week and is seeking a valuation of \$1.5 billion.

Poshmark, a fashion resale marketplace, is also preparing to debut in the public markets as soon as this fall, The Wall Street Journal has reported.

On StockX, buyers make an offer that any seller can accept. Sellers can either list items at their own price and wait until a buyer accepts it or sell their merchandise to the highest bidder. They ship the goods to StockX, which authenticates the products before shipping them to the seller.

Like a stock exchange, the website displays pricing information such as the 52-week high of an item and the volatility.

Like eBay Inc. or other marketplaces, StockX charges sellers fees. It collects a 3% processing fee, as well as transaction fees that range from 8% to 9.5% for sneakers and streetwear. Its fees for watches and handbags are higher.

The startup also said it was bringing on a new chief executive, Scott Cutler, a former executive at eBay and the New York Stock Exchange.

The company's co-founder, Josh Lubner, will step aside as CEO but continue to serve on the executive-leadership team and board of directors.

Write to Khadeeja Safdar at khadeeja.safdar@wsj.com

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

Exhibit 9

A giant new investment will make StockX the first billion-dollar sneaker reseller

DST, the venture capital firm founded by Yuri Milner, is expected to lead the deal.

By **Theodore Schleifer** and **Jason Del Rey** | Apr 19, 2019, 6:45am EDT



The Nike Air Yeezy 2 “Red October” sneaker. | Mike Lawrie/Getty Images

The online sneaker resale marketplace StockX is in advanced talks to be valued at at least \$1 billion in a new round of financing, **Recode** has learned.

DST Global, the late-stage venture firm run by Russian-American billionaire Yuri Milner, is expected to lead the deal, according to people familiar with the matter. It will be the latest bet by the firm on an e-commerce startup after backing companies like DoorDash, Wish, and Faire.

The exact size of the financing round couldn't be learned. Another expected participant is GGV Capital, the venture firm famous for investing in both the US and China, according to the people. StockX is planning to make some other major company announcements when it unveils the fundraising round, which is likely to be closed in the next few weeks.

StockX, DST, and GGV all declined to comment.

StockX launched in 2016 and was founded by Dan Gilbert, the billionaire owner of the Cleveland Cavaliers, COO Greg Schwartz and CEO Josh Luber, who previously ran Campless, a site that eventually became StockX and displayed data about hard-to-find sneakers.

StockX plays matchmaker for sneakerheads looking for rare kicks and resellers looking to flip unworn, in-demand sneakers for a profit. Sellers ship their goods to StockX facilities where employees authenticate that the sneakers are genuine before shipping them out to a buyer.

StockX, which is not profitable, charges a minimum \$5 selling fee, plus as much as 12.5 percent in transaction and payments fees. Luber told the New York Times a year ago that StockX generated about \$2 million in gross sales every day. The company has 700 employees.

The Detroit-based company gets its name from its stock market-like pricing structure, which lets shoppers either pay the lowest asking price from one of StockX's sellers or place an even lower bid and see if it eventually matches up with

a seller's asking price. StockX also makes the pricing history of a given sneaker transparent, which is one reason it bills itself as a next-generation eBay. While sneakers are StockX's sweet spot, the site also sells watches, handbags, and streetwear through the same model.

Like competitors GOAT and Stadium Goods, StockX has benefited from the rising popularity of acquiring tough-to-buy sneakers, especially among millennial men and teenage boys.

And the valuations of the companies in the space show it. The luxury e-commerce website Farfetch paid around \$250 million to acquire Stadium Goods, which uses a consignment model, last year. And GOAT, which also owns the boutique sneaker store chain Flight Club, was valued at more than \$550 million when Foot Locker invested \$100 million in the company earlier this year.

Because of its real-time pricing model, StockX is often able to offer slightly cheaper prices, But StockX's success and billion-dollar valuation are predicated on these high-end sneakers remaining fashionable or collectors' items — and that's no guarantee.

Previously, StockX has been financially backed by Gilbert, as well as Battery Ventures and GV, Alphabet's early-stage arm.



Recode Daily

Email (required)

By signing up, you agree to our [Privacy Policy](#) and European users agree to the data transfer policy.

SUBSCRIBE

This article originally appeared on Recode.net.

Exhibit 10

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/this-website-is-the-stock-market-for-nikes-and-rolaxes-1543251772>

ON TREND

This Website Is the Stock Market for Nikes and Rolexes

StockX, a Dan Gilbert backed start-up has revolutionized the secondary market for sneakers, streetwear, handbags and watches. With a new London office, it has its sights set on global expansion



Mitch Blunt ILLUSTRATION: MITCH BLUNT



By
Jacob

Gallagher

Nov. 26, 2018 12:02 pm ET

It was Tuesday, Nov. 13, 2018. Though Josh Luber would rather it didn't, in three days, Adidas was planning to re-release the Yeezy Boost 350 V2 "Zebra," a black-and-white striped version of its Kanye-West-designed sneaker. Mr. Luber, co-founder of StockX, an online trading platform for sneakers, streetwear, handbags and watches, hates when companies disrupt his market strategy. "The one thing that breaks the supply-and-demand model and the purity of it in the secondary market is when brands artificially f--- with it when they restock stuff," said Mr. Luber, a scruffy 40-year-old who wore a hoodie throughout our interview. Within a week, his hypothesis was confirmed: Yeezy Zebras were trading for about \$270 on StockX, just \$50 above retail and well below their peak of \$2,000.

Tracking sneaker values has long been Mr. Luber's obsession. In the late 2000s, he was a strategy analyst at IBM in New York who spent his nights trawling eBay for data on how much sought-after shoes were selling for on the secondary market. He compiled those figures into Campless, a sort of Kelly Blue Book for sneaker-resale value. But Mr. Luber wasn't satisfied with eBay. His beefs weren't limited to the bad photos that sellers posted or their habit of selling fakes. What really bugged him was the absence of price standardization. One dealer might peddle a pair of Nike Dunks for \$100 and another might list the same shoes for \$300. Mr. Luber envisioned a more orderly market, with a New York Stock Exchange-style ticker, that would make the value of a pair of sneakers transparent, in real time. When those Dunks sold for \$100, everyone on the market would know about it, thus forcing other sellers to knock their prices down to the going rate.

Around that same time, Dan Gilbert, the founder of mortgage lending company Quicken Loans, noticed that his teenage son was flipping sneakers on eBay for profit. Intrigued, Mr. Gilbert founded a research team on sneaker reselling who discovered what Mr. Luber was working on. Mr. Gilbert bought Campless in 2015 and the pair joined forces (along with COO Greg Schwartz), launching StockX, "the stock market of things," based in Mr. Gilbert's hometown of Detroit in February 2016.



The sprawling, sneaker-filled StockX offices in Detroit. PHOTO: STOCKX

Today, StockX employs nearly 550 people worldwide, and has added watches, handbags and streetwear (including widely hyped hoodies, T-shirts and even skateboards from brands like Fear of God, Off-White and Bathing Ape) to its marketplace. Mr. Luber explained that StockX only deals in rarefied products that balance liquidity and scarcity. A J. Crew gingham shirt will never be on StockX because it's too common, nor will a

Picasso painting, because it's too rare. A variety of Nike Air Jordans of which only 1,000 pairs may exist is ripe for StockX's marketplace.

Because of these items' scarcity, fakes remain a major issue on the resale market. StockX only accepts new merchandise and employs over 100 authenticators to identify counterfeits. "When we started the business three years ago, we couldn't go to LinkedIn and find sneaker authenticators," said Mr. Luber. "We basically created that career." It takes about 90 days to train authenticators who use scales, durometers (to measure density) and apps to spot fakes.

Korre Jefferson, 20, a retail associate in Brooklyn, N.Y., said he liked knowing that someone had validated the authenticity of the sweater and pair of sneakers he purchased on StockX this year: “Sometimes on [resale marketplace] Grailed you might have someone selling something that’s clearly fake, so it’s nice to have that security with StockX.” Over email, Grailed co-founder Jake Metzger explained, “We have a team of experienced moderators combing the site every day looking for suspicious users and listings. Any user caught actively selling fake merchandise is banned from the platform.”

When a transaction is “completed” on StockX’s website, that’s really only the beginning. The seller then sends the shoes to one of StockX’s four authentication centers (Detroit, Tempe, Ariz., Moonachie, N.J. and the latest outpost in London), where they are authenticated and shipped out to the buyer. If all goes to plan, the turnaround at the authentication center takes less than a day.



An employee at StockX inspects a pair of Nikes for authenticity. PHOTO: STOCKX

Further mitigating risk for the buyer, StockX acts as a middleman for payment and does not release proceeds of the sale to the seller until the shoes have been verified. Carlos Chavez, 34, an engineer and part-time sneaker seller in Los Angeles, prefers using StockX (or GOAT, a rival app) to eBay, after he experienced a “chargeback,” in which PayPal froze his proceeds of a sale for two weeks because the buyer

used a counterfeit payment.

“I’ve sold on both eBay and Grailed but the big reason I prefer StockX for shoes is to not be scammed,” said Mr. Chavez, who in September used his funds from flipping sneakers to finance a vacation to Oaxaca with his wife. In a statement, an eBay spokesperson noted that it offers a money-back guarantee if a buyer identifies a counterfeit and that since 1998 it has had the Verified Rights Owner Program (VeRO), which allows brands themselves to more easily report fake items on eBay. Further, in October 2017 eBay launched “eBay Authenticate” which inspects and validates luxury items such as Prada handbags and Rolex watches.

For its part, StockX takes a cut of every sale: 9.5% on sneakers and streetwear, 9.9% on any watch sale and 14.5% for any handbag sale. The vast majority of transactions involve sneakers

or streetwear, with items from the highly sought-after brand Supreme comprising about 85% of StockX's clothing sales.

Though expansion across all four categories is important, Mr. Luber stressed that StockX's future success really lies in expanding the sneaker-buying market. His target buyer, he said, is "that guy who bought his last pair of shoes at Foot Locker or Nike.com, and never in a million years would've tried to wade through eBay to buy a pair of Jordans or Yeezys." By Mr. Luber's estimation, the United States sneaker resale market is currently a \$2 billion industry, while the primary sneaker market is at \$19.6 billion according to the market analysts at NPD Group. If StockX can convert a sliver of those primary market customers, the website's profits could be significant.

The aim is not to turn novices into sneakerheads willing to pay 11 times the retail cost for a pair of Nike's Off-White Air Jordans. Rather Mr. Luber would like to create a destination for sneaker buyers of every ilk. He noted that a lot of items on StockX do sell for less than their sticker price: "Sometimes it's just access. It's a general-release shoe from three years ago, but it's just not available on Nike.com so now you can get it on StockX."

In further attempts to expand its reach, last month StockX opened an office in London and has its sights set on China. There are regional differences here and there—fewer basketball sneakers in Europe, more Nike Air Force Ones in New York—but by and large, users want the same sneakers and clothes whether they're in Brussels or Brooklyn. Often these days, that means Yeezys, Off-White Nikes and Supreme.

For Lucio Nunes, 20, a student in Switzerland who has sold shoes on StockX for two years, using the London office has improved his selling experience. Shipping rates are cheaper, as he no longer has to send his shoes further abroad, and his money clears faster. Still he said, the one downside to StockX is that it has lowered prices throughout the sneaker flipping-world. "The prices are much more visible because everyone looks at StockX and takes it as the market price," said Mr. Nunes. It's harder to cheat the market when the ticker price is just a click away.

Corrections & Amplifications

An earlier version of this article incorrectly stated that StockX took 14.5% of the proceeds of any watch sale. It takes 9.9% of any watch sale. (Nov. 26, 2018)

Write to Jacob Gallagher at Jacob.Gallagher@wsj.com

MORE IN STYLE & FASHION

- 'Just How Important Is a Presidential Candidate's Hair? August 12, 2019
- 'Finger-Toe Shoes: Strange, Yet Beloved By Many August 5, 2019
- 'Does Anyone Really Need a \$5,000 Vape Case? Apparently, Yes July 31, 2019
- 'Is the Souvenir Cap the Ultimate Humblebrag? July 24, 2019
- 'Are K-Pop Stars the World's Biggest 'Influencers'? July 15, 2019

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

Exhibit 11

Why Cavs Owner Dan Gilbert Is Investing in Sneaker Resellers

The billionaire explains his plans for StockX.

BY SOLE COLLECTOR (/AUTHOR/SOLE-COLLECTOR)

🕒 FEB 8, 2016

(https://
/about.
compl

STYLE

FOLLOW SOLE COLLECTOR (HTTP://TW

LIKE SOLE COLLECTOR (HTTP://FACEB

EXHIBIT 11



(//images.solecollector.com/complex/image/upload/jxr2xmtlirivx3bbl33w.jpg)

via StockX (<https://stockx.com/>)

by Pete Forester

(<https://about.compl>) The future of sneaker reselling is happening right now.

STYLE

FOLLOW SOLE COLLECTOR ([HTTP://T](http://t))

LIKE SOLE COLLECTOR ([HTTP://FACEB](http://faceb))

ex.co
m)

After founding **Campless** (<https://solecollector.com/focus/campless/>), a site that monitors the buying and reselling of sneakers on eBay, **Josh Luber** started to get a ton of attention in the sneaker industry. The exhaustive tracking of sneaker sales caught the attention of sneakerheads and anyone with a vested interest in flipping sneakers, but Luber had a bigger plan.

His idea wasn't a store. It wasn't an auction platform. It was something entirely new. The problem was that no one was interested in it.

Enter Dan Gilbert.

The billionaire investor and owner of the Cleveland Cavaliers was watching his sons buy and sell sneakers through eBay and he wondered if there was anything to it.

"The amount of interest and activity among my boys and their friends about sneakers was just crazy," Gilbert said. "Then I start asking other people that have teenage boys, and it's almost 90-95 percent of the people that I asked said the same thing."

It was Gilbert's first window into sneaker reselling that would end up planting a seed in his mind. He saw problems within the culture. Transactions were murky, information was limited, and it was based on trusting strangers with your money. But he also saw an opportunity.

"I've just always wondered why a stock market of things had not emerged yet on the Internet. You always had a great case for a stock market," Gilbert said. "It's worked beautifully for the last 200 years in this country, if not longer, and the Internet is a vehicle that takes it to a level where anything can be done that way."

(<https://solecollector.com/news/2016/02/campless-stockx-dan-gilbert>)

STYLE

FOLLOW SOLE COLLECTOR ([HTTP://TWITTER.COM/SOLECOLLECTOR](http://twitter.com/solecollector))LIKE SOLE COLLECTOR ([HTTP://FACEBOOK.COM/SOLECOLLECTOR](http://facebook.com/solecollector))

MOST POPULAR[®]

VIEW MORE

MARKET MOVERS[®]

VIEW MORE



LATEST NEWS

CONFESSIONS OF AN UNLIKELY RESELLER
(EP. 2) - PROFESSOR JEN
CAMPLESS - JANUARY 5, 2016

THIS IS WHAT HYPE LOOKS LIKE
CAMPLESS - DECEMBER 31, 2015

THIS IS WHAT \$278K OF FAKE SNEAKERS
LOOKS LIKE
CAMPLESS - DECEMBER 31, 2015

SNEAKER PORTFOLIOS EP1: MARK
WAHLBERG \$100K
CAMPLESS - NOVEMBER 24, 2015

CONFESSIONS OF A NYC RESELLER
CAMPLESS - OCTOBER 27, 2015

ISO RELEASE CALENDAR (INITIAL SNEAKER OFFERING)[®]

JAN 14 NIKE AIR PRESSURE RETRO WHITE CEMENT BID	JAN 15 ZOOM KOBE ICON METALLIC GOLD BID	JAN 15 CURRY 2 HAIGHT STREET BID
JAN 16 JORDAN 4 RETRO DENIM (GS) BID	JAN 16 JORDAN 1 RETRO BHM 2016 (GS) BID	JAN 16 JORDAN HORIZON BHM (2016) BID

FOLLOW SOLE COLLECTOR (HTTP://TWITTER.COM/SOLECOLLECTOR) LIKE SOLE COLLECTOR (HTTP://FACEBOOK.COM/SOLECOLLECTOR)

KAWS \$910 ▼ AFI-3MSNK \$250 ▲ AFI-BOBPIL \$200 ▲ AFI-CROCLUX \$1,000 ▲ AFI-DJCKBF \$158 ▲ AFI-FLX14 \$295 ▼

(https://
about.

compl (//images.solecollector.com/complex/image/upload/dolmambegisppqnfhksw.jpg)

ex.co
m)

As Luber was turning down partnerships that offered directions counter to his own, Gilbert was looking for someone to help make the idea a reality. When Gilbert found Luber they talked about the million dollar idea: a stock market for sneakers.

Luber's work at Campless gave them the data they needed, Gilbert's passion for building companies offered the resources and their combined passion for commerce offered the energetic sustenance a project like this would demand. Everything clicked and in the middle of 2015, Luber moved his family to Detroit, where Gilbert's based. **StockX** (<https://stockx.com/>) was born.

The easiest way to describe StockX is how its founders do: "The stock market of things." The actual stock market is a peer-to-peer marketplace where assets are sold, as slices of ownership in a company.

What the stock market offers is a marketplace for this commerce to happen. The stock market doesn't sell you stock, it just offers a place to buy and sell them. Whenever you're considering a stock, you can find the full history of stocks from first purchase to the most recent. This ensures that a buyer is fully educated on what they're getting into and the seller knows what to reasonably ask for.

StockX offers the same thing, but for sneakers.

We know from watching Campless develop over the last four years that they've been able to take eBay data to make histories on the value of a sneaker. This information is powerful for both buyers and sellers because information creates an arena where everything is fair. It makes it much harder for anyone to be taken advantage of.

"Imagine selling stocks like the secondary market for sneakers. One guy on one corner would be selling a share of Google for \$180 and another guy on the next corner is selling it for \$400," explains Gilbert. "Nobody would really know or feel good because you just don't have the last comps and the last sales."

([https://
about.
compl](https://about.compl)

STYLE

FOLLOW SOLE COLLECTOR ([HTTP://TW](http://twitter.com/solecollector)

LIKE SOLE COLLECTOR ([HTTP://FACEB](http://facebook.com/solecollector)

ex.co
m)

The current system of auctions and Twitter sales offers something of a perfect storm of problems. First, you have to deal with buyers and sellers essentially face to face. Even if you're not looking at the other person in the transaction, you're interfacing with them directly, getting money from them directly, and sending product to them directly.

"When you buy a share of Apple stock from the New York Stock Exchange, there's an actual seller on the other end of that specific trade, but you'll never know who that is and you don't care who that is," explains Luber. "All you care about is the price you got the stock for, and you know it's authentic because it's from the New York Stock Exchange. We set up the same construct here."

(https://
/about.
compl

STYLE

FOLLOW SOLE COLLECTOR (HTTP://T)

LIKE SOLE COLLECTOR (HTTP://FACEB)

Search for brand, size, color, etc.

PRICE GUIDEMY ACCOUNTANALYSISFAQSELL

HOMEBROWSEAIR JORDANAIR JORDAN 1

JORDAN 1 RETRO SHATTERED BACKBOARD

SNEAKERHEAD SIGNIFICANCE: 84TICKER: AJ1-SBBCONDITION: DEADSTOCK

SIZE

MULT

LAST SALE\$435-\$15 (-3%)
SIZE: 10.5
VIEW ALL SALES

LOWEST ASK\$400


BID

VIEW ALL ASKS

HIGHEST BID\$370

SELL

VIEW ALL BIDS



STYLE: 555088-005COLORWAY: BLACK/STARFISH-SRELEASE DATE: 06.27.15ORIGINAL RETAIL PRICE: \$160

52 WEEK HIGH/LOW\$600\$299DEADSTOCK RANGE (12 MOS.)\$412 - \$458VOLATILITY 5.2%

LATEST SALES OF JORDAN 1 RETRO SHATTERED BACKBOARD

SIZE	SALE PRICE	DATE	TIME
10.5	\$435	Thursday, January 14, 2016	8:35 am EST
10	\$450	Thursday, January 14, 2016	8:35 am EST
10.5	\$450	Wednesday, January 13, 2016	8:08 am EST
10.5	\$400	Tuesday, January 12, 2016	12:08 pm EST
10	\$450	Monday, January 11, 2016	12:07 pm EST

VIEW ALL SALES


Zoom

Jan 2, 2016

Jan 14, 2016

From

To




12 MONTH HISTORICAL

DEADSTOCK SOLD 207


PRICE PREMIUM (OVER ORIGINAL RETAIL PRICE) 171.9%

AVERAGE DEADSTOCK PRICE \$427


RELATED PRODUCTS




JORDAN 1 RETRO BRED (1994)
\$999
LAST SALE: --




JORDAN 1 RETRO CARMINE (2014)
\$175
LAST SALE: \$240



JORDAN 1 RETRO CHICAGO BULLS
\$375
LAST SALE: \$375



JORDAN 1 PT5 RETRO CHICAGO (2015)
\$145
LAST SALE: \$160



JORDAN 1 RETRO BLAKE GRIFFIN PE
\$109
LAST SALE: \$135

(https://
/about.
compl

STYLE

FOLLOW SOLE COLLECTOR (HTTP://T

LIKE SOLE COLLECTOR (HTTP://FACEB

https://solecollector.com/news/2016/02/campless-stockx-dan-gilbert

7/19



(//images.solecollector.com/complex/image/upload/hyrjsd1u0jzmcqwkbkgm.jpg)

So how does it work?

If you were looking for a pair of "Bred" Air Jordan 1s on eBay, you'd type that in and get dozens of results. Each auction would have its own photos, description and variables. And with each of those listings comes a seller who you don't know and you can't vet.

On StockX there's one page for all "Bred" Jordan 1s. There's one page per product, and no uploading photos. On that page you can find the full sales history data from Campless on the shoe with a market price, provided by Campless and StockX history. On a drop-down menu you choose the size and you're brought to a page with every pair that's available and each of their prices, and you can compare to the market price. If you click "buy," the seller sends the shoes to StockX who authenticates them, and then you get your shoes. If you don't like any of those prices you can submit a bid that remains live until a seller decides they like your price and accepts it. There are no legit checks, there's no dealing with unknown sellers, there's no wondering about pricing.

If StockX gets the shoe and finds it's not authentic, they will send the shoes back to the seller, penalize them financially and do what they can to work with their other sellers to find the same pair of shoes for the same price (as long as the price was within reason). If they can't find anything, they'll refund you with their apologies.

Not everyone is going to understand the breadth of StockX until they get their hands on it. DJ Skee was one of those people.

"I was skeptical because there are so many different things in the marketplace and there's so much noise out there and a lot of people are trying to solve this problem. Now it seems like everybody has their own sneaker consignment store,"

(https://
about.
compl

Skee said.

STYLE

FOLLOW SOLE COLLECTOR (HTTP://T)

LIKE SOLE COLLECTOR (HTTP://FACEB)

ex.co
m)

If you're like Skee and have a lot of social influence, you'd think that discretion is key, but for him there are more crucial issues that StockX is solving.

"The biggest challenge with anything in the community is fraud and fakes," Skee explains. "As well as people trying to con other people over and get cash, and with what [StockX has] in place it's probably one of the most secure ways to buy things because the second you lose that layer of security or trust that will kill any brand... They kind of realize that and have taken a lot of steps to position themselves in the proper manner."

This system is set up so that any interest level can make use of it. Whether you have a ton of volume and want to become something of a day trader in sneakers (something that Gilbert says they're anticipating), or just need to cop a pair of Jordan 11s for your buddy's birthday, you can dive as deep as you want.

Gilbert has a history of investing in projects like StockX. He built his empire with Quicken Loans, which just launched Rocket Mortgage, another financial platform that connects homebuyers with banks who are looking to invest in each other. Rocket Mortgage doesn't create their own deliverable; instead they're the liaison between the two parties. StockX is the same.

"We're the bridge that you drive over. We're the bridge. We're not the destination," explains Gilbert.

StockX connects buyers and sellers directly, allowing the product's life to extend beyond the retail experience, while having the same dependable platform. And its potential reaches much farther than sneakers. Handbags, watches and cars were all items that Gilbert mused about possibly putting on the platform.

"That might work," he said. "The possibilities are nearly endless."

SHARE

TWEET

(https://
about.
compl

STYLE

FOLLOW SOLE COLLECTOR (HTTP://T)

LIKE SOLE COLLECTOR (HTTP://FACEB)

ex.co

m)


TAGS • DAN GILBERT (/TAG/DAN-GILBERT)

POPULAR IN THE COMMUNITY




Sponsored

Sneakersnstuff Made New Balances for 'Grown Ups'

 **CyanRadio**
4d


If y'all think New Balance is ugly you don't have good taste. Period. This colorway is very...

A Pair of Zion Williamson's Sneakers Just Sold For...


 **PurplePumpkin**
5d

If he pans out, great investment. If he doesn't make the playoffs at all during his first contract o...

Maharis for Its N

 **Gi**
3d

These are argue the



(https://dynamic-cdn.spot.im/yad/optout.html)


CONVERSATION

Have a Disqus Account?  **Log In**

Be the first to comment...


[Terms](#) · [Privacy](#) Add Spot.IM to your site

LATEST NEWS

**Pharrell's NMD Hu Returns in Four New Colorways With Gum Bottoms (/news/2019/08/pharrel...**BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO)  1 HOUR AGO

(https://solecollector.com/news/2019/08/pharrell-hu-nmd-returns-in-four-new-colorways-with-gum-bottoms)

compl

**Tyga's Sneaker Collection Is Worth Over \$100,000 (/news/2019/08/tyga-complex-...**BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO)  1 HOUR AGO

The multi-platinum rapper is the latest guest on 'Complex Closets.'

**Best Look Yet at the 'Knicks' Air Jordan 3 (/news/2019/08/air-jordan-3-iii-knicks-release-date-...**

BY BRANDON RICHARD (/AUTHOR/BRANDON-RICHARD)

ex.co

m) (/news/2019/08/nike-shox-bb4-toronto-raptors-white-cd9335-100)



Nike Pays Homage to Vince Carter with Toronto Raptors-Inspired Shox BB4...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) ☺ 20 HOURS AGO

Celebrating the early years of Vinsanity.



'Lucky Green' Air Jordan 13 Rumored For July 2020 (/news/2019/08/air-jordan-13-xiii...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) ☺ AUG 18, 2019

Early release details.



These Nike PG 3s Are Perfect for the Entire Team (/news/2019/08/nike-pg-3-team-...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) ☺ AUG 17, 2019

Just in time for the new season.



Kevin Garnett's Nike Air Flightposite 2 Is Returning Soon (/news/2019/08/nike-air-...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) ☺ AUG 17, 2019

(https://www.solecollector.com/news/2016/02/campless-stockx-dan-gilbert) Early details on the Big Ticker's Olympic sneaker retro. compl



Undeclared x Nike Zoom Kobe 4 Protro Pack Releasing on Mamba Day (/news/2019/08/undeclared-...

BY BRANDON RICHARD (/AUTHOR/BRANDON-RICHARD) ☺ AUG 17, 2019

Four colorways featuring both of Kobe Bryant's jersey numbers.

ex.co

m)



Nike Extends Protection for Pregnant Female Athletes (/news/2019/08/nike-extends-...

BY JORDAN ROSE (/AUTHOR/J-ROSE)
🕒 AUG 16, 2019

Following backlash over the summer.



First Look at Kyrie Irving's Next Signature Sneaker (/news/2019/08/nike-kyrie-6-bla...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) 🕒 AUG 16, 2019

Nike Kyrie 6 coming soon.



Nike Is Adding Realtree Camo to the Air Max 1 Golf Shoe (/news/2019/08/nike-air-max-1-...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) 🕒 AUG 16, 2019

New colorway of the hybrid shoe will release next week.



Travis Scott Debuts Never-Before-Seen Air Jordan 6 Collab (/news/2019/08/travis-scott-...

BY RILEY JONES (/AUTHOR/RILEY-JONES)
🕒 AUG 16, 2019

The 'Cactus Jack' collabs keep coming.



Detailed Look at the 'Vast Grey' Nike Kobe AD NXT (/news/2019/08/nike-kobe-ad-nx...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) 🕒 AUG 16, 2019

New colorway releasing on Kobe Bryant Day.



Levi's Is Rumored to Get an Air Jordan 6 Collab (/news/2019/08/air-jordan-6-vi-...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) 🕒 AUG 16, 2019

Next denim Retro expected in 2020.

CLOSE



New Kyrie 5 Tennis Sneakers Are Releasing This Month (/news/2019/08/nikecourt-air-...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) © AUG 16, 2019

Ahead of the 2019 U.S. Open.



More Dragon Ball Z x Adidas Sneakers Are Coming Soon (/news/2019/08/dragon-ball-z-...

BY JORDAN ROSE (/AUTHOR/J-ROSE) © AUG 15, 2019

Detailed look at the 'Oolong' Nizza Hi.



A Better Look at the Rumored Adidas Ultra Boost 2020 (/news/2019/08/adidas-ultra-...

BY BRANDON RICHARD (/AUTHOR/BRANDON-RICHARD) © AUG 15, 2019

See the details on the next-gen runner.



Maharishi Made Air Max 90s for Its New Location (/news/2019/08/maharishi-nike-...



Meek Mill's Renovated Basketball Court Gets Unveiled This Weekend (/news/2019/08/meek-...

BY JORDAN ROSE (/AUTHOR/J-ROSE)



A Better Look at the Titan's Nike LeBron 16 Low 'Agimat' (/news/2019/08/titan-nike-lebro...

BY JORDAN ROSE (/AUTHOR/J-ROSE)

CLOSE

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) ⌚ AUG 15, 2019

Collab created with organic materials.



More Sacai x Nike Blazers Are Releasing Next Month (/news/2019/08/sacai-nike-blaze...

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) ⌚ AUG 15, 2019

New monochrome colorways for the coveted collaboration.

⌚ AUG 15, 2019

In partnership with Puma and local Philly organizations.



Nike Allegedly Discussed Paying Zion Williamson to Attend Duke (/news/2019/08/nike-allegedly-...

BY RILEY JONES (/AUTHOR/RILEY-JONES) ⌚ AUG 15, 2019

Details on the alleged \$35,000+ payout.

⌚ AUG 15, 2019

This collaboration with the Filipino retailer drops next week.



Closer Look at One of the Camo Jordan 10s Coming Soon (/news/2019/08/air-jordan-10-...



Nike Confirms Next Sacai x LDWaffle Releases (/news/2019/08/sacai-nike-...



'University Gold' Air Jordan 12 Expected to Debut Next Summer (/news/2019/08/air-jordan-12-...

BY BRANDON RICHARD

BY VICTOR DENG (/AUTHOR/VICTOR-DENG) ☺ AUG 15, 2019

Two camouflage colorways on the way.



'Black Grape' Air Jordan 5s Getting Turned Into Golf Shoes (/news/2019/08/air-jordan-5-low...

BY JORDAN ROSE (/AUTHOR/J-ROSE) ☺ AUG 14, 2019

Another one.

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) ☺ AUG 15, 2019

Three colorways coming next month.



Sneakersnstuff Made New

Balances for 'Grown Ups' (/news/2019/08/sneakersnstuff-...

BY JORDAN ROSE (/AUTHOR/J-ROSE) ☺ AUG 14, 2019

Made-in-England collab coming next week.

(/AUTHOR/BRANDON-RICHARD) ☺ AUG 14, 2019

Rumored release information for the upcoming colorway.



Rose Gold Air Jordan 1s

Releasing for Women Only (/news/2019/08/air-jordan-1-hig...

BY RILEY JONES (/AUTHOR/RILEY-JONES) ☺ AUG 14, 2019

A new 'Fearless' colorway coming soon.



CLOSE

Detailed Look at Travis Scott's Air Jordan 6 Collaboration (/news/2019/08/travis-scott-air-...

BY BRANDON RICHARD
(/AUTHOR/BRANDON-RICHARD)
🕒 AUG 14, 2019

Coming soon.



A Pair of Zion Williamson's Sneakers Just Sold For Almost \$20,000 (/news/2019/08/zion-...

BY BEN FELDERSTEIN (/AUTHOR/BEN-FELDERSTEIN) 🕒 AUG 13, 2019

Details on the game-worn pair.



This Atmos x Air Max 1 Could Be Releasing Again (/news/2019/08/atmos-nike-air-...

BY RILEY JONES (/AUTHOR/RILEY-JONES)
🕒 AUG 14, 2019

Another chance at one of the 'Animal Pack 3.0' colorways.



The Adidas Yeezy Boost 350 V3 Is Reportedly Releasing Soon (/news/2019/08/adidas-yeezy-...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) 🕒 AUG 13, 2019

A new look at the 'Alien' colorway.



Another Off-White x Nike Dunk Low Rumored to Release This Fall (/news/2019/08/virgil-abloh-...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) 🕒 AUG 14, 2019

Two of three colorways surface.



The Off-White x Nike Waffle Racer Pack Is Reportedly Dropping Next Month (/news/2019/08/off-...

BY RILEY JONES (/AUTHOR/RILEY-JONES)
🕒 AUG 13, 2019

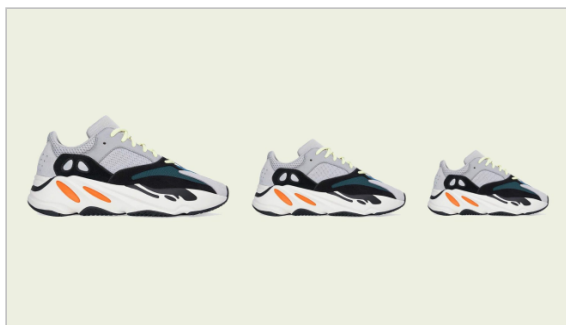
The latest news on Virgil Abloh's next collab.

CLOSE

Paris Saint-Germain x Air Jordan 1 Lows Release Very Soon (/news/2019/08/air-jordan-1-low...

BY BRANDON RICHARD
(/AUTHOR/BRANDON-RICHARD)
🕒 AUG 13, 2019

The latest pair from the ongoing partnership.



'Wave Runner' Yeezy Boost 700s Are Restocking Again (/news/2019/08/adidas-yeezy-...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) 🕒 AUG 13, 2019

Sizes for the whole family.



<https://solecollector.com/news/2016/02/campless-stockx-dan-gilbert>

Cactus Plant Flea Market Is Releasing Another Nike Collab (/news/2019/08/cactus-plant-fle...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) 🕒 AUG 13, 2019

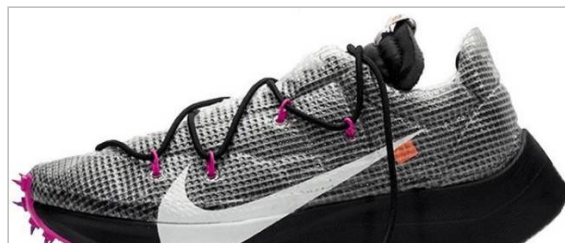
Official release details for the Blazer CPMF Sponge By You.



Release Roundup: Sneakers You Need To Check Out This Weekend...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) 🕒 AUG 13, 2019

Nike Joyride, 'Stranger Things' x Nike, 'Satin Black Toe' Air Jordan 1 High, and more.



Cara Delevingne Actually Wore Rihanna's Puma Sneakers to the White House (/news/2019/08/ca...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) 🕒 AUG 12, 2019

The model and actress is the latest guest on Complex's 'Sneaker Shopping.'



CLOSE



Official Look at the Latest UNC-Inspired Air Jordan 1 (/news/2019/08/air-jordan-1-sail...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) ⓘ AUG 12, 2019

Arriving later this month.



More Off-White x Nikes Are Reportedly Releasing This Fall (/news/2019/08/off-white-nike...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) ⓘ AUG 12, 2019

Three colorways of the Vapor Street for women.



Nike Unveils a New Way for Parents to Buy Shoes for Their Kids (/news/2019/08/nike...

BY MIKE DESTEFANO (/AUTHOR/MIKE-DESTEFANO) ⓘ AUG 12, 2019

Introducing the Adventure Club.

LOAD MORE

 (<http://www.facebook.com/SoleCollectorMag>)

 (<https://twitter.com/SoleCollector>)

 (<https://instagram.com/solecollector/>)

 (<https://www.youtube.com/user/solecollector>)



SOLECOLLECTOR PARTICIPATES IN VARIOUS AFFILIATE MARKETING PROGRAMS, WHICH MEANS SOLECOLLECTOR GETS PAID COMMISSIONS ON PURCHASES MADE THROUGH OUR LINKS TO RETAILER SITES. OUR EDITORIAL CONTENT IS NOT INFLUENCED BY ANY COMMISSIONS WE RECEIVE.

© 2019 COMPLEX MEDIA, INC. ALL RIGHTS RESERVED.

CLOSE

Exhibit 12

Fast-growing Detroit startup StockX sniffs out fake sneakers

JC Reindl, Detroit Free Press

Published 6:00 a.m. ET July 9, 2018 | Updated 8:02 a.m. ET July 9, 2018



(Photo: Kimberly P. Mitchell, Detroit Free Press)

The pair of allegedly rare Air Jordan sneakers arrived last month to the bunker-like Authentication Center of StockX, a Dan Gilbert-backed company that is one of Detroit's fastest-growing startups.

The black-and-red Jordans were purportedly from 1995. For sneakerheads who collect such things, that's close to antique.

If these shoes were authentic, they might fetch \$500 on [StockX's online marketplace](https://stockx.com/) (<https://stockx.com/>), which functions like a stock market for the re-selling of hard-to-find sneakers, sportswear, watches and handbags.

But this pair didn't pass the smell test.

One of the center's "authenticators" took a whiff of the Jordans and immediately knew something was off. Smell is one of the 25 to 30 indicators they can use to distinguish a legit shoe from a cheap knockoff.



Sadelle Moore, 31, of Detroit is the head sneaker authenticator at Stock X. (Photo: Kimberly P. Mitchell, Detroit Free Press)

"It just had a very distinct smell that we hadn't smelled before," recalled sneaker authenticator Sadelle Moore, 31, of Detroit, "so we knew automatically that was fake."

This army of dozens of merchandise authenticators form the backbone of StockX and its effort to become the world's leading resale marketplace for scarce consumer goods.

Launched in February 2016 with just a handful of employees, StockX has grown to 370 employees, including about 40 workers at its western U.S. authentication center in Tempe, Ariz.

Read more:

Tsunami of robocalls may be headed to your cell

(<https://www.freep.com/story/money/personal-finance/susan-tompor/2018/07/05/robocalls-rules-review-fcc/750545002/>)

State OKs bid for cemeteries that aren't for sale

(<https://www.freep.com/story/money/business/2018/07/04/michigan-strategic-fund-cemeteries/743908002/>)

The company says it currently processes thousands of pairs of shoes a day and handles about \$2 million in daily sale transactions. It plans to open new centers in New Jersey and London this year.

StockX CEO Josh Luber, 40, said one of the company's latest challenges in finding enough people to hire.

"There are 200 people we'd hire tomorrow, if we can find the right people," Luber said. "We'd triple the engineering team, we'd double the authentication team, we'd double the customer service team. That is just part of hyper-growth."



Tre Cadwell, 22, of Farmington carries sneakers to a station to be authenticated at the Stock X operations center in Detroit on Tuesday, July 3, 2018. (Photo: Kimberly P. Mitchell, Detroit Free Press)

StockX is headquartered on the same floor as Gilbert's personal office in downtown Detroit's One Campus Martius building. It recently moved its authentication and operations staff to additional space inside the Quicken Loans Data Center, 1401 Rosa Parks.

Roughly 70 percent of StockX's merchandise is currently sneakers, followed by about 20 percent streetwear and about 5 percent watches and handbags. StockX only sells authentic sneakers that are unworn and in their original box.

The company says it overtook eBay last year for sneaker resales. Its competitors also include online sellers and platforms such as GOAT, Grailed, Flight Club and Stadium Goods.

There is significant money in reselling sneakers. Shoe companies intentionally produce limited quantities of desirable models, such as the latest Adidas Yeezy or Air Jordans, which makes it hard for consumers to buy a pair before inventories sell out.

Similar to the dynamics of event ticketing, this confluence of small supply and big demand creates a market of people who are willing to pay lofty sums for a must-have commodity. Hot sneakers can sell for hundreds or sometimes thousands of dollars above their original retail price.

StockX's innovations include its elaborate authentication process and unique sales platform that functions like a stock market.

The way the platform works is buyers place bids and sellers place "asks." When a bid and ask match, a sale occurs automatically. StockX then tracks and graphs the completed sales, showing the current and historical market value of a particular sneaker, watch, handbag or other item.

StockX takes a 9.5 percent cut of each sneaker transaction, with the fee lowering to 8 percent for high-volume sellers.

Similar to what Kelley Blue Book is for used cars, StockX has already become a leading gauge of market value in the sneaker resale world — even for transactions that don't happen on the StockX platform.

That dynamic was on display June 30 at a sneakers and streetwear trade event called the Michigan Sneaker Xchange in Cobo Center. The event, which was sponsored by StockX, was jammed with sellers displaying like-new and lightly worn merchandise with price tags that could hit several hundred dollars or more.

Many in the crowd of buyers were teenage boys. Some looked no older than 12.



Mohamed Ibrahim of Toledo attended the Michigan Sneaker Xchange on June 30, 2018 at Cobo Center in downtown Detroit. He is holding a Sean Wotherspoon Air Max 1/97, which can sell for nearly \$1,000 (Photo: JC Reindl, Detroit Free Press)

Sneaker seller Mohamed Ibrahim, 21, of Toledo said it's common to see buyers check the price of a shoe on StockX.

"Everyone references StockX when they're at these events," Ibrahim said. "They'll pull out their phone before they'll even think about purchasing something."

Sellers typically like how StockX uses stock photos and standardized descriptions for merchandise, which makes the sales process easier for them than platforms requiring photos and written descriptions for each item.

Roland Coit, 39, of Pontiac has sold as well as bought shoes through StockX.

His purchases included a roughly \$700 pair of black Air Jordan 4 Retro X Kaws (<https://stockx.com/air-jordan-4-retro-kaws-black>) and a pair of Yeezy Wave Runner 700s (<https://stockx.com/adidas-yeezy-wave-runner-700-solid-grey>) for which he paid under \$500.

"The dope thing about it is you know it's real and you don't have to worry about counterfeit or anything like that," Coit said.

Not everyone at the sneaker event was a StockX fan. The owner of a Columbus, Ohio, store called Addicted 2 Kicks, who would only give his Instagram nickname "Juice," (https://www.instagram.com/stay_n_yourlane_ent/?hl=en) said he stopped selling on StockX because it forbids worn shoes, which he often sells. StockX only allows so-called "deadstock" shoes in never-worn condition.

He instead sells on rival reseller website GOAT.

"I was making a lot of money with StockX at first, but they got too many stipulations," he said. "They suspend your account, a lot of BS they put you through, and I had no problem with GOAT. I'm making crazy money on there."

The startup story

StockX emerged from the foundation of Luber's earlier Philadelphia-based startup called Campless. That company launched in 2013 and used eBay sales data to produce a price guide for sneakers that was the first of its kind.



It even was used by insurance companies to write policies for large sneaker collections. However, Campless was not a sales platform.

"My idea was, 'Look, eBay is the largest marketplace. That seems inefficient, and it also seems crazy how you look on eBay and one shoe is selling for \$1,000, and the other shoe is selling for \$400. What's the right price?' " Luber recalled.

By 2015, Gilbert, who founded Detroit-based mortgage giant Quicken Loans and owns the Cleveland Cavaliers NBA team, was looking to start a business to test an idea he had for a "stock market of things" for consumer goods in a marketplace using real-time trades.

He tapped Greg Schwartz, an entrepreneur he had backed through his venture capital fund, to help set up the business. They decided that sneakers would be a good first product to demonstrate the stock market concept.



Greg Schwartz, co-founder and chief operations officer for StockX. (Photo: StockX)

But neither Gilbert nor Schwartz felt they knew enough about sneakers. So they reached out to Luber, then living in Philadelphia.

Read more:

[Dan Gilbert-backed helmet maker is butting heads with industry players \(/story/money/2017/06/11/dan-gilbert-xenith-football-helmet/332416001/\)](https://story/money/2017/06/11/dan-gilbert-xenith-football-helmet/332416001/)

[Michigan fund OKs \\$26.5M for scandal-plagued cemeteries that owner says aren't for sale \(/story/money/business/2018/07/04/michigan-strategic-fund-cemeteries/743908002/\)](https://story/money/business/2018/07/04/michigan-strategic-fund-cemeteries/743908002/)

Luber, who owns a personal collection of more than 350 pairs of sneakers, recalled being pleasantly shocked to hear how Gilbert and Schwartz shared his own long-desired goal of using sneaker sales data to operate a stock market-like platform.

All the other corporate executives Luber had sat down with simply wanted to incorporate his sneaker data into their existing business models, he said.

Soon after, Luber sold his company to Gilbert and moved to Detroit to start StockX.

"Dan is a cofounder in this," said Luber, whose office attire is often backward baseball caps and hoodie sweatshirts. "He's not like the billionaire investor who wrote a check. He literally had the same idea."

Gilbert financed much of StockX's early growth. Other investors have included Eminem, actor Mark Wahlberg, Pittsburgh Steelers cornerback Joe Haden, entertainment executive Scooter Braun and fashion designer Jon Buscemi, among others.

Biggest sales

The asking price for StockX's sneaker inventory last week ranged from a \$40 pair of tan Vans to \$25,000 for the auto-lacing Nike Air MAG (<https://stockx.com/nike-air-mag-back-to-the-future-bttf-2016>). "Back To the Future" shoes. The ultra-rare MAGs came out in 2016. Just 89 pairs reportedly were made. So far, nine have resold on StockX; the highest sale price was \$32,275 for a size 11.



Sneakers are stacked up in the inventory area of the new Stock X authentication center in Detroit, photographed on Tuesday, July 3, 2018. (Photo: Kimberly P. Mitchell, Detroit Free Press)

Teko Harmon, a manager for the authentication center, said the staff will wear white showroom gloves for extra careful handling whenever a pair of Air MAGs arrives.

Other shoes with big-dollar StockX sales include the University of Michigan-themed Air Jordan 5 Retro (<https://stockx.com/air-jordan-5-retro-michigan-pe>) (\$4,500); Air Yeezy 2 Red Octobers (\$9,600, originally \$250 retail) and the "rust pink" (<https://stockx.com/air-jordan-1-retro-rust-pink>) Air Jordan 1 Retros (\$2,400, originally \$160 retail).

No fakes guarantee

Weeding out replica sneakers from authentic originals is key to StockX's business model. The company guarantees that the merchandise it ships is "100 percent authentic." So if too many knockoffs were to get through and customers then complained on social media, StockX's brand would suffer.

Luber said there are strong incentives to make knockoffs of rare sneakers and pass them off as genuine.

"It's a really big business because of the margins that these fake factories can make," he said. "They can make a fake shoe for \$40 in China and sell it for \$1,000 on eBay."

Ebay does not authenticate resold sneakers.

When StockX started two years ago, about 15 percent of the sneakers it received from sellers turned out to be replicas or fakes. Nowadays, the company says that figure is down to about 2 percent.

StockX bans sellers from its platform that willfully or repeatedly attempt to sell fakes. Would-be buyers whose orders are stopped by the discovery of a fake get refunds if no similar item is available.

"Because we check, most people don't even try to send fakes through us," Luber said. "Most of the fakes that we see are people that generally don't know they have the fakes themselves. Because if you have a fake shoe and want to scam somebody, you are better off going to eBay, somewhere where people aren't in the middle checking."

On the Reddit.com community Repsneakers (<https://www.reddit.com/r/Repsneakers/>), which focuses on replica sneakers, a few people have claimed to receive knockoff sneakers from StockX.

One user named "bwheezzy" wrote, "there's really no way to trust that someone is going to authenticate your shoes, especially when it's such a madhouse there and they have to check so many shoes."

Those who alleged to have received fakes said that after they notified StockX, the company gave them a full refund and a \$20 discount code for future purchases.

Legit check training

StockX sneakers authenticators go through a 90-day training period. They study a company "fake book" showing telltale signs of knockoffs. They also examine actual fake sneakers that StockX encountered in the past, such as the infamous "Yeezy Supremes." (Such a shoe was never officially released.)



Calais Sewell, 27, of Detroit prepares authenticated goods for shipping at the new Stock X operations center on Tuesday, July 3, 2018. (Photo: Kimberly P. Mitchell, Detroit Free Press)

"We bring in fake sneakers, we rip them apart, we note every single difference between all of them. And then we teach people, 'Here are the real ones, here are the fake,' " Luber said. "It could be different color stitching, it could be different materials, it could be different packaging. Sometimes it's the box."

And sometimes it's the smell.

Learning how to smell a knockoff is part of the training and legit check process.

"The first thing that every authenticator does with every shoe is they smell the shoe, because the glue on the fake shoes usually has a much more distinct smell," he said.

Many of the factories producing knockoffs are believed to be in China and Vietnam, he said. Some are even said to be located next door to factories producing authentic versions of the shoes they are ripping off.

Luber has yet to tour a factory that makes fake sneakers, but he hopes to someday.

"It's one of those things that is on my bucket list as a sneakerhead that I want to go and see," he said.

Contact JC Reindl: 313-222-6631 or jcreindl@freepress.com. Follow him on Twitter @JCReindl. (<http://www.twitter.com/JCReindl>).

Read or Share this story: <https://on.freep.com/2u5Uba5>

Exhibit 13

The New York Times

YOUR MONEY

Identity Theft Poses Extra Troubles for Children

By Ron Lieber

April 17, 2015

The note that arrived in the mail, dated March 25 and addressed to my grade-school-age daughter, said what we had expected and feared: Like tens of millions of other Americans, including untold numbers of children, she may have fallen victim to thieves who gained access to Social Security numbers and other personal data from the health insurance giant Anthem.

In three single-spaced pages, it noted that anyone who had dealt with the company and many Blue Cross and Blue Shield insurance plans over the last decade could be vulnerable. The letter pointed us to anthemfacts.com for more information, which it described as “our source of truth.”

Here’s what the note did not fully address, however: What are the odds that someone will steal a child’s identity? Why would a thief do that, and what exactly can parents do to keep it from happening?

I know better than to overreact to this sort of thing. Thieves have to get the data, choose to use it (instead of chickening out), pick yours to use in nefarious ways and then do so successfully before any damage to a child’s credit record can occur. Still, a 2011 joint industry-academic examination of 40,000 children caught up in a data breach found that someone else appeared to be using 10.2 percent of their Social Security numbers. Most of those instances happened before the breach in question.

EXHIBIT 13

So crime like this does happen, and here's why: Children's credit reports are clean. That's attractive to people who want to begin their financial lives anew for any number of reasons. Plus, minors don't check their credit reports or review monthly bills the way grown-ups do, which means thieves may not get caught for years or even decades.

One way that people can protect themselves from many kinds of identity theft is to put a freeze on their credit reports with Equifax, Experian and TransUnion, the three agencies that make a lot of money tracking our financial histories and selling that information to companies we want to do business with.

You have 4 free articles remaining.
Subscribe to The Times

A credit freeze is more stringent than the more popular fraud alerts that many consumers have used in the past. Putting your reports on ice means that any new creditor trying to open an account in your name won't have access to your credit report unless you go into the system and thaw it. Without seeing your credit report, companies that you are not already patronizing generally won't open a new account in your name, so the freeze usually has the effect of thwarting thieves.

The problem with the freeze, however, is that you need to have a credit report in the first place before you can put it in cold storage. Because most children don't, it's usually been nearly impossible to freeze a child's credit file.

In the last few years, though, that's been changing. According to Heather Morton, a program principal with the National Conference of State Legislatures, 19 states now require the credit agencies to help parents and guardians create a new credit report for a minor child for the express purpose of immediately freezing it. Those states are Arizona, Delaware, Florida, Georgia, Illinois, Indiana, Iowa, Louisiana, Maryland, Michigan, Montana, Nebraska, New York, Oregon, South Carolina, Texas, Utah, Virginia and Wisconsin.

Last month, Representative Jim Langevin, Democrat of Rhode Island, introduced legislation that would force the credit bureaus to let all of us do this. Equifax claims that it already lets any parent set up a freeze for a child in the other 31 states. Experian and TransUnion do not, though TransUnion, on its website, has a form that parents can complete so the company can check to see if there are any existing credit files under a child's Social Security number.

The bureaus aren't big fans of freezes, because they're an administrative annoyance and they throw a giant roadblock in their business of peddling our information. Equifax, on its website, introduces freezes as something a consumer does after being victimized, as if we'd all want to wait until the burglar has left the premises to hire a security guard. TransUnion deserves credit for at least mentioning that children may be able to get one. All of them, however, worry about creating vulnerabilities where there were none by creating a credit file that did not previously exist.

Still, if you try to set one up for your child, you're in for a battle. The agencies want reams of information, including copies of your child's birth certificate and Social Security number plus certain bills that prove where you live. Equifax and TransUnion ask you to put all of this private information in an envelope and drop it into a mailbox. Even worse, two Equifax customer service representatives I spoke to this week insisted that I should put "minor child" at the top of the address. It might as well say, "Steal this envelope!"

I'm doing it anyway (though without saying, "Steal Me"), if only to annoy the agencies that so clearly do not want me to do this.

Freezes won't stop every kind of theft, alas. Thieves sometimes use children's Social Security numbers and other data to file fake tax returns and get illegitimate refunds, gain access to health care and work legally even if they are not citizens. In each of those instances, there may never be a credit check that reveals the freeze.

So what are the ways to keep private data private that are within our control? Don't carry around Social Security cards. Keep them under lock and key at home. Keep your child's date of birth off social media. Talk to your offspring about where to click and not to click on websites and in incoming email. Question school officials and doctors who want children's Social Security numbers for forms, as it may not truly be necessary.

Also, keep your voice down at the pharmacy and physician's office.

Robert P. Chappell Jr., author of "Child Identity Theft: What Every Parent Needs To Know," sometimes jots down names, insurance information and other bits and pieces as he listens in those places and then approaches people afterward to gently correct their data hygiene. So far, nobody has punched him in the nose. "Most of them are very nice and have no idea about the harm that can come from it," said Mr. Chappell, who works in law enforcement by day. "Usually, I'm in civilian clothes."

One problem with the various legislative efforts to fix the problem is that they won't do much about the many situations where it's the children's own parents who commit the identity fraud. Mothers and fathers may do this out of desperation, having already wrecked their own credit or experienced some acute financial calamity. Foster children are frequent identity theft victims, too. Whatever the reason for the crime, these parents aren't about to freeze their children's files.

So what could stop them? One possibility exists only in theory, and it's called the 17-10 registry. The idea here is that when children are born, their Social Security numbers automatically go into a "do not break the glass until two months before age 18" database. Parents could be prohibited from opting out of the database for their children, and credit reporting agencies (and employers and the Internal Revenue Service) would hopefully crosscheck it before letting anyone use any Social Security number. TransUnion is experimenting with its own database that families in Utah can put their children in.

My daughter seems unscathed so far, and we are signing up for the free monitoring service that Anthem is making available for two years. But Adam Levin, the founder or co-founder of two credit- and identity-related businesses and the author of a book scheduled for release in November called "Swiped: What Identity Thieves Do and How to Stop Them," questioned why the free service ought to halt then, even if Anthem is paying for a longer period than other breached organizations have in the past.

"Social Security numbers are like money in the bank, and thieves don't need to use them at any specific moment in history," he said. "You're going to have to look over your shoulder for the rest of your life."

Then again, you're probably already doing that. The companies we pay and the governmental agencies that keep track of us have proved with startling consistency that they are not up to the task of keeping our data safe. Then, they compound that by dragging their feet when tools emerge that allow us to flip a switch and try to contain the damage.

Until that changes, you're more or less on your own. But you already knew that, right?

Twitter: @ronlieber

Make the most of your money. Every Monday get articles about retirement, saving for college, investing, new online financial services and much more. Sign up for the Your Money newsletter here.

A version of this article appears in print on April 17, 2015, Section B, Page 1 of the New York edition with the headline: Identity Theft Poses Extra Risk for Children

READ 66 COMMENTS

Exhibit 14



[Skip Navigation](#)



- [Sign In](#)
- [Pro](#)
- [Watchlist](#)
- [Make It](#)
- [USA](#)
- [INTL](#)



[Markets](#)
[Watchlist](#)
[Business](#)
[Investing](#)
[Tech](#)
[Politics](#)
[CNBC TV](#)
[Menu](#)

Identity theft isn't just an adult problem. Kids are victims, too

[SEARCH QUOTES](#)

Investor Toolkit

Identity theft isn't just an adult problem. Kids are victims, too

Published Tue, Apr 24 2018 9:23 AM EDT

[Kelli B. Grant@kelligrant](mailto:Kelli.B.Grant@kelligrant)

Key Points

- More than 1 million children were victims of identity theft or fraud last year, according to a new report from Javelin Strategy & Research.
- Two-thirds of those victims were age 7 or younger.
- Six in 10 child victims personally know the perpetrator.

EXHIBIT 14

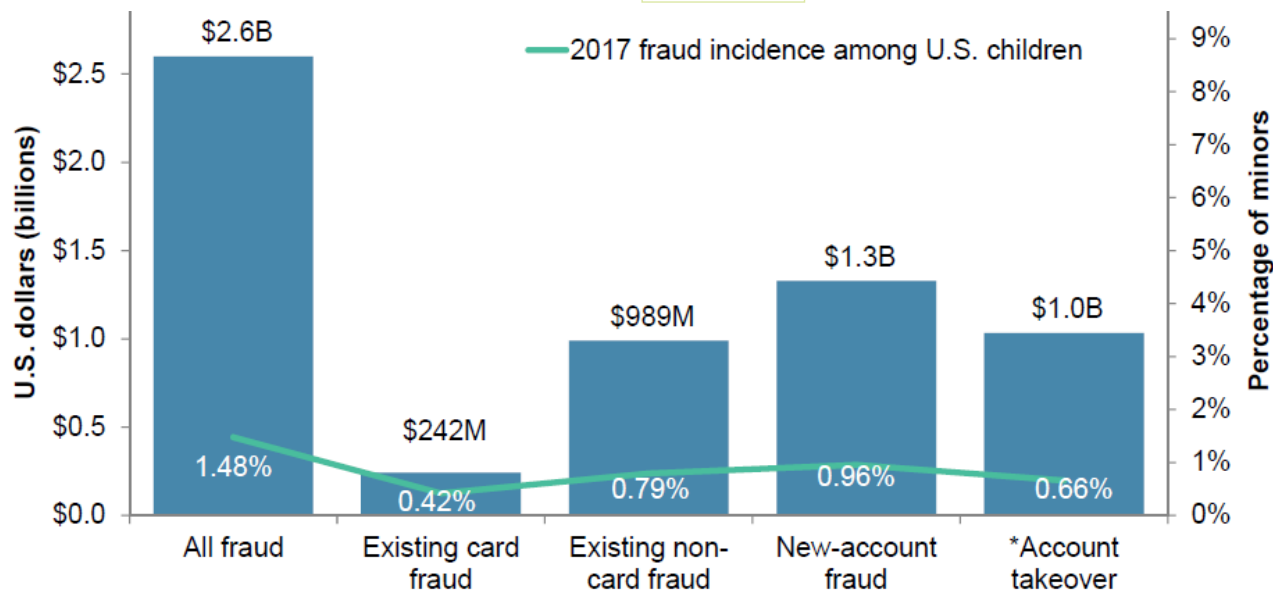


Hero Images | Getty Images

Should your toddler receive a jury-duty summons in the mail, or debt collectors start calling for your tween, don't be so quick to dismiss those interactions as a quirk of mistaken identity.

More than 1 million children — or 1.48 percent of minors — were victims of identity theft or fraud in 2017, according to a new report from Javelin Strategy & Research. Two-thirds of those affected were age 7 or younger.

“As adults, we're hypersensitive right now to the idea that our identities are at risk and our personal information is out there,” said Al Pascual, senior vice president of research and the head of fraud and security at Javelin. “We've Jedi mind-tricked ourselves into thinking this is an adult problem.”



*Overlaps with existing card fraud and existing non-card fraud

Source: Javelin Strategy & Research, 2018

Child ID theft risks

Minors face some of the same risks as adults do, with their information being [compromised in data breaches](#).

But thieves are more likely to capitalize on kids' data. Among notified breach victims last year, 39 percent of minors became victims of fraud, versus 19 percent of adults, according to Javelin.

While adults make prime targets for [their account balances](#), the "blank slate" a child provides can enable a criminal to do more damage by opening new lines of credit before someone catches on.

More from Investor Toolkit:

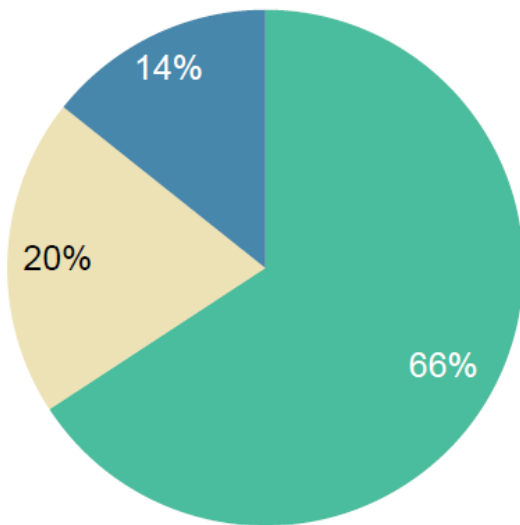
[When did you last update beneficiary designations?](#)

[3 tips for handling stock market swings](#)

[Channel anxiety to avoid bad investment decisions](#)

"There's a lot of value in that there's no credit report tied to that Social Security number," said Pascual.

So-called synthetic identity theft, where thieves create new identities using a combination of real and fictitious information, is another risk for minors, said Eva Velasquez, chief executive and president of the Identity Theft Resource Center, which helps consumers dealing with such fraud. The [change to randomized Social Security numbers](#) in mid-2011 means a crafty thief could potentially build a profile around a number before there's a victim, she said.



Source: Javelin Strategy & Research, 2018

“We’re talking to folks who are having these numbers issued to their kids, and they’re already tainted,” Velasquez said. A newborn’s SSN, when you go to file taxes, “might have earnings associated with it and a five-year credit history.”

Minors are also much more likely than adults to become victims of familiar fraud — [meaning the identity thief is someone they know](#).

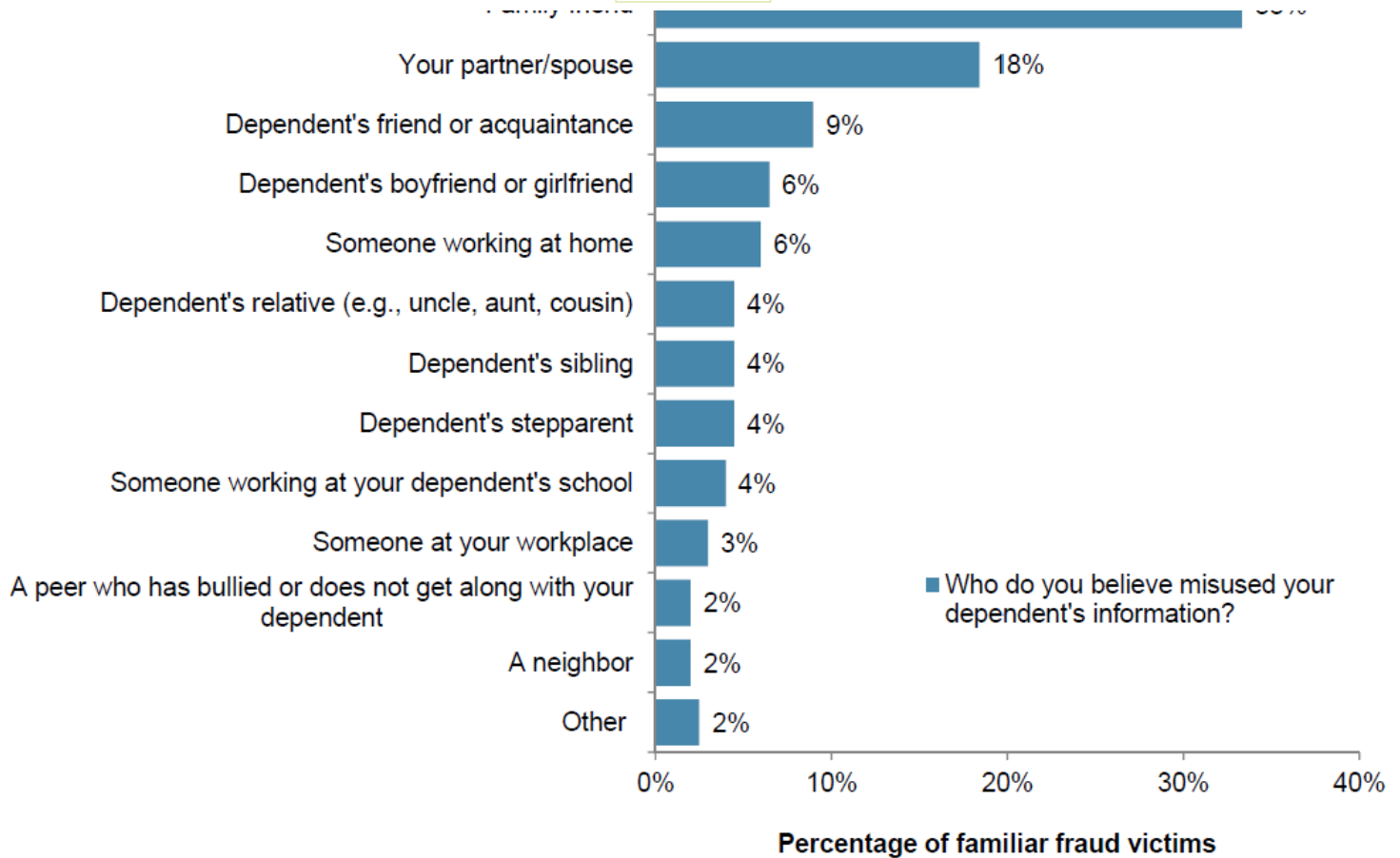
Javelin estimates that 6 in 10 child victims personally know the perpetrator, compared to 7 percent of adults. Family friends were the most common suspect, accounting for a third of cases.

“The big threat is going to be people who are close to the child, for sure,” Pascual said.

Child identity theft is a growing and expensive problem

PAD TUESDAYS 10P ET

WATCH NOW



Source: Javelin Strategy & Research, 2018

Protecting your kids

You might think that being 5 years old would be a pretty good “It wasn’t me” defense against a fraudulent five-figure credit card bill. But experts say untangling identity theft and fraud committed against a minor is just as complicated as when an adult is the victim.

You’ll still have to go through the same steps with that bank or creditor to prove the fraud, said Melba Amissi, chief operating officer at Identity Guard, which sponsored the Javelin report.

The high rate of [familiar fraud](#) makes it tougher to build your case, said Javelin’s Pascual. Perpetrators may have used your verified home address or phone to apply for the account, for example. And victims may not be willing to make the necessary law-enforcement complaints to document the problem.

“Do I file a police report against my brother?” he said.

With that in mind, it’s key to take steps to prevent your child’s identity from being compromised in the first place and act quickly if you suspect a problem.

1. Keep data out of circulation

Don’t overshare personal details, such as your child’s Social Security number, said ITRC’s Velasquez. Not every entity that might ask for it (think: summer camp or the doctor’s office) actually requires it.

“Once it’s out of your hands ... there’s not a lot you can do,” said Velasquez. “You’re counting on the company to be good stewards of that information.”

SIGN UP FOR OUR NEWSLETTER

YOUR WEALTH

Weekly advice on managing your money

SIGN UP NOW

Get this delivered to your inbox, and more info about our products and services.
By signing up for newsletters, you are agreeing to our [Terms of Use](#) and [Privacy Policy](#).



Familiar fraud is often a crime of opportunity: The perpetrator either already knows or has easy access to a child's Social Security number and other details.

Keep any sensitive personal and financial information out of sight, said Velasquez at ITRC. Lock up paper documents such as birth certificates and tax returns, and password-protect your home electronic devices.

VIDEO1:3601:36

How to protect yourself from identity theft in the wake of Equifax data breach

[Digital Original](#)

3. Freeze your child's credit

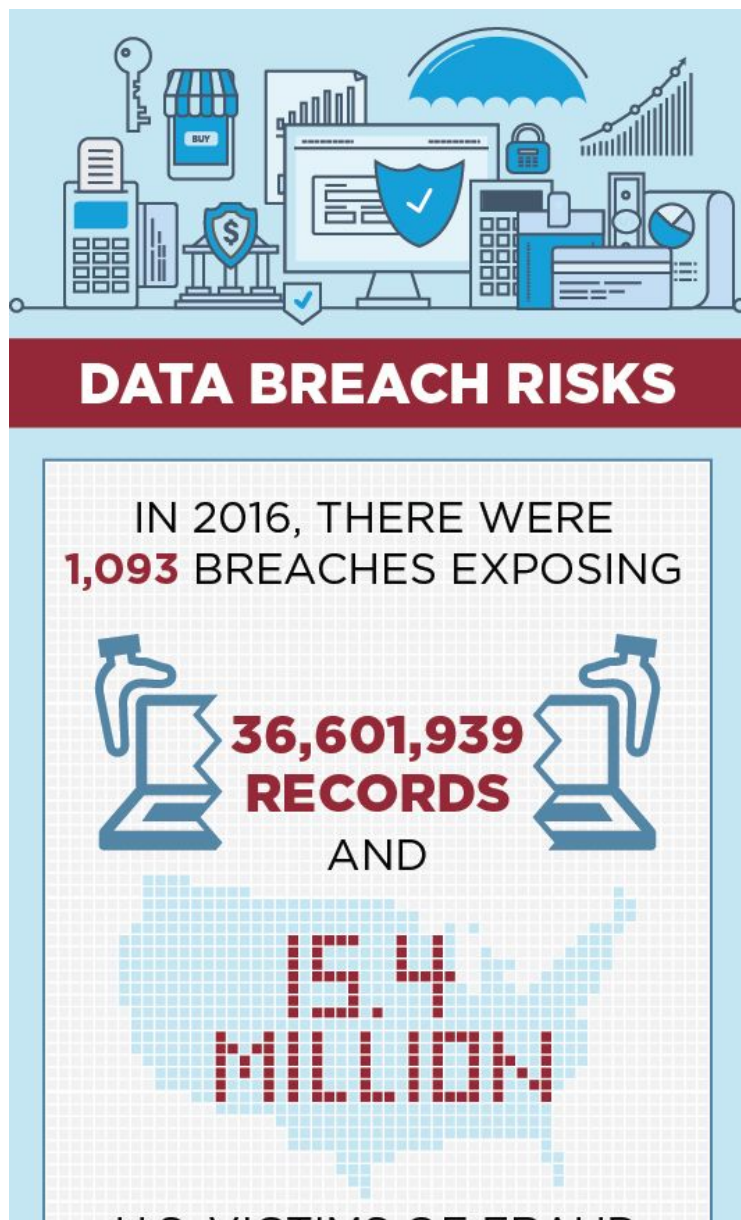
Depending on the state where you reside, you may be able to proactively [freeze your child's credit file](#) so that no one (not even your child) can open new lines of credit in his or her name, Velasquez said. Check with your state attorney general and the three major credit reporting companies — [Equifax](#), [Experian](#) and [TransUnion](#) — for details on the process.

If you take that step on behalf of your children, make sure that you're not the only person to know the PIN to lift the freeze, Velasquez said. (You might [share that detail](#) with your estate planner or the person named as guardian in your will, for example.)

4. Monitor for red flags

A credit freeze only helps on credit, and there are plenty of other avenues where a Social Security number or other data can be misused, Amissi said. Think fraudulent tax returns, for example, or exploitation to obtain medical treatment or mislead law enforcement.

So be alert for unusual calls or mailings that would point to an adult problem, like that jury summons, collection calls or a rush of preapproved credit card offers.



HOW TO PROTECT YOURSELF

1 SHIELD IMPORTANT DATA

You can't control how companies protect your data. So limit what data they have:

Don't provide your Social Security number unless required.

Use only one credit card for online purchases.

Send bill payments from your bank instead of giving the account number to third parties like your gym or cellphone carrier to make automatic withdrawals.



2 BEEF UP ACCOUNT SECURITY



Enable two-step verification where possible. This protection requires users logging in to also enter a code sent to a cellphone or email linked to that account. In other words, a would-be thief will have to compromise more than one account to succeed.

3 GET SMART ABOUT PASSWORDS

Don't use an obvious combo, and don't use the same password everywhere.

Criminals try login details stolen in one breach on other accounts — like bank and email — hoping you've done just that. Free password managers like LastPass or Dashlane string random letters and numbers into tough-to-crack passwords and remember them for you.



The most common passwords in 2016: "123456," followed by "123456789" and "qwerty."

4 SECURE YOUR DEVICES



Keep the operating systems and software on your computer, phone and other devices up to date. Password-protect them to thwart prying eyes. If you're not the only one

using a device, don't set sites to automatically log in or save passwords.



to see hackers create rogue networks with names similar to that of a nearby business, to snare unsuspecting consumers. Even if the network is legit, there's no guarantee it's secure. Thieves could intercept data like your account login or credit card number.



6 MONITOR ACCOUNTS



Regularly check financial statements for possible fraud. Opt in to receive text or email alerts from your bank and credit card issuers

for events like a big-ticket purchase or account changes like when a new bill payee is set up or the password changes.

SOURCES: IDTHEFTCENTER.ORG,
JAVELIN STRATEGY,
KEEPERSECURITY.COM,
CNBC.COM REPORTING.

INFOGRAPHIC DESIGN BY ROGER AN



Related Tags

- [Social Security](#)
- [Financial consulting](#)
- [Investment management](#)
- [Personal finance](#)

You May Love

The Highest Paying Cashback Card Has Hit The Market

Wise Bread

8 Cars So Cool It's Hard to Believe They Cost Under \$20k

Auto Enthusiast | Search Ads

Wells Fargo \$400 Welcome Bonus Offer. Learn More

Wells Fargo - Member FDIC

Play this for 1 minute and see why everyone is addicted

Vikings: Free Online Game

Sponsored Links by Taboola

Related



2. [Here's what is not covered by Medicare and here's how you can prepare](#)



3. [The Queen of England gets a supreme salary ... see how other world leaders stack up](#)



4. [Buffett: How to invest in stocks when inflation spikes](#)



5. [5 criteria to consider when selecting stocks](#)

[More In Investor Toolkit](#)

[Taking a loan from your 401\(k\) does come with risks](#)

[Sarah O'Brien](#)

[Social Security calculators aim to take the complexity out of deciding when to claim](#)

[Lorie Konish](#)

[Why index investing makes sense for most people](#)

Paul Sydlansky, founder of Lake Road Advisors

[Read More](#)



- [Subscribe to CNBC PRO](#)
- [Licensing & Reprints](#)
- [Join the CNBC Panel](#)
- [Supply Chain Values](#)
- [Advertise With Us](#)
- [Closed Captioning](#)
- [Digital Products](#)
- [Terms of Service](#)
- [Privacy Policy](#)
- [News Releases](#)
- [Internships](#)
- [Corrections](#)
- [About CNBC](#)
- [AdChoices](#)
- [Site Map](#)
- [Podcasts](#)
- [Contact](#)
- [Careers](#)
- [Help](#)

-
-
-
-
-
-
-

News Tips

Got a confidential news tip? We want to hear from you.

[Get In Touch](#)

CNBC Newsletters



© 2019 CNBC LLC. All Rights Reserved. [A Division of NBCUniversal](#)

Data is a real-time snapshot *Data is delayed at least 15 minutes. Global Business and Financial News, Stock Quotes, and Market Data and Analysis.

Data also provided by

Exhibit 15

[CONSUMER](#)

More than 1 million children were victims of ID theft last year

Two-thirds of the victims were under the age of eight.



By the time the ID theft has been discovered, the fraudsters are long gone – and all parents can do is try to clean up the mess.

Mint Images / Mint Images RF/ Getty Images

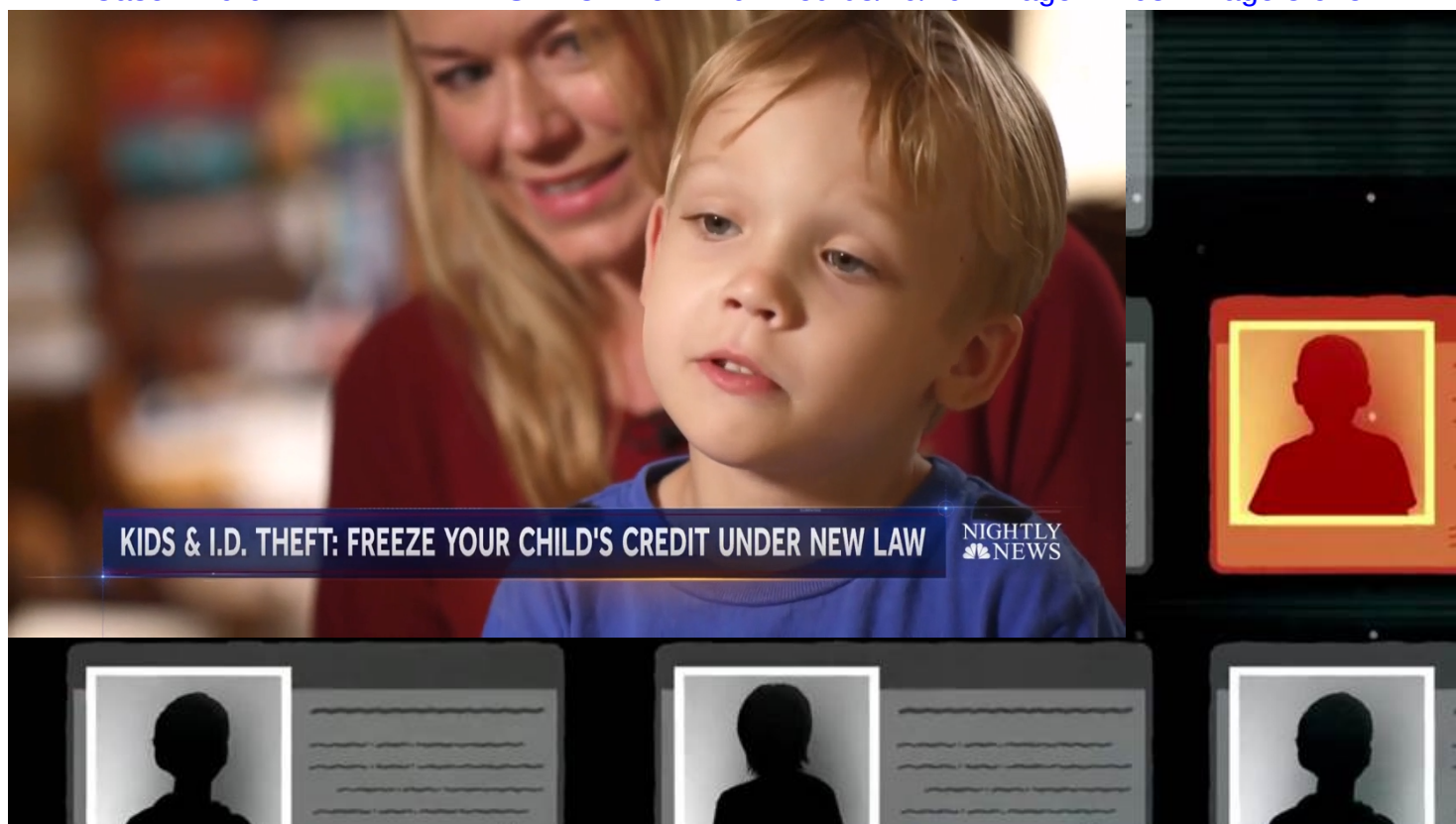
June 21, 2018, 10:24 AM CDT

By Herb Weisbaum

EXHIBIT 15

We think of [identity theft](#) as an “adult” problem, but no one is immune from this crime. More than 1 million children in the U.S. were ID theft victims last year, resulting in losses of \$2.67 billion, according to the [2018 Child Identity Fraud Study](#) by Javelin Strategy & Research.

No one is too young to be targeted. Javelin found that two-thirds of the victims were under the age of eight. Another 20 percent were eight to 12 years old.



KIDS & I.D. THEFT: FREEZE YOUR CHILD'S CREDIT UNDER NEW LAW

NIGHTLY NEWS

[As more identity thieves target children, new law aims to help parents protect their kids](#)

SEPT. 7, 2018 01:22

“And this is just the tip of the iceberg; odds are there were far more than a million victims last year,” said Al Pascual, Javelin's senior vice president for research. Minors are “an extremely vulnerable population with minimal ability to protect itself,” according to the report.

Another key finding: Data breaches are more of a risk for minors than they are for adults. Last year, 11 percent of all U.S. households had at least one minor. Of those who were notified that their information was breached, 39 percent of the children became fraud victims, compared with 19 percent of the adults notified about a breach.

“Children are more likely to become fraud victims after a breach because their core identity elements, like Social Security numbers, are more valuable for criminals,” Pascual told NBC News. “Criminals can have a field day with a child's identity information because it's never been used before. When a bank or other company pulls a credit report, they're not going to find anything, and so the criminal has a clean pallet to work on.”

Fraudsters can buy a child's Social Security number on the dark web for about two dollars, former ID thief Brett Shannon Johnson told NBC News. Johnson, who served more than six years behind bars, [is now a consultant who specializes in fighting the crimes he helped perfect.](#)

Parents should look for warning signs such as their child receiving pre-approved credit card offers in the mail.

A child's SSN is typically used to create what's called a "synthetic identity," Johnson said. The thief takes the legitimate (stolen) number, adds a different name, birthdate, address and phone number to start a new and bogus credit file.

"Then you can go to town using it for whatever nefarious purposes you want," Johnson said. "A crook can build up the credit score on that synthetic identity in about 30 days and then apply for loans and credit cards, get medical treatment or file fraudulent tax returns. By the time the crime is identified, by the time the child or parents discovers they're a victim, the crooks are long gone and all you can do is try to clean up the mess."

Last month, Sara Woodington, a single mom who lives in southeastern Pennsylvania, discovered that a crook in Texas had used her 17-year old son's SSN to create a synthetic identity for himself. The fraudster had combined his name and address with her son Jon's SSN to create a false identity, to get restaurant jobs in Austin.

Woodington's son, John, is severely autistic and cannot work. His mother lives on government assistance. Sara learned about the ID scam when her benefits were threatened because the government thought John was working in Texas.

Woodington fears her benefits will now be constantly threatened – and she worries what other damage this situation will create for her son.

"I have the man's name and address, and no one will help," Woodington told NBC News. "The police told me to go to welfare, welfare told me to go to Social Security, Social Security sent me to the IRS. It's like a big bureaucratic circle. I'm extremely angry and extremely frustrated that no one wants to help."

Sara is now getting help from the non-profit [Identity Theft Resource Center](#). Eva Velasquez, the center's president and CEO, told NBC News this is a common situation.

"Law enforcement is simply not equipped to deal with the epidemic of identity fraud," Velasquez said.

Keeping it in the family

All too often, child-identity theft is an inside job. Javelin found that 60 percent of child victims know their perpetrator – a parent or guardian, other family member or family friend. By comparison, only 7 percent of adult-ID theft victims know who did it.

One reason it's so difficult to prevent this familial crime: Many of these perpetrators have legitimate access to the child's personal information.

"Children are just easy targets. They're not monitoring their credit or monitoring their accounts," said Javelin's Pascual.

The most common identity fraud against children is new-account fraud – where the criminal uses their personal information to open a new credit card or bank account.

Rod Griffin, director of consumer education and awareness at credit monitoring giant Experian, advises parents to find out once a year if their child has a credit report – even if that child is too young to have a credit file.

For a minor 14 or older, go to [annualcreditreport.com](#) and request their credit report. If your child is 13 or younger, you will need to fill out paperwork to prove you have the right to this information. The site has detailed information about [requesting a credit report for a minor](#).

"If there's no record on file, that's a good sign; it says your child's identity is not being used to commit credit fraud and that may be the only step you need to take," Griffin said. "If the child does have a file for a legitimate reason – such as

you made them an authorized user for your credit card – check the file to make sure everything is accurate and look for signs of fraud. If everything is in order, parents may want to freeze the credit file.”

In 29 states, parents, legal guardians or other representatives of minors are allowed to place a security freeze on that child’s credit report at each of the three credit bureaus. To start the process, go to [TransUnion](#), [Experian](#) and [Equifax](#).

“I’m a big believer in credit freezes for kids,” said Neal O’Farrell, executive director of the non-profit [Identity Theft Council](#). “It closes that file off to new credit, the same as an adult credit freeze. It’s not going to prevent criminal impersonation, employment fraud or tax fraud, but it will prevent the creation of a new account, which is what most identity thieves want to do.”

Velasquez urges parents to look for warning signs that “someone is using your child’s identity to operate like an adult in the adult world.” These would include: A credit card bill, jury summons, driver’s license renewal, bills for medical care or other purchases, collection calls or notices, and pre-approved credit card offers.

“Don’t assume it’s a mistake or clerical error,” Velazquez said. “Don’t ignore these red flags. You need to follow up on them right away.”

Herb Weisbaum is The ConsumerMan. Follow him on [Facebook](#) and [Twitter](#) or visit [The ConsumerMan website](#).

[ABOUT](#)[CONTACT](#)[CAREERS](#)[PRIVACY POLICY](#)[TERMS OF SERVICE](#)[NBCNEWS.COM SITE MAP](#)[ADVERTISE](#)[ADCHOICES](#)

© 2019 NBC UNIVERSAL

NEWS

MSNBC

TODAY

Exhibit 16

CHILD IDENTITY THEFT

New Evidence Indicates Identity Thieves are Targeting
Children for Unused Social Security Numbers

*By Richard Power,
Distinguished Fellow, Carnegie Mellon CyLab*

EXHIBIT 16

EXECUTIVE SUMMARY

In the cyber-centric world of the 21st Century, parents have many risks and threats to ponder as they attempt to provide a safe present and a secure future for their children. Each day, a new danger seems to capture the headlines, from exposure to online predators to the cyber-bullying by schoolmates. Meanwhile, those parents are looking over their own shoulders, careful to guard against the crime of identity theft, so that they can continue to provide that safe present, and to build that secure future. Well, it just got worse.

Because, as this report suggests, it is possible that you could be quite effective at warding off online predators and cyber-bullies, as well as proving quite successful at guarding your own hard-earned good credit, only to find that your child's identity has been violated, and your family's financial and emotional well-being threatened in an almost inconceivable way.

What would you do if your child was in foreclosure on a home in another state? Wouldn't you want to know if your child had run up a huge utility bill across town?

These are not theoretical questions, these are real-life questions that the parents and guardians of children in this report have been forced to come to grips with. In Child Identity Theft, you will find a hard look at what child identity theft means, including an analysis of over 4,000 incidents of child identity theft, and the actual stories of several victims. The report also lists recommendations for preventative measures that should be taken by both public and private sector institutions, as well as protective steps for parents to take directly.

WHAT WOULD YOU DO IF YOUR
CHILD WAS IN FORECLOSURE
ON A HOME IN ANOTHER STATE?

KEY POINTS INCLUDE

1

First large child ID theft report ever published, based on identity protection scans of over 40,000 U.S. children.

2

Unused Social Security numbers are uniquely valuable as thieves can pair them with any name and birth date. This is particularly useful for illegal immigration.

3

A child's identity is a blank slate, and the probability of discovery is low, as the child will not be using it for a long period of time. Parents typically don't monitor their children's identities.

4

The potential impact on the child's future is profound; it could destroy or damage a child's ability to win approval on student loans, acquire a mobile phone, obtain a job or secure a place to live.

5

The primary drivers for such attacks are illegal immigration (e.g., to obtain false IDs for employment), organized crime (e.g., to engage in financial fraud) and friends and family (e.g., to circumvent bad credit ratings, etc.).

parents*

** typically don't monitor their children's identities*

KEY FINDINGS INCLUDE

1	2	3	4
4,311 or 10.2% of the children in the report had someone else using their Social Security number – 51 times higher than the 0.2% rate for adults in the same population	Child IDs were used to purchase homes and automobiles, open credit card accounts, secure employment and obtain driver's licenses	The largest fraud (\$725,000) was committed against a 16 year old girl	The youngest victim was five months old; 303 victims were under the age of five

4,311 or 10.2%*

** of the children in the report had someone else using their Social Security number*

METHODOLOGY

This child identity theft report is not based on survey results. It is based on identity protection scans on 42,232 children (age 18 and under) in the U.S during 2009-2010. This pool of 42,232 child identities includes everyone under 18 in a database of over 800,000 identity records.

The participants were enrolled in the Debix AllClear ID Protection Network after receiving notice that their personal information may have been compromised during a data breach. Excluded from this report were children and adults who were affected by data breaches that resulted in targeted attacks against the population.

Note: The attacks do not appear related to the data breach events. For example, 78% of the child attacks occurred prior to the data breach events. Moreover, the attack rate for the adults affected by these same data breaches is very low at 0.2% - below the national average of 1% for the general population (Source: Javelin 2010).

This is a non-scientific report. The data does not project or imply any estimate of total number of child identity theft incidents, or what percent of children's identities are stolen, or what percent of total number of identity theft incidents involve children.

What this data does is provide some disturbing evidence that identity thieves are targeting children due to the unique value of unused Social Security numbers. It highlights some serious risks and threats, and raises some serious questions that should be the subject of a scientific study, e.g., to determine the scope of the problem, and how it is trending.

what
this
data
does*

** is provide some
disturbing evidence
that identity thieves
are targeting children
due to the unique
value of unused Social
Security numbers.*

INTRODUCTION

OVER FOUR THOUSAND CHILDREN'S IDENTITIES VIOLATED

Identity theft is a perennial crime that has taken on new dimensions in the Information Age. It is no longer a one-on-one crime dependent upon a lost social security card or a carelessly discarded credit card receipt. Industrialized by organized cyber criminals, 21st Century identity theft is global in its reach and exhaustive in its applications. For the individual who has been victimized, 21st Century identity theft can prove devastating in its consequences.

The numbers are shifting sands.

Hundreds of millions of identities are exposed every year; tens of millions of these identities are exploited in the commission of financial fraud.

In this report, we will focus on just a few thousand of these exposed identities.

But there is something different about this handful of sand grains.

They have a common characteristic, one that is both startling and disturbing: these several thousand identities belong to children.

In 2008, Debix the provider of AllClear ID, released a small Child Identity Theft Study based on 500 cases. This follow-up report is the largest child identity theft report ever published. The data we explore in this 2011 report is based on identity scans of over 40,000 children, and the resulting investigations that uncovered over 4,000 possible cases of child identity theft.

These 4,000+ cases raise some compelling questions.

In this brief report, we will provide some context, then explore the data and its implications, and conclude with some recommendations.

HUNDREDS OF MILLIONS
OF IDENTITIES ARE EXPOSED EVERY YEAR.

IDENTITY CRISIS

In 2009, the American Bankers Association released a survey that indicated that “for the first time, more bank customers (25%) prefer to do their banking online compared to any other method. *ABA, 9-21-09*

In January 2011, Starbucks launched a mobile payment program in all U.S. company-operated stores, allowing customers to pay for in-store purchases with BlackBerrys and iPhones. *San Francisco Chronicle, 1-19-11*

The ease of use with which you can now shop online, bank online, make travel arrangements online, pay your bills online, and pursue your personal interests online, is also available to the cyber criminal.

According to the U.S. Department of Justice, an estimated 11.7 million persons, representing five percent of all persons age 16 or older in the United States, were victims of identity theft between 2006 and 2008. These 11.7 million instances resulted in total financial losses of over \$17 billion. But some of the cost is not quantifiable. Cleaning up after being victimized by identity thieves can be painful and time-consuming: “An estimated 27 percent spent more than a month clearing up the problems. Victims who spent more than six months resolving the problems associated with the identity theft were more likely to report that the experience was severely distressing... Overall,

about 20 percent of victims described the identity theft as severely distressing.” 11.7 million persons reported identity theft victimization in 2008, *US Department of Justice, 12-16-10*

Another reliable source of data is the Identity Theft Resource Center (ITRC). Its 2010 Breach List documents 662 breaches, in which 16,167,542 identities were exposed. *Information Week, 1-4-11*

Of course, this number includes only those breaches reported by credible sources. The total number is likely higher, perhaps much higher. The ITRC report only reflects events publicly acknowledged. There are other significant events, which have gone unreported; there are also likely to be events that were not even detected. Furthermore, the ITRC total of 16,167,542 identities exposed could easily be dwarfed by a single significant event; for example, in 2009, over 130 million credit and debit card numbers were breached in the Heartland hack, and approximately 76 million U.S. military veterans records were exposed in an accidental breach involving a recycled disk drive.

The numbers are shifting sands.

But what does this handful of sand grains tell us, what are the implications of these 4,000 plus cases involving the exposure of child identity?

11.7 million

persons reported identity theft victimization in 2008

CHILDHOOD'S END

From cyber bullying to sexting to prowling predators, the Information Age has brought with it a new spectrum of risks and threats for parents to guard their children against, and now that spectrum of threats has expanded to include child identity theft.

The online experience has changed childhood, for both better and worse. It enables children to explore the life of the world, but without proper precautions, it also enables the world to explore your child's life.

Consider a random sampling of recent surveys and news stories:

"Online bullying is a problem that affects almost half of all American teens, according to the National Crime Prevention Council. In a recent survey conducted by the Cyberbullying Research Center, 20 percent of middle-school students admitted to "seriously thinking about attempting suicide" as a result of online bullying." *MSNBC*, 3/9/11

"More young children know how to play a computer game (58%) than ride a bike unaided (52%). While a quarter of young children can open a web browser window, just 20% can swim unaided. Incredibly, while over two-thirds (69%) of 2-5 year olds can operate a computer mouse, just 17% can tie their own shoelaces." *Biz Report*, 1-20-11

"More than a quarter of young people have been involved in sexting in some form, an Associated Press-MTV poll found. ... Half of all young people said they have been targets of digital bullying." *Associated Press*, 12-3-10

"Four out of five children can't tell when they are talking to an adult posing as a child on the internet, according to researchers working on software to track pedophiles online." *Science Daily*, 6-2-10

"At least three Prince Edward Island teens have been contacted on Facebook by a fake talent scout promising them a career as a model in exchange for photos of themselves in lingerie, incidents that highlight the risk to children who expose their personal details online." *National Post*, 1-17-11

"A pedophile has been arrested for allegedly breaching a restraining order and contacting children on Facebook. The arrest in Adelaide has prompted a police warning to parents to talk to their children about using the Internet safely." *Adelaide Now*, 12-23-10

"High School students have sued the Lower Merion School District in Philadelphia for spying on them using their laptops' built-in cameras. School administrators activated the webcams remotely and recorded students' activities at home." *Gizmodo*, 2-18-10

Dena Haritos Tsamitis, CyLab's Director of Education, Training and Outreach, and the developer of www.MySecureCyberspace.com, a free educational resource on cyber security and privacy for children and their parents, commented that "With increased cyberawareness, individuals are seeking ways to secure their personal financial information more than ever before. Based on this report, it's clear they need to go further and extend that protection for their children. Parents are already struggling to handle the threats of cyberspace, including securing their own computers and talking with their children about the many risks in cyberspace from online predators to cyberbullying. The trend in child identity theft is added weight on their shoulders. Although it will be a challenge for them to manage, it is essential to safeguarding their children's futures."

And now, to this troubling litany, add the issue of child identity theft.

A GLIMPSE INTO WHAT THE DATA REVEALS

The data examined for this report includes the identities of 42,232 minors.

Minors whose identities showed up in the wrong places ranged from infancy to 18:

- *Cases involving identities of minors 5 and under: 303*
- *Cases involving identities of minors from 6 to 10: 826*
- *Cases involving identities of minors from 11 to 14: 1212*
- *Cases involving identities of minors from 15 to 18: 1849*

Some compelling data points emerge from this handful of sand grains, including:

- *Cases with suspect name associated with a child's Social Security number (SSN): 5,497 (Note: There are many cases with more than one suspect attached to a single child's identity. Not only is the child's ID stolen, it is shared.)*
- *Cases in which child's SSN appeared in loan and credit account records: 6,948 (Note: Within each case, there can be multiple records connected to one child.)*

- *Cases in which a child's SSN appeared in utility service records: 1,767*
- *Cases in which a child's SSN appeared in records related to property assessments, deeds, mortgages and foreclosures: 537*
- *Cases in which a child's SSN appeared in driver's license records: 415*
- *Cases in which a child's SSN appeared in vehicle registration records: 235*

There is another fascinating and disturbing number that jumps out while going through the data. The child ID theft rates stand in stark contrast to adult ID theft rates from the same security breach population. 10.2% (4,311) of these 42,232 minor's Social Security numbers had loan, property, utility and other accounts associated with them. This is fifty-one (51) times higher than the 0.2% identity theft rate for adults in the same population over the same period – 633 of the 347,362 adults had someone else use their Social Security number used to commit fraud.

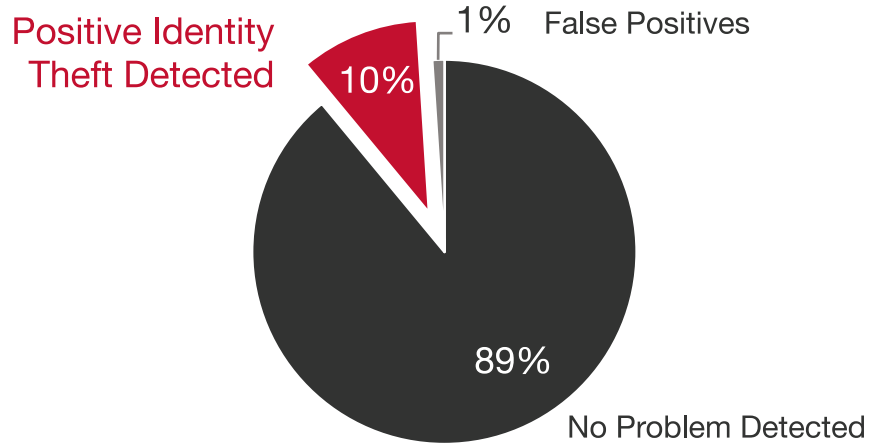
Are child Social Security numbers a hot commodity? Are cyber criminals and other fraudsters seeking them out? Are child IDs preferable for fraudsters?

children had 51 times
higher attack rate than adults

GRAPHS & CHARTS

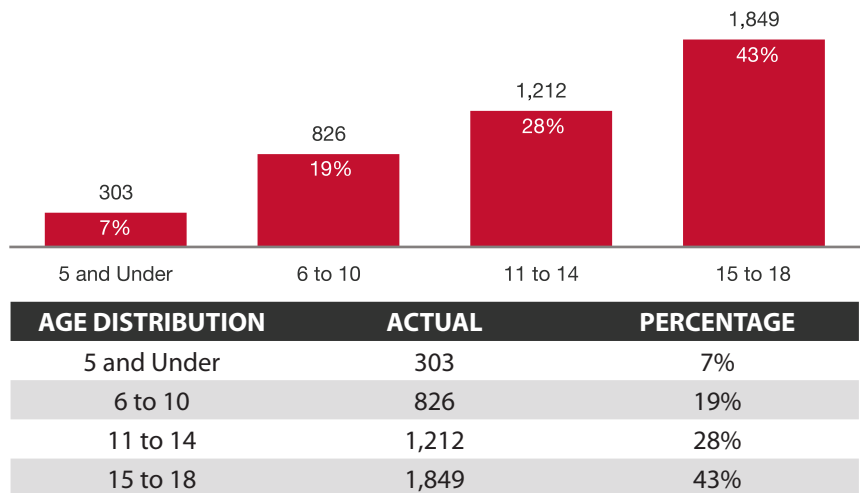
10.2% of Child Identities Scanned Exhibited Evidence of Identity Theft

Total: 42,232 Minors
Identities Scanned
Time Period: 10/09 to 11/10



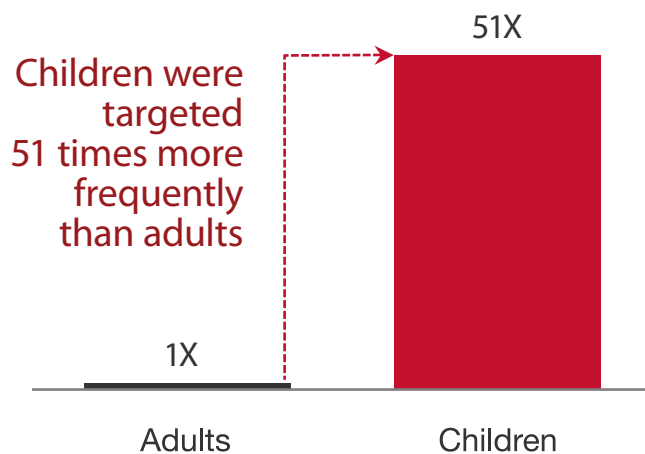
Age Distribution: Possible Cases of Child Identity Theft

Total: 4,311 cases
Note: Age data not available on 121 children



Rate of Child Attacks (10.2%) Vs. Rate of Adult Attacks (0.2%)

The chart to the right is based on 663 attacks against 347,362 adults and 4,311 attacks against 42,232 children, out of a total population of 351,673 (Source: Debix AllClear ID)



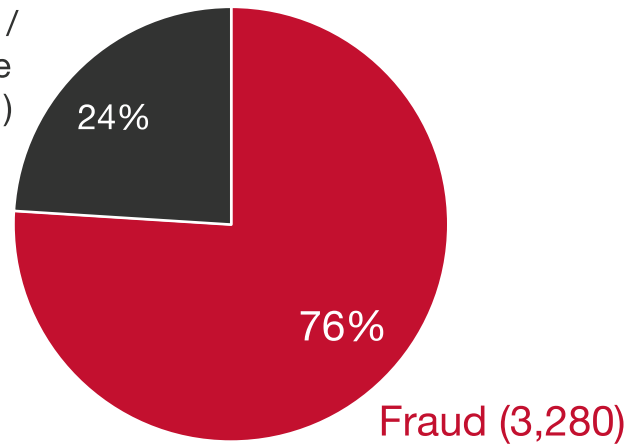
GRAPHS & CHARTS

Child Identity Theft Investigation Results

Total: 4,311

Note: File Contamination/Mixed File indicates events caused by mistakes in reporting, not fraud. The impact to the child is the same as fraud in that the child is unable to utilize their SSN; it is assigned to someone else.

File Contamination/
Mixed File
(1,031)

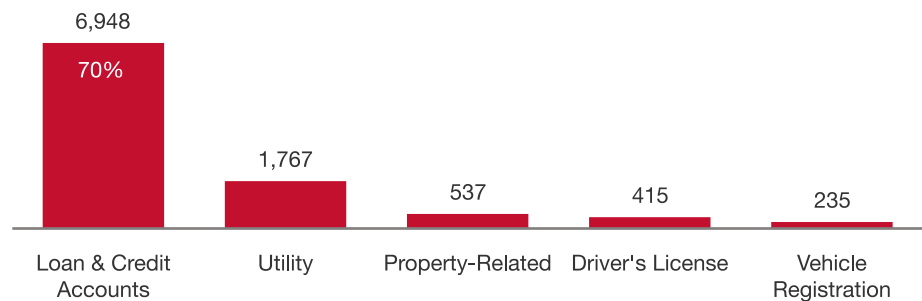


TYPE	ACTUAL	PERCENTAGE
Fraud	3,280	76%
File Contamination/Mixed File	1,031	24%

Types of Records Involved in Child Identity Theft Cases

Total: 4,311

Note: Data includes cases in which child may be affected by more than one type of identity theft, resulting in a higher total of record types than children.



RECORD TYPE	ACTUAL	PERCENTAGE
Loan & Credit Accounts	6,948	70%
Utility	1,767	18%
Property Assessments, Deeds, Mortgages, Foreclosures	537	5%
Driver's License	415	4%
Vehicle Registration	235	2%

IMPLICATIONS AND CONSEQUENCES

Although the data's statistical significance is yet to be determined, it is certainly profoundly significant on a practical, human level to the thousands of children and families who have thus been victimized. Furthermore, from my perspective, having tracked the evolution of cyber crime over two decades, it is only common sense to surmise that the problem goes beyond those breached accounts included in this report, and that there are many thousands more children and their families at risk.

But even if it were only one child, what if that child were yours?

Wouldn't you want to know your child was in foreclosure on a home in another state? Wouldn't you want to know if your child had run up a huge utility bill across town? Wouldn't you want to know that your child had a hunting license? Wouldn't you want to know that your child had a driver's license and a car registered in his or her name?

This AllClear ID data raises some serious questions. Wouldn't you want to know how this happened? And who was responsible? Was it the result of a security breach at a bank or a medical center or an online social media site? Was the perpetrator a petty cyber criminal or an organized cyber crime syndicate operating beyond our borders? Or was the perpetrator perhaps an insider, a family member or a close friend or a childcare worker? What recourse would you have?

Where would you turn? What would the long-term consequences be for you and your child? What would it take to undo the damage done? How would you know such a crime had occurred?

The data raises broader societal questions as well. How widespread is the problem? And is it growing? What should be done governmentally? What should be done organizationally? What should be done within families? There is other evidence that child identity is an issue that demands further study.

CyLab researcher Alessandro Acquisti, co-author of the blockbuster paper, *Predicting Social Security Numbers from Public Data* *Proceedings of the National Academy of Science*, July 7, 2009, explains: "In our investigation of the predictability of Social Security numbers we found evidence of two trends that, combined, are particularly worrisome: criminals are increasingly targeting minors' (even infants') SSNs for identity theft, and the SSNs of younger US residents are much easier to predict than the SSNs of those born before the 1990s. Ultimately, this reminds us that our current identity-verification infrastructure is flawed and vulnerable, as it relies on authentication of numbers too widely available and too easy to compromise."

The Social Security Administration will begin assigning randomized number series <http://www.ssa.gov/employer/randomizationfaqs.html> as of June 25, 2011. Unfortunately, the more predictable Social Security numbers will remain in effect for individuals born before June 25, 2011.

STORIES FROM VICTIMS OF CHILD ID THEFT

The impact of child identity theft can prove substantial to both adults and children. For parents and guardians, it means a lot of time, money, and effort spent to clear the child's name. For children, if it's not discovered in time, it could mean the loss of educational and job opportunities, and starting off adulthood at a serious disadvantage – with someone else's bad credit in your name.

Here are some stories from real-life cases investigated by AllClear ID.

CHRIS FROM ARIZONA

AllClear ID discovered that a 17-year-old girl has over \$725,000 in debt. Chris's daughter's Social Security number was linked to eight different suspects living in border states. The suspects opened 42 open accounts including mortgages, auto loans, credit cards, and bills in collections including medical, credit cards, and utilities.

STATUS: *The case is in progress.*

NATHAN FROM KENTUCKY

Nathan, a 14-year-old, had a credit history that went back more than 10 years. Several credit cards and a foreclosed mortgage were already in his credit history, all from a suspect living in California. The thief established good credit for the first 10 years and was able to finance a \$605,000 home in CA through first and second mortgages. He also used the boy's SSN to open several credit accounts.

Then, the home loans went into default and the bank foreclosed. Additionally, a credit account with over \$2,000 in unpaid charges went into collections. His parents filed a police report and the fraud was assessed at over \$607,000.

"I was very upset; you just don't think someone will use your child's identity," Nathan's father said. "He was only three years old when somebody started using it, and the thought of that made me sick to my stomach."

RESOLUTION: *AllClear ID has restored Nathan's identity and cleared his credit report.*

GREG FROM WASHINGTON

Greg discovered that the misuse of his 18-year-old daughter's Social Security number spanned her entire lifetime, due to an accidental transposition of some of the numbers. Although there was no malice, Greg's daughter still had a credit file using her SSN with over \$325,000 in debt. This issue put their plans for college loans and scholarships in jeopardy.

Greg contacted law enforcement, but the police could not issue a complaint without a credit report. To further complicate matters, the credit agency denied Greg's request to pull a report because the owner was a minor.

"My oldest [daughter] just graduated [from college]," Greg said. "We thought this should be a piece of cake. But especially for my younger daughter, it would have been devastating if it hurt her chances of getting into college."

STORIES FROM VICTIMS OF CHILD ID THEFT

CONTINUED

RESOLUTION: AllClear ID worked with the creditors and cleared the fraudulent accounts from the minor's file, and his daughter was able to file her student loan applications on time.

STEPHANIE FROM IDAHO

AllClear ID discovered that Stephanie, a minor, had a credit file with unpaid debt. The suspect used Stephanie's Social Security number to open two different accounts with mobile phone companies, leaving over \$1,000 in unpaid bills. The unpaid bills had moved into collections and were reported to the credit bureaus – establishing a history of bad credit for Stephanie.

RESOLUTION: AllClear ID worked with Stephanie's parents to file police reports and restore her credit file and identity.

GARY FROM OHIO

AllClear ID learned that 12 people living in border states were using Gary's 17-year-old son's Social Security number to obtain credit, utilities and employment. The thieves racked up over \$58,000 in bad debt including a \$30,000+ car, thousands in an unpaid apartment lease, and over \$23,000 in unpaid credit card bills.

RESOLUTION: AllClear ID worked with law enforcement to identify the suspects, and one was arrested and deported for using an SSN to illegally gain employment.

LINDSEY FROM TEXAS

Lindsey applied for an internship during college, and after accepting an offer, a background check revealed someone was using her Social Security number for employment – and had been for many years – accidentally transposing some of the numbers. Lindsey was classified “unemployable” because she did not “own” her SSN. She spent months resolving issues with credit bureaus, the Social Security Administration, and her employer.

“It was like a full-time job,” Lindsay recalled. “I spent hours and hours doing paperwork, standing in line, and sitting on the phone computers. I’m extremely careful now...I check my credit incessantly.”

RESOLUTION: Her identity was restored and she was able to accept the internship months later.

BELIEVE IT OR NOT...

HERE ARE SOME STRANGER THAN FICTION FACTS EVERY PARENT SHOULD KNOW.

1

Many commercial and public sector entities do not treat Social Security numbers as unique identifiers. It is possible for one SSN to appear on more than one credit file, employment report, criminal history – all mapped to different names.

2

One reason that minor SSNs are so valuable is that there is currently no process for organizations, like an employer or creditor, to check what name and birth date is officially attached to that SSN. As long as an identity thief has a SSN with a clean history, the thief can attach any name and date of birth to it.

3

In some cases, parents can open utility bills under their child's name and SSN to take advantage of the child's clean SSN. Most parents do not intend to harm their child's future, but in fact, this is identity theft.

4

When parents opt their children out of pre-approved credit card offers, it actually creates a credit file for the minor. These files cannot be deleted once created, but can be suppressed upon request of the parent. Parents need to contact each credit bureau regarding suppressing their child's file.

5

When parents try to deal with creditors to clean up issues, the creditors can ask to speak to the child – children as young as 1-2 years old – to verify their identity. Obviously creditors don't get very far using this method!

6

Children with the same name as a parent are frequently mixed up with their parents' credit file, causing them to have to deal with their same-name parents' credit – and any related issues. Mix-ups involving names can occur for different reasons including:

- *Certain information is reported and does not contain a SSN (for example, civil judgments)*
- *Collection agencies have been known to report debts only under name and address*

7

While it is not a requirement for children to obtain SSNs, many hospitals include applying for an SSN as one of the steps for parents to complete before leaving the hospital with their newborn.

RECOMMENDATIONS

As you can see the AllClear ID data raises a lot of disturbing questions; disturbing questions for which substantive answers should be found. Therefore, my first recommendation is that this issue be the subject of academic research to learn more and better evaluate the issues involved. But whether or not these questions are answered, certain steps should be taken, because even a few thousand cases are of concern when we are dealing with the future financial security of children (and perhaps even their current safety), including:

- *Creditors and other businesses need to do a better job of authorizing accounts. There is also a known gap regarding the use of SSN as default national ID. The SSA does not share the names and date of birth with creditors and other authorizing agents, so they are left to guess that the person with the SSN is the rightful owner.*
 - *The ITRC has proposed one way for government agencies and organizations to work together would be “1710 Database” that would hold the name, Social Security number and birth month/year of every child up to the age of 17 years and 10 months. Creditors could check the database to see if credit applicants are using a minor’s information. The database would be run with coordination from the Social Security Administration, state motor vehicle departments, and the three credit reporting agencies, as suggested by Jay Foley, executive director of the ITRC. The database would be of no value to marketers because it wouldn’t contain addresses.*
- *Public service resources that provide guidance for individuals on identity theft prevention and mitigation, etc., should be revised and expanded to incorporate guidance on the particular issue of child identity theft and what is required of parents or guardians.*
- *Organizational strategies for dealing with the threat of identity theft among customers, employees, etc., should be revised and expanded to address the particular issue of child identity*

theft and what is required of the enterprise or agency to deal with the threat.

- *Cyber security awareness and education campaigns in both the public and private sectors should incorporate information on the threat of child identity theft, and what parents and guardians need to know and do.*
- *Parents need to do cyber risk assessment for children who are, or will be going online, and develop risk mitigation plans for their online activities. Child identity theft is among numerous risks and threats that factor into the assessment. Also, just as one monitors one’s own financial identity, through reviewing credit bureau reports, etc., one should monitor the SSN, etc., of any dependent minors.*

AllClear ID
data raises
a lot of
disturbing
questions*

* *disturbing questions for which substantive answers should be found.*

TIPS TO PROTECT YOUR CHILD'S IDENTITY

As a parent or guardian, there are some easy steps to take to lessen the chance of your child falling victim to fraud:

- *Watch for mail in your child's name: If you begin receiving pre-approved credit cards or other unsolicited financial offers in your child's name, it is an indicator that your child may have an open credit file.*
- *Teach your child about identity theft and online safety: Talk to your child about the dangers of sharing personal data online. Children surfing the web are particularly vulnerable to exposing personal information in chat rooms or on social networking sites. Make sure children understand the importance of keeping this data private.*
- *Don't make your child susceptible to "friendly" identity theft: Don't ever use your child's name to open utility or other credit accounts. Protect your child's personal information by keeping it locked up in your home where visitors cannot access it.*
- *Keep your child's sensitive documents safe: Gauge your child's level of responsibility before you share banking and credit information with them, even accounts in their name. Most children will need their Social Security card when they go off to college, but make sure they know to keep their card in a safe place rather than carry it around in a wallet or purse.*
- *Sign up for a free service like AllClear ID that will repair your child's identity at no cost if it is stolen.*

Taking proactive measures to prevent childhood identity theft provides a sense of relief and security that cannot be underestimated. By protecting your child's identity, you are removing the potential for an enormous amount of suffering and hardship when they reach adulthood and encounter the problem on their own. Enrolling in college, beginning a career, starting a family – all become immensely difficult when your child is digging out from under the burden of restoring his or her credit history and reclaiming his or her identity.

TAKING PROACTIVE MEASURES TO PREVENT CHILDHOOD IDENTITY THEFT PROVIDES A SENSE OF RELIEF THAT **CANNOT BE UNDERESTIMATED.**

CONCLUSION

If it were only one child, it would be one too many. But this report documents over four thousand children, and there are likely many more.

This report offers disturbing evidence concerning the nature and appeal of child identity theft, and highlights some real risks and threats, e.g.:

- *10.2% is a significant rate and is dramatically higher than the attack rate for adults. Parents need to think about their children's future, and take the time to look into this frequently overlooked problem*
- *Take steps to protect your children, especially in advance of key financial milestones like student loans, college, first job, apartment rental*
- *Even though some identity theft results from non-malicious things like mixed credit files, the results are the same for parents and children. All child identity theft can result in credit, financial, and identity issues that greatly impact a child's future including school loans, job opportunities, and more*

It also raise some serious questions that should be the subject of a scientific study, e.g., to determine the scope of the problem, and how it is trending. Research needs to be conducted to quantify the scope and trending of the phenomena.

Meanwhile, institutions in both the public and private sector need to address the issue of child identity theft more aggressively.

And whether or not any action is taken on either of these fronts, parents must be proactive.

Put plainly, it is not simply enough to guard your own identity in the 21st Century, you must also guard your child's.

IF IT WERE ONLY ONE CHILD,
IT WOULD BE ONE TOO MANY.
BUT THIS REPORT DOCUMENTS
OVER FOUR THOUSAND CHILDREN,
AND THERE ARE LIKELY MANY MORE.

About CyLab

CarnegieMellonCyLabisaboldandvisionaryeffort, which establishes public-private partnerships to develop new technologies for measurable, secure, available, trustworthy and sustainable computing and communications systems. CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy, as well as security awareness among cyber-citizens of all ages.

Building on more than two decades of Carnegie Mellon leadership in Information Technology, CyLab is a university-wide initiative that involves over fifty faculty and one hundred graduate students from more than six different departments and schools.

Richard Power, a CyLab Distinguished Fellow, writes and speaks on cyber security. From 1995 to 2002, he directed the CSI/FBI Computer Crime and Security Survey, a widely cited study that identified several trends which have come to shape the spectrum of 21st Century cyber risks and threats.

Mr. Power is the author of *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace* (Que) and co-author of *Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21ST Century* (Syngress).

www.cylab.cmu.edu

About AllClear ID

AllClear ID, a new product from Debix, offers free, essential identity protection to everyone. Debix is a pioneer and leading force in the identity protection industry, and using advanced technology created the world's first and only Identity Protection Network.

Fortune 500 companies, universities, state and local governments, healthcare companies, and many other national organizations use Debix to protect their customers, and Debix has protected over 1 million individuals.

Debix and AllClear ID are led by experienced and respected Executives and a renowned Advisory Board. Founded in 2004, Debix is headquartered in Austin, Texas and is privately funded.

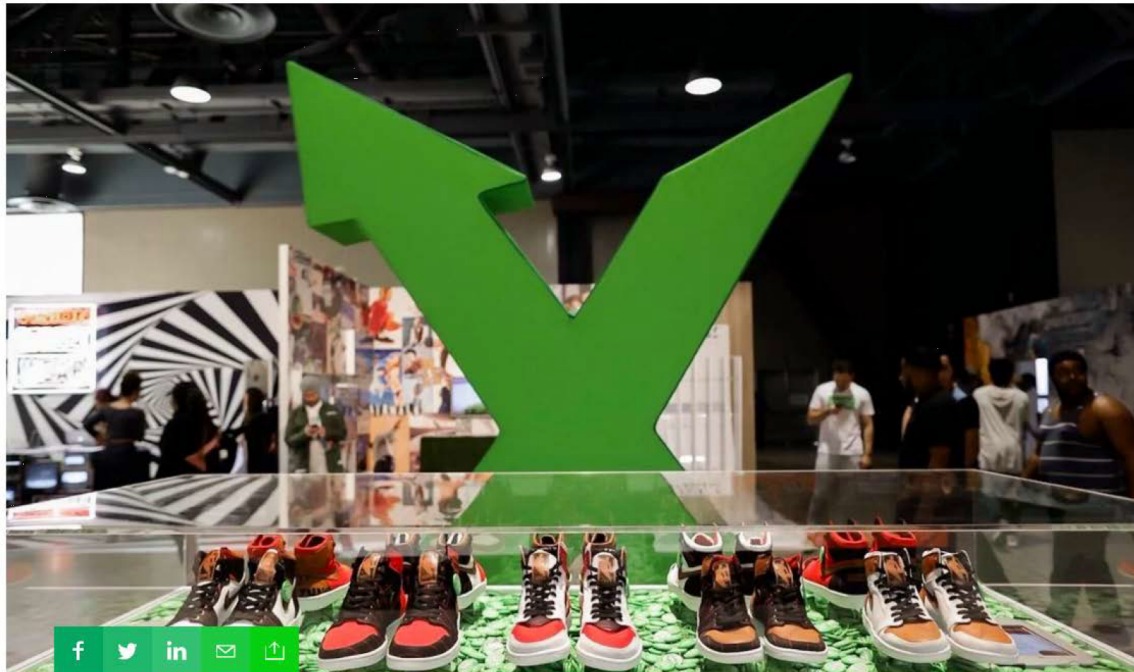
www.AllClearID.com

Exhibit 17

StockX was hacked, exposing millions of customers' data

Zack Whittaker @zackwhittaker / 11:00 am CDT • August 3, 2019

Comment



It wasn't "system updates" as it **claimed**. StockX was mopping up after a data breach, TechCrunch can confirm.

The fashion and sneaker trading platform **pushed out a password reset email** to its users on Thursday citing "system updates," but left users confused and scrambling for answers. StockX told users that the email was legitimate and not a phishing email as some had suspected, but did not say what caused the alleged system update or why there was no prior warning.

A spokesperson eventually told TechCrunch that the company was "alerted to suspicious activity" on its site but declined to comment further.

But that wasn't the whole truth.

An unnamed data breached seller contacted TechCrunch claiming more than 6.8 million records were stolen from the site in May by a hacker. The seller declined to say how they obtained the data.

In a dark web listing, the seller put the data for sale for \$300. One person at the time of writing already bought the data.

The seller provided TechCrunch a sample of 1,000 records. We contacted customers and provided them information only they would know from their stolen records, such as their real name and username combination and shoe size. Every person who responded confirmed their data as accurate.

The stolen data contained names, email addresses, scrambled password (believed to be hashed with the MD5 algorithm and salted), and other profile information — such as shoe size and trading currency. The data also included the user's device type, such as Android or iPhone, and the software version. Several other internal flags were found in each record, such as whether or not the user was banned or if European users had accepted the company's GDPR message.

Under [those GDPR rules](#), a company can be fined up to four percent of its global annual revenue for violations.

When reached prior to publication, neither spokesperson Katy Cockrel nor **StockX** founder Josh Luber responded to a request for comment. A voicemail left on the spokesperson's cell was not returned. A non-attributable statement [published](#) late on Saturday confirmed our reporting, but the company did not answer our specific questions, including why it failed to inform customers when it first learned of the data breach and why it misled customers prior to our reporting.

Neither Luber nor chief executive Scott Cutler have commented on the breach.

Jake Williams, founder of Rendition Infosec, said the company “robbed their users of the chance to evaluate their exposure” by not informing customers of the breach when it happened.

StockX was last month valued [at over \\$1 billion](#) after a \$110 million fundraiser.

Updated with comment from StockX.

StockX admits ‘suspicious activity’ led to resetting passwords without warning



StockX, a popular site for buying and selling sneakers and other apparel, has admitted it reset customer passwords after it was “alerted to suspicious activity” on its site, despite telling users it was a result of “system updates.” “We recently completed system updates on the StockX platform,” said the email to customers sent to TechCrunch ... [Continue reading](#)

 TechCrunch



[Add a Comment](#)

Exhibit 18



EXHIBIT 18

TECH • APPLE

Here's How Much Your Stolen Apple ID Login Costs on the Dark Web

By [Don Reisinger](#) March 7, 2018

Fraudsters can buy [Apple](#) ID credentials pretty cheaply on the so-called Dark Web, a difficult-to-find, shadowy area of the Internet. Stolen logins for other services like [Amazon](#) and [eBay](#) are an even better bargain.

The average price of an Apple ID username and password sold on the Dark Web is \$15.39, making them the most valuable non-financial credentials for sale on the Dark Web, according to [research](#) by the

website Top10TV and earlier reported on... time, eBay accounts go for about \$12 while Amazon and Walmart accounts cost \$10 or less, according to the study.

Hackers use a variety of techniques to steal login credentials from unsuspecting victims. In most cases, those hackers use phishing scams that coax victims into unwittingly handing over their usernames and passwords to high-value accounts by creating fake login pages that look like the real thing.

Hackers sometimes use those credentials themselves to make fraudulent online purchases. In other cases, they're sold over the Dark Web, to people who want to engage in fraud.

Get Data Sheet, Fortune's technology newsletter

In addition to credentials, the Dark Web is also home to illegal content, like unlawful pornography. It's also where people, including whistleblowers and activists, can speak anonymously without government or law enforcement oversight.

Ultimately, financial-related accounts are the most valuable on the Dark Web. PayPal account credentials, for instance, cost \$274, according to the report. The average bank accounts typically sells for \$160.15, which translates to around 10% of the account's available balance. Lastly, debit cards numbers cost \$67.50 while credit cards are \$50.

You May Like

ENTERTAINMENT

Sass as a Strategy: How Netflix's Twitter Became Just as Entertaining as Its Shows and Movies



HEALTH

Former GE CEO Jeff Immelt: To Combat Costs, CEOs Should Run Health Care Like a Business



HEALTH

For Edie Falco, an 'Attitude of Gratitude' After Surviving Breast Cancer





Subscribe & Save

Subscribe today and save 79% off the cover price.

SUBSCRIBE NOW

Sign Up for Our Newsletters

Sign up now to receive FORTUNE's best content, special offers, and much more.

SUBSCRIBE

FORTUNE



40 Under 40

100 Best Companies

Fortune 500

Global 500

Most Powerful Women

World's Greatest Leaders

World's Most Admired Companies

All Rankings

Home

Automotive

Careers

Design

Energy and Environment

Executive Travel

Finance

Commentary

Health

International

Leadership

Luxury

Retail

Sports

Technology

The Ledger

Venture

Photography

Newsletters

Magazine

[FORTUNE Knowledge Group](#)[FORTUNE Branded Content](#)[Fortune Data Store](#)[Fortune Conferences](#)[Customer Service](#)[EU Customer Service](#)[U.S. Privacy Policy](#)[Advertising](#)[About Us](#)[Subscribe](#)[Give a Gift](#)[Online Behavioral Advertising Notice](#)[FORTUNE Website and Application Terms and Conditions of Use](#)

© 2019 Fortune Media IP Limited. All Rights Reserved. Use of this site constitutes acceptance of our [Terms of Use](#) and [Privacy Policy \(Your California Privacy Rights\)](#).

Fortune may receive compensation for some links to products and services on this website. Offers may be subject to change without notice.

Quotes delayed at least 15 minutes. Market data provided by [Interactive Data](#), ETF and Mutual Fund data provided by [Morningstar](#), Inc. Dow Jones Terms & Conditions: <http://www.djindexes.com/mdsidx/html/tandc/indexestandcs.html>.

S&P Index data is the property of Chicago Mercantile Exchange Inc. and its licensors. All rights reserved. [Terms & Conditions](#). Powered and implemented by [Interactive Data Managed Solutions](#). | [EU Data Subject Requests](#)



Exhibit 19

Play Live Radio



LIVE RADIO

SHOWS



TECHNOLOGY

Take A Peek Inside The Market For Stolen Usernames And Passwords

LISTEN · 3:36

PLAYLIST

Download

Transcript

February 22, 2018 · 4:20 PM ET
Heard on All Things Considered



STACEY VANEK SMITH

Our usernames and passwords, to all kinds of websites, are for sale on the dark web. Some, like bank account passwords, are obviously valuable. But hackers can extract money from this information in all kinds of creative ways.

ARI SHAPIRO, HOST:

Most of us have a long list of usernames and passwords to sign into accounts online - eBay, Amazon, Expedia. Those credentials are valuable to hackers, and they're for sale online. Stacey Vanek Smith from our Planet Money team got a look into the market place for stolen passwords.

STACEY VANEK SMITH, BYLINE: I have in front of me a list. It is four and a half pages long, and there are a bunch of company names on it all in alphabetical order. It has banks and airlines and clothing stores. And next to each company name is a price. This list comes from a site on the dark web where people buy and sell stolen usernames and passwords. It is a price list. I got a copy of this list from an investigative journalist named Brian Krebs.

EXHIBIT 19

BRIAN KREBS: Author of the website krebsonsecurity.com.

VANEK SMITH: And you spend a lot of time on the dark web.

KREBS: Yeah. It's kind of an occupational hazard.

VANEK SMITH: Krebs got this particular list from a site called Seller's Paradise.

KREBS: It looks like a pretty nicely indexed e-commerce site where you might go and buy, you know, blenders or whatever it is you want to buy.

VANEK SMITH: But in this case, instead of blenders, people are buying stolen usernames and passwords. Some account information like bank account passwords are obviously valuable. But for others, it can be kind of hard to know why anyone would be interested. There's Costco for 15, David's Bridal for 10. And what are you doing with these passwords if you buy them? So if you - if I buy someone's David's Bridal password for ten bucks, like, what am I doing with it?

KREBS: (Laughter) One of the longest-running scams is the points. They go to use their points, and they're like, I don't have any points; I don't really know what's going on.

VANEK SMITH: So, like, if you buy someone's, like - I'm looking at Best Buy - costs \$13.

KREBS: Right. I could in theory sign into your Best Buy account, change your address, and you would be none the wiser when they send me, you know, a set of \$400 Bose headphones (laughter), you know? Cyber thieves think of really ingenious ways to cash these things out, and cash them out they do.

VANEK SMITH: I mean, how scared should I be about this - about my passwords being out there?

KREBS: Well, that depends. Are you the type of person who reuses the same password all over the place? Then you should...

VANEK SMITH: Let's say that I were that kind of person (laughter). How scared should I be?

KREBS: OK, yeah, I think you should be pretty concerned. I mean...

VANEK SMITH: Really?

KREBS: One of the biggest pieces of feedback I get from, you know, mere mortals who - you know, they take pride in the fact that they don't really understand computers or understand why anybody would want to hack their computer. And I just say, look; you have probably 20, 30 sets of credentials stored in your browser or on your computer that have value. You may not think that they do, but they absolutely do. And this service kind of, you know, puts a pretty fine point on that.

VANEK SMITH: What does this mean - the existence of this marketplace - like, for most of us mere mortals?

KREBS: It means that it's 2018, and we're all still stuck with the stupid passwords.

VANEK SMITH: Krebs thinks we will eventually get to a post-password world. In that world, your phone could essentially become your password. After all, it has tons of data on you, your location, maybe even your fingerprints or your face. And that data can be used to verify your identity. So we'd essentially be carrying our passwords around in our pockets.

But for now, we are stuck with these same old passwords and the same old advice we've been hearing for years. If you want to protect yourself from hackers, be sure to turn on two-factor authentication, and do not reuse the same passwords again and again and again like I do. Stacey Vanek Smith, NPR News.

Copyright © 2018 NPR. All rights reserved. Visit our website terms of use and permissions pages at www.npr.org for further information.

NPR transcripts are created on a rush deadline by Verb8tm, Inc., an NPR contractor, and produced using a proprietary transcription process developed with NPR. This text may not be in its final form and may be updated or revised in the future. Accuracy and availability may vary. The authoritative record of NPR's programming is the audio record.

Sign Up For The NPR Daily Newsletter

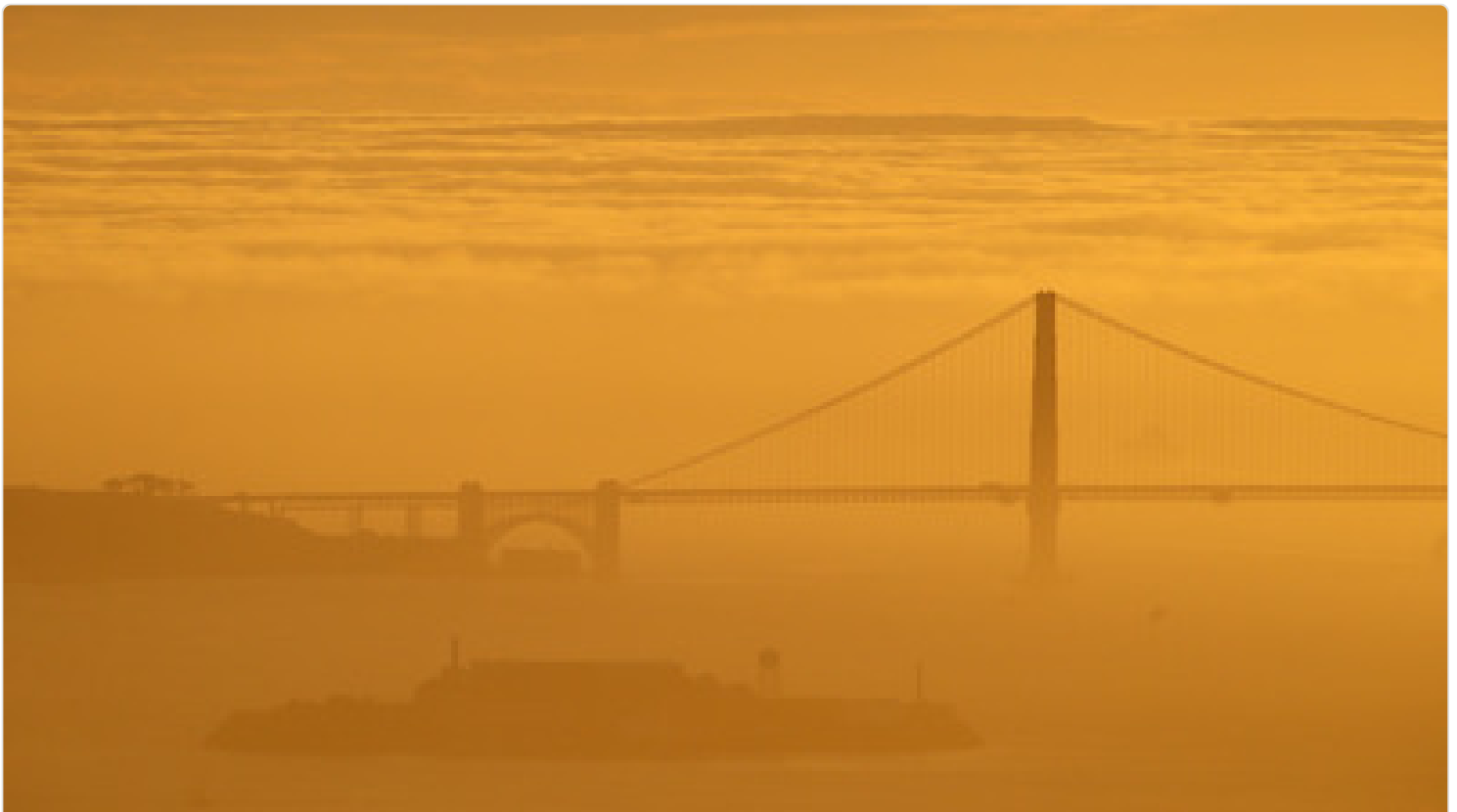
Catch up on the latest headlines and unique NPR stories, sent every weekday.

SUBSCRIBE

By subscribing, you agree to NPR's terms of use and privacy policy.

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

More Stories From NPR



NATIONAL

The End Is Nigh For FogCam, Billed As The Internet's Oldest Running Webcam

**ANIMALS****Maybe The Way To Control Locusts Is By Growing Crops They Don't Like****READ & LISTEN****Home****News****Arts & Life****Music****Podcasts****Programs****CONNECT****Newsletters****Facebook****Twitter****Instagram****Contact****Help****ABOUT NPR****Overview****Finances****People****Press****Public Editor****Corrections****GET INVOLVED****Support Public Radio****Sponsor NPR****NPR Careers****NPR Shop****NPR Events****Visit NPR**

terms of use

privacy

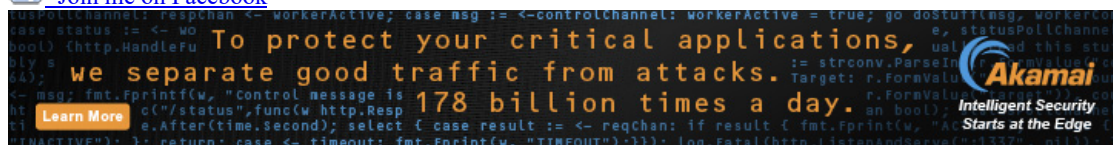
your privacy choices

text only

© 2019 npr

Exhibit 20

Advertisement

[Subscribe to RSS](#)[Follow me on Twitter](#)[Join me on Facebook](#)

Krebs on Security

In-depth security news and investigation



- [About the Author](#)
- [Advertising/Speaking](#)

18
Dec 17

The Market for Stolen Account Credentials

Past stories here have explored the myriad [criminal uses of a hacked computer](#), the various ways that [your inbox can be spliced and diced](#) to help cybercrooks ply their trade, and [the value of a hacked company](#). Today's post looks at the price of stolen credentials for just about any e-commerce, bank site or popular online service, and provides a glimpse into the fortunes that an enterprising credential thief can earn selling these accounts on consignment.

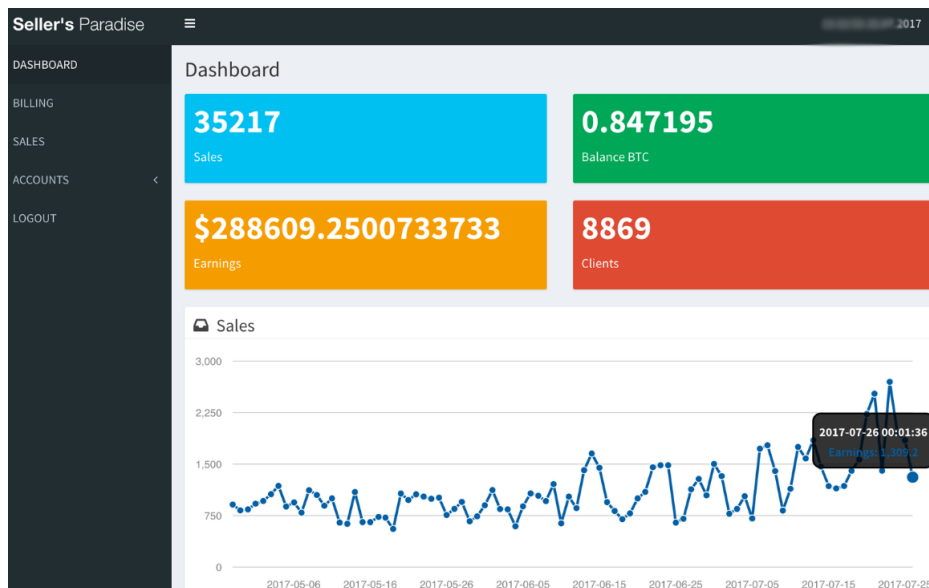
Not long ago in Internet time, your typical cybercriminal looking for access to a specific password-protected Web site would most likely visit an underground forum and ping one of several miscreants who routinely leased access to their "bot logs."

These bot log sellers were essentially criminals who ran large botnets (collections of hacked PCs) powered by malware that can snarf any passwords stored in the victim's Web browser or credentials submitted into a Web-based login form. For a few dollars in virtual currency, a ne'er-do-well could buy access to these logs, or else he and the botmaster would agree in advance upon a price for any specific account credentials sought by the buyer.

Back then, most of the stolen credentials that a botmaster might have in his possession typically went unused or unsold (aside from the occasional bank login that led to a juicy high-value account). Indeed, these plentiful commodities held by the botmaster for the most part were simply not a super profitable line of business and so went largely wasted, like bits of digital detritus left on the cutting room floor.

But oh, how times have changed! With dozens of sites in the underground now competing to purchase and resell credentials for a variety of online locations, it has never been easier for a botmaster to earn a handsome living based solely on the sale of stolen usernames and passwords alone.

If the old adage about a picture being worth a thousand words is true, the one directly below is priceless because it illustrates just how profitable the credential resale business has become.



This screen shot shows the earnings panel of a crook who sells stolen credentials for hundreds of Web sites to a dark web service that resells them. This botmaster only gets paid when someone buys one of his credentials. So far this year, customers of this service have purchased more than 35,000 credentials he's sold to this service, earning him more than \$288,000 in just a few months.

The image shown above is the wholesaler division of "**Carder's Paradise**," a bustling dark web service that sells credentials for hundreds of popular Web destinations. The screen shot above is an earnings panel akin to what you would see if you were a seller of stolen credentials to this service — hence the designation "**Seller's Paradise**" in the upper left hand corner of the screen shot.

This screen shot was taken from the logged-in account belonging to one of the more successful vendors at Carder's Paradise. We can see that in just the first seven months of 2017, this botmaster sold approximately 35,000 credential pairs via the Carder's Paradise market, earning him more than \$288,000. That's an average of \$8.19 for each credential sold through the service.

Bear in mind that this botmaster *only makes money based on consignment*: Regardless of how much he uploads to Seller's Paradise, he doesn't get paid for any of it unless a Carder's Paradise customer chooses to buy what he's selling.

Fortunately for this guy, almost 9,000 different customers of Carder's Paradise chose to purchase one or more of his username and password pairs. It was not possible to tell from this seller's account how many credential pairs total that he has contributed to this service which went unsold, but it's a safe bet that it was far more than 35,000.

[A side note is in order here because there is some delicious irony in the backstory behind the screenshot above: The only reason a source of mine was able to share it with me was because this particular seller re-used the same email address and password across multiple unrelated cybercrime services].

Based on the prices advertised at Carder's Paradise (again, Carder's Paradise is the *retail/customer side of Seller's Paradise*) we can see that the service on average pays its suppliers about half what it charges customers for each credential. The average price of a credential for more than 200 different e-commerce and banking sites sold through this service is approximately \$15.

NEWS

CREDIT CARDS <

SSN <

SIN <

SSN W/ REPORT <

CREDIT REPORTS

ACCOUNTS ▾

BUY ACCOUNTS

ORDERS

BIN BASE

LOGOUT

Accounts

Verizonwireless.com(25) Select

Account	Price	Available			
Verizonwireless.com	\$12	25	- 1 +	Buy	
Airbnb.com	\$15	32	- 1 +	Buy	
Ebay.com	\$10	37	- 1 +	Buy	
Fido.ca	\$20	93	- 1 +	Buy	
Chase.com	\$25	15	- 1 +	Buy	
Citibank	\$25	17	- 1 +	Buy	
Navyfederal.org	\$60	0	- 1 +	Request	
Target.com	\$10	44	- 1 +	Buy	
Wellsfargo.com	\$25	9	- 1 +	Buy	
Rbcroyalbank.com	\$65	3	- 1 +	Buy	
BB&T.com	\$25	22	- 1 +	Buy	
TDBank.com online rout+acc	\$25	0	- 1 +	Request	
Ally.com	\$25	33	- 1 +	Buy	

Part of the price list for credentials sold at this dark web ID theft site.

Indeed, fifteen bucks is exactly what it costs to buy stolen logins for **airbnb.com**, **comcast.com**, **creditkarma.com**, **logmein.com** and **uber.com**. A credential pair from **AT&T Wireless** — combined with access to the victim's email inbox — sells for \$30.

The most expensive credentials for sale via this service are those for the electronics store **frys.com** (\$190). I'm not sure why these credentials are so much more expensive than the rest, but it may be because thieves have figured out a reliable and very profitable way to convert stolen fry's.com customer credentials into cash.

Usernames and passwords to active accounts at military personnel-only credit union **NavyFederal.com** fetch \$60 apiece, while credentials to various legal and data aggregation services from **Thomson Reuters** properties command a \$50 price tag.

The full price list of credentials for sale by this dark web service is available in [this PDF](#). For CSV format, [see this link](#). Both lists are sorted alphabetically by Web site name.

This service doesn't just sell credentials: It also peddles entire identities — indexed and priced according to the unwitting victim's [FICO score](#). An identity with a perfect credit score (850) can demand as much as \$150.

Carder's Paradise

SUPPORT BILLING

NEWS

CREDIT CARDS <

SSN <

SIN <

SSN W/ REPORT ▾

HIGH SCORE

MEDIUM SCORE

ORDERS

CREDIT REPORTS

ACCOUNTS <

BIN BASE

LOGOUT

High Score SSN with Credit Report

SCORE	SEX	DOB	ZIP	STATE	CITY	PRICE	
850	M	11/23/1957	55428	MN	NEW HOPE	\$150	Buy
849	F	10-08-1956	31216	GA	MACON	\$145	Buy
847	F	04-09-1957	31210	GA	MACON	\$145	Buy
842	F	06-05-1957	31210	GA	MACON	\$145	Buy
842	M	08-16-1956	31211	GA	MACON	\$145	Buy
840	F	06-23-1956	31220	GA	MACON	\$145	Buy
840	F	11/21/1969	55337	MN	BURNSVILLE	\$135	Buy
827	M	4/13/1959	55446-2117	MN	PLYMOUTH	\$125	Buy
825	F	04-03-1957	31204	GA	MACON	\$120	Buy
824	M	03-02-1956	31204	GA	MACON	\$120	Buy

Stolen identities with high credit scores fetch higher prices.

And of course this service also offers the ability to pull full credit reports on virtually any American — from all three major credit bureaus — for just \$35 per bureau.

It costs \$35 through this service to pull someone's credit file from the three major credit bureaus.

Plenty of people began freaking out earlier this year after [a breach at big-three credit bureau Equifax](#) jeopardized the Social Security Numbers, dates of birth and other sensitive data on more than 145 million Americans. But as I have been trying to tell readers for many years, this data is broadly available for sale in the cybercrime underground on a significant portion of the American populace.

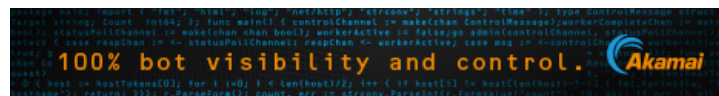
If the threat of identity theft has you spooked, place a freeze on your credit file and on the file of your spouse (you may even be able to [do this for your kids](#)). Credit monitoring is useful for letting you know when someone has stolen your identity, but these services can't be counted on to stop an ID thief from opening new lines of credit in your name.

They are, however, useful for helping to clean up identity theft after-the-fact. This story is already too long to go into the pros and cons of credit monitoring vs. freezes, so I'll instead [point to a recent primer on the topic](#) and urge readers to check it out.

Finally, it's a super bad idea to re-use passwords across multiple sites. KrebsOnSecurity this year has written about multiple, competing services that sell or sold access to billions of usernames and passwords exposed in high profile data breaches at places like LinkedIn, Dropbox and Myspace. Crooks pay for access to these stolen credential services because they know that a decent percentage of Internet users recycle the same password at multiple sites.

One alternative to creating and remembering strong, lengthy and complex passwords for every important site you deal with is to outsource this headache to [a password manager](#). If the online account in question allows [2-factor authentication \(2FA\)](#), be sure to take advantage of that.

Two-factor authentication makes it much harder for password thieves (or their customers) to hack into your account just by stealing or buying your password: If you have 2FA enabled, they also would need to hack that second factor (usually your mobile device) before being able to access your account. For a list of sites that support 2FA, check out [twofactorauth.org](#).



Tags: [carder's paradise](#), [credit freeze](#), [seller's paradise](#), [twofactorauth.org](#)

This entry was posted on Monday, December 18th, 2017 at 2:13 pm and is filed under [A Little Sunshine](#), [Web Fraud 2.0](#). You can follow any comments to this entry through the [RSS 2.0](#) feed. Both comments and pings are currently closed.

34 comments

1. ASitte
[December 18, 2017 at 3:07 pm](#)

Excellent research and article Brian. Your efforts are much appreciated by all of us.

More and more, I am beginning to despise logon/password credentials.

o Victoriano
[December 18, 2017 at 4:33 pm](#)

Wait for SQL! <https://www.grc.com/sqrl/sqrl.htm> It'll change the world!! (I hope) 😊

▪ jbmartin6
[December 19, 2017 at 8:52 am](#)

A lot of websites in China already use this sort of system for logins using a smart phone, such as with WeChat/QQ. I don't know anything about how secure the back end might be.



■ *ASitte*

[December 19, 2017 at 1:44 pm](#)

Although SQRL could be helpful in some use cases, where identity assurance is necessary I feel it falls a little flat.

Many crucial use cases require identity assurance: “the ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity.”

https://en.wikipedia.org/wiki/Identity_assurance

I do not have a strong belief that SQRL can effectively address identity assurance requirements for many organizations or purposes... yet.

SQRL probably could achieve the identity assurance requirements if the model provided a method/capability of third party verification of the claimant identity, but from what I can determine SQRL is focused on avoiding that kind of thing.

I see SQRL as a great idea, but only one aspect of a very complex problem.



■ *Olly*

[December 20, 2017 at 5:43 pm](#)

Surely, a site can use SQRL for login and then verify the user's identity in a conventional way such as via credit card if it needs to.



2. *Winston*

[December 18, 2017 at 3:16 pm](#)

“Plenty of people began freaking out earlier this year after a breach at big-three credit bureau Equifax jeopardized the Social Security Numbers, dates of birth and other sensitive data on more than 145 million Americans. But as I have been trying to tell readers for many years, this data is broadly available for sale in the cybercrime underground on a significant portion of the American populace.”

I think the “freaking out” justifiably came from the realization that if one's complete personal data hadn't previously been available to such sites, it was probably much more likely to be so after the completely inexcusable Equifax fiasco.



○ *Brian Krebs*

[December 18, 2017 at 3:22 pm](#)

Meh. *IF* the data was stolen by or has made its way into the hands of people who would sell it to fraudsters, the worst it would do for most people is refresh the data on them that is already for sale on cybercriminal shops like the one in this post.



3. *Karan Saini*

[December 18, 2017 at 3:37 pm](#)

Interesting article. It is surprising that Amazon credentials were sold for a much more cheaper rate than Frys, since crooks have pretty much known for years that it's possible to SE Amazon into sending replacements for expensive items or refunds in the form of gift cards.



○ *Brian Krebs*

[December 18, 2017 at 3:45 pm](#)

Well, I think it's important to keep in mind that this dark web site is one of many, and that they all have different prices for things. It could be that Seller's Paradise has a fair number of customers who are looking to buy frys.com accounts, and so they have increased the price as the demand has increased. But again, that's speculation.



4. *Felix*

[December 18, 2017 at 4:33 pm](#)

Brian, my Macbook was accessed by an unauthorized person while getting fixed at a 3rd party Apple supplier. This person changed my passwords for numerous financial websites. I quickly updated those said passwords, but wondering if there is a way I could find out if my credentials are being sold online? Thanks for any input.



5. *Ben*

[December 18, 2017 at 5:11 pm](#)

Frys could be popular to buy crypto-mining rig components...



o vb

[December 18, 2017 at 6:37 pm](#)

I'm guessing that Frys must have an easy method to purchase gift cards. Gift cards can be re-sold for hard cash.



o Lack Thereof

[December 19, 2017 at 3:23 am](#)

Fry's also sells name-brand large appliances, which are both valuable and extremely easy to resell.



▪ CTB

[December 19, 2017 at 9:54 am](#)

Exactly. What would be really interesting to know is the success rate of the credentials.

Brian does "Carder's Paradise" have an Amazon style rating system for stolen credentials? I would think the reviews would be an interesting if not amusing read.



▪ Gramon

[December 19, 2017 at 12:17 pm](#)

I second that request. I imagine a certain percentage of these credentials are already void by the time they get sold, and that percentage only goes up for every day that goes by.

So do the sellers offer a guarantee or return policies? I know, right? I'm shaking my head as I write this...



▪ CTB

[December 20, 2017 at 10:29 am](#)

If I am remembering correctly, one of Brian's previous posts on dark web sites that sell cards and related data the sellers do offer some sort of guarantee on the stolen cards. They also sell them by zip/postal code so that the buyer can "buy/shop" local with a better chance of going undetected by Issuers. I slight digression from the topic at hand but you get my point. These guys are running serious businesses with all the same concerns and business practices of legitimate businesses so it wouldn't surprise me if they had customer testimonials.



6. DeeAitch

[December 18, 2017 at 5:47 pm](#)

I like that I'm able to share Brian's articles with my parents who are VERY far from the internet generation. The same threats I have warned them about for years are suddenly real when they read one of these articles. Much appreciated.



7. vb

[December 18, 2017 at 6:35 pm](#)

It's not clear if they are selling Dropbox creds with clear text passwords or hashed passwords.

Because if the Dropbox passwords are from the 2012 breach, the passwords taken were hashed and salted with bcrypt, at worst some older ones were hashed with SHA-1.




o Brian Krebs

[December 18, 2017 at 6:41 pm](#)

VB – I'm going to guess you missed the part about how most of these credentials are being sold into the service for resale by people running large botnets of hacked computers. Those botnets are powered by malware that completely subverts the security of the Web browser on the infected PC, such that any usernames and passwords submitted on a Web login form get stripped out *prior to being encrypted as part of the browser session*.

Hence, what's being sold here are credentials stolen directly from bot-infected computers — not credentials stolen en-masse from some public data breach at a big company.

8.  *Jurk Juggler*
[December 18, 2017 at 7:06 pm](#)


@DeeAitch – IMO Brian knows how to write something intrinsically designed for people who would *wish* to read it rather than just “a piece” – The fact that he does so and puts it out for free without paywall to end readers says a lot to me about his intentions. Plus he’s put himself out there to be targeted by the goon squad, as documented in entertaining detail.

So a deserved golf clap! Jolly good Brian.

Look up NavyFederal.com and all their ATM’s/branches seem to be in the Hayward stretch – and if you know Fry’s they’re all in the San Jose – Concord – P.alto corridor. Hmm.

9.  *IRS iTunes Card*
[December 18, 2017 at 11:02 pm](#)


Very interesting article !

10.  *Robin M. Holt*
[December 19, 2017 at 9:23 am](#)


I have had my credit reports locked since 2007, always used unique usernames, email addresses (thanks to an email hosting provider I use), and passwords generated on a Linux system with a TRNG using cat, tr, and cut so I can audit the tools to make sure everything is exactly as I would assume.

Now that I read this article, I would love to do an audit, but I have no idea how to find there nefarious sites and/or if accessing information about myself, given it involves payments for illegal services, is even legal.

If you could consider doing a post some time about doing an audit and its legal implications, I would appreciate the information greatly.

11.  *John Pavon*
[December 19, 2017 at 10:06 am](#)


I noticed that peoples names are being hacked and used buy some company to send out unwanted emails that want the end user you to open the email because you are familiar with the name so you would open it thinking its from your relative or best friend? Facebook refuses to listen to me, all the TV and Radio news refuses to mention it? Can you help?

12.  *Wladimir Palant*
[December 19, 2017 at 10:09 am](#)


I’m all for using a password manager. Trouble is, few password managers are really secure. Last Pass for example is often recommended but definitely not safe to use. I published an in-depth analysis a while ago under <https://security.stackexchange.com/a/137307>. Since then, more security issues have been reported, again affecting the same weak spots.

An offline password manager like KeePass is much easier to secure but not too comfortable to use. I suspect that people will often install one of the browser extensions available for KeePass integration. I looked into two of those – one was fairly basic and secure, the other more extensive and likely not safe to use.


So it’s not really clear how a “mere mortal” is supposed to choose a good password manager that won’t expose you to the risk of leaking all passwords at once. Maybe I should look into Dashlane, haven’t heard about that one before.

- o  *Matt*
[December 21, 2017 at 9:07 am](#)


KeePass has had issues just like many other password managers. LastPass, unlike a lot of other software companies responds to security issues pretty quickly. If you use a password manager and 2FA on sites that allow it you will be in pretty good shape. Of course someone can always pop your PC/browser or whatever and steal what you are entering, but at that point you are owned. It doesn’t matter if you type your passwords from memory or use a manager. For most people KeePass being offline only is a serious issue because the average person will not back it up.

-  *Wladimir Palant*
[December 22, 2017 at 3:18 am](#)


LastPass is good at PR, that’s it – you seem to have bought it. Their incident response mostly consists of downplaying the issue, that’s far from ideal.

-  [Wladimir Palant](#)
[December 22, 2017 at 8:00 am](#)


2FA won't help you if the browser extension is vulnerable and leaks all data to arbitrary websites after you already authenticated.

-  [Taylor](#)
[December 26, 2017 at 11:45 am](#)

That would indeed be true, but once you use the token for the 2FA, it will not work again for the same authentication. So even if they do have the password, without a way to get that token to proc again and go to them before you use it, it is useless.

13.  [theckel](#)
[December 19, 2017 at 10:24 am](#)

I would imagine a large part of the price variance on these (like Fry's vs Amazon – as people have noted) is based on the presence or lack thereof of 2-factor authentication in addition to other account security checks/notices. As such, a more expensive, less secure account may have a higher “success” rate than several [potentially] more secure accounts.

14.  [cxd](#)
[December 19, 2017 at 11:50 am](#)


I'm curious why Amazon credentials are not more of a focal point. There are simple merchandise scams of course, but it seems to me that the real criminal money, especially these days, is in getting someone's Amazon account, setting up AWS, and mining bitcoins. I got hit with an absurd \$6700 bill which happened from redirections from a manipulated search engine result for “aws” (browser logs reported). (N.B. never click on a search engine link if it's important.) Why would criminals go through that trouble when they can buy credentials so cheap and Amazon does so little to cap such absurd use?

Thanks to you Brian for great reporting!

-  [BeBopp](#)
[December 20, 2017 at 11:14 am](#)


Cxd —

Can you provide a few more details?? Sounds fairly important to other readers.... Brian? Future article?

15.  [Mike](#)
[December 20, 2017 at 1:15 pm](#)

“They are, however, useful for helping to clean up identity theft after-the-fact.”

Just an editor's note: you don't hyphenate commonly used prepositional phrases such as “after the fact” when used this way. The phrase is hyphenated when the whole phrase is used as an adjective, such as, “an after-the-fact explanation.” It gets hyphenated as an adjective because its normal, non-hyphenated use is adverbial.

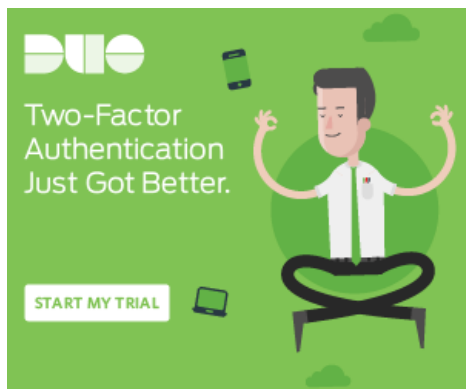
16.  [Nixon](#)
[January 2, 2018 at 12:19 am](#)

Awesome Article Brian!!! I search but didn't found the site which you posted here. how to experience with my own eyes?any address?

-  [Dixon](#)
[January 4, 2018 at 4:24 pm](#)

Must be 18+

Advertisement



•

• Mailing List

[Subscribe here](#)

•

A promotional graphic for Akamai. The background is a dark grey with a light grey grid pattern. Overlaid on the grid is a large, bold, white text that reads "Which 1 phishing variant was responsible for \$1.2 billion in losses?". Below this text is a large, orange button with the text "Download Report". At the bottom of the graphic is the Akamai logo, which consists of a stylized blue and orange 'A' followed by the word "Akamai" in a bold, sans-serif font. Below the logo is the tagline "Intelligent Security Starts at the Edge". The top of the graphic features a snippet of code in a light grey font, which appears to be a Go program. The code is partially obscured by the text and the button.

• Recent Posts

- [The Rise of "Bulletproof" Residential Networks](#)
- [Meet Bluetana, the Scourge of Pump Skimmers](#)
- [Patch Tuesday, August 2019 Edition](#)
- [SEC Investigating Data Leak at First American Financial Corp.](#)
- [iNSYNQ Ransom Attack Began With Phishing Email](#)

•

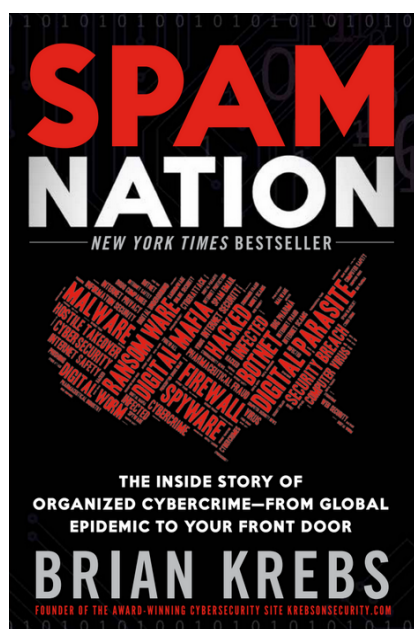
• All About Skimmers



Click image for my skimmer series.



• Spam Nation



A New York Times Bestseller!



• The Value of a Hacked PC



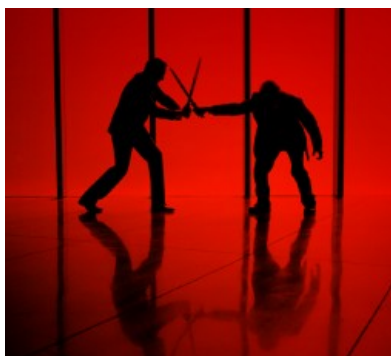
Badguy uses for your PC

• Tools for a Safer PC



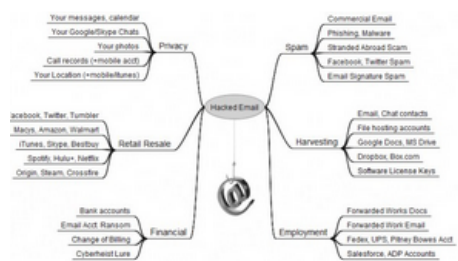
Tools for a Safer PC

• The Pharma Wars



Spammers Duke it Out

• Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

• eBanking Best Practices



eBanking Best Practices for Businesses

• Most Popular Posts

- [Sextortion Scam Uses Recipient's Hacked Passwords](#) (1076)

- o [Online Cheating Site AshleyMadison Hacked](#) (798)
- o [Sources: Target Investigating Data Breach](#) (620)
- o [Cards Stolen in Target Breach Flood Underground Markets](#) (445)
- o [Reports: Liberty Reserve Founder Arrested, Site Shuttered](#) (416)
- o [Was the Ashley Madison Database Leaked?](#) (376)
- o [True Goodbye: 'Using TrueCrypt Is Not Secure'](#) (363)
- o [Who Hacked Ashley Madison?](#) (361)
- o [Following the Money, ePassporte Edition](#) (353)
- o [U.S. Government Seizes LibertyReserve.com](#) (315)

• Category: Web Fraud 2.0

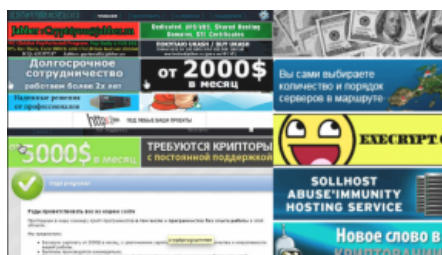


Innovations from the Underground



ID Protection Services Examined

• Is Antivirus Dead?



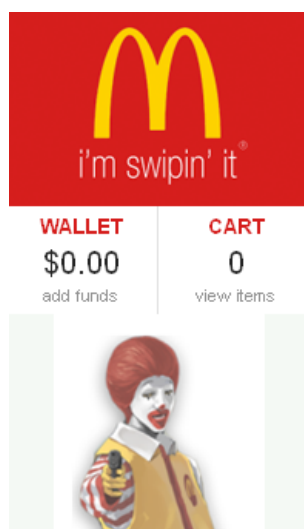
The reasons for its decline

• The Growing Tax Fraud Menace



File 'em Before the Bad Guys Can

• Inside a Carding Shop



A crash course in carding.

• Beware Social Security Fraud



At each stage of your life, **my Social Security** is for you. Your personal online **my Social Security** account is a valuable source of information beginning in your working years and continuing throughout the time you receive Social Security benefits.

If you receive benefits or have Medicare, you can:

Use a **my Social Security** online account to:

- Get your **benefit verification letter**;
- Check your benefit and payment information and your earnings record;
- Change your address and phone number; and
- Start or change direct deposit of your benefit payment.

Sign up, or Be Signed Up!

• How Was Your Card Stolen?



Finding out is not so easy.

- **Krebs's 3 Rules...**



...For Online Safety.

© 2019 Krebs on Security. Powered by [WordPress](#). [Privacy Policy](#).

Exhibit 21

Best VPN Mobile Industry Best Web Hosting Best Antivirus Security Best Website Builders Best WordPress

TechRadar is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. [Learn more](#)

Nearly 620 million stolen accounts for sale on dark web

By Mike Moore February 12, 2019 Internet

Number of popular sites have user account information stolen and put up for sale.



(Image credit: Shutterstock)

(Image credit: Shutterstock)

Hundreds of millions of stolen online accounts have been found for sale on the [Dark Web](#).

As many as 617 million accounts from 16 popular websites were detected on the Dream Market website on the notorious Tor network.

RECOMMENDED VIDEOS FOR YOU...

techradar.pro

The Top iOS 13 Public Beta Features

EXHIBIT 21

00:05 / 01:47

For the equivalent of \$20,000 in Bitcoin, hackers could get hold of information including account names, email addresses and passwords - although the latter appear to still be hashed, meaning they still require cracking to be able to be used.

- [Best antivirus](#) of 2019
- Why risk-based security is the key to [driving business value](#) in 2019
- How AI can [prevent a Marriott situation](#) from happening again

Stolen accounts for sale

The haul was highlighted to [The Register](#) by the apparent seller, who provided the site with sample records from the collection.

Some of the worst hit sites were Dubsmash (162 million accounts) MyFitness Pal (151 million) and MyHeritage (92 million), with other victims including dating sites, ecommerce stores and gaming studios.

The database was put up for sale by a single hacker, who according to The Register, claimed the information was stolen during 2018. The hacker cracked security vulnerabilities within web apps to be able to deploy remote-code execution, allowing them to easily extract user account data.

The Register contacted MyHeritage to see if the sample information it was provided was real, as the site had suffered a data breach last year, with the genealogy site confirming the data was legitimate.

The hacker claimed to already have secure one buyer, with more potentially to come.

- Keep your data private online with the [best VPN](#) of 2019

SEE MORE INTERNET NEWS ►

MORE ABOUT INTERNET

LATEST

[READ MORE ►](#)

Capital One hack may have been bigger than thought

By [Mike Moore](#) August 15, 2019

[READ MORE ►](#)

Four top web hosting hacks to boost SEO

By [Marc Woodhead](#) August 14, 2019

[READ MORE ►](#)

Moscow wants to be a model smart city; this is how they plan to achieve it

By [TechRadar Pro](#) August 14, 2019

[READ MORE ►](#)

Advertisement



Free to Access, Read and Share
Build Your First Website eBook

In association with GoDaddy

Techradar Pro has teamed up with GoDaddy to produce a website-hosting tips eBook, looking at how to plan your website, picking the right domain name and great ways to promote your website.

READ MORE TODAY ►

Have a read and let us know what you think. The aim is to inform and provide insight to those interested in building

Nearly 620 million stolen accounts for sale on dark web | Tech Radar

their first real website.

techradar.pro

Advertisement

MOST POPULAR

MOST SHARED



1 **UFC 241 live stream: how to watch Cormier vs Miocic 2 (and the rest) from anywhere tonight**

2 **iPhone 11R release date, price, news and leaks**

3 **The best laptop 2019: our pick of the 15 best laptops you can buy this year**

Advertisement

TechRadar is part of Future US Inc, an international media group and leading digital publisher. **Visit our corporate site.**

[About Us](#)[Terms and conditions](#)[Privacy policy](#)[Cookies policy](#)[Advertise with us](#)[Web notifications](#)

© Future US, Inc. 11 West 42nd Street, 15th Floor, New York, NY 10036.

Powered by OptinMonster

Exhibit 22

Home > News > Security > Database from StockX Hack Sold Online, Check If You're Included

Database from StockX Hack Sold Online, Check If You're Included

By **Lawrence Abrams**

August 11, 2019

09:37 PM

0



A database reportedly containing 6,840,339 unique user accounts from the recent StockX data breach is being sold and distributed online. Bad actors have stated that they have already begun to decrypt the passwords and it is expected for this information to be used in future attacks.

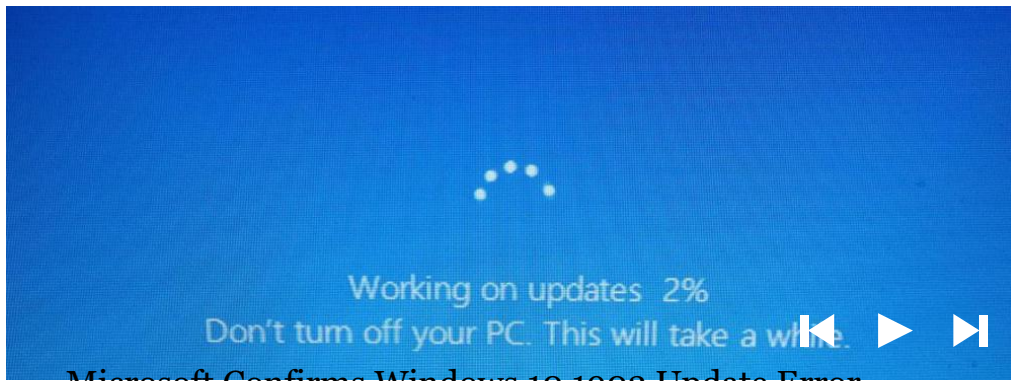
Last week it came to light that StockX was hacked and an attacker stole user account information. This information included user names, email addresses, addresses, shoe size, purchase history, and encrypted passwords.

Over the weekend, data breach site Have I been Pwned added the StockX database to their site so that users can check if their emails are part of the breach. This database was shared by password crashing site Dehashed.com and consists of 6,840,339 accounts containing "unique email addresses, names, physical addresses, purchases and passwords stored as salted MD5 hashes".

TOP ARTICLES 1/5



EXHIBIT 22



Microsoft Confirms Windows 10 1903 Update Error Working on Fix

[READ MORE >>](#)

StockX Information on Have I Been Pwned

To check if your information has been exposed as part of this breach, you can enter your email address into <https://haveibeenpwned.com/> and it will report if your information has been found in any breaches, including the StockX one.

Database being sold on hacker forums

Security researcher Jim Scott, who has assisted HIBP in finding data dumps in the past, has told BleepingComputer that the StockX database was originally being sold on the Apollon marketplace for \$300.

Since then, the username and password combinations have been found being distributed on underground hacker forums for as little as \$2.15.

As these prices make the database essentially free, it will now be in the hands of numerous attackers who will try to crack the passwords.

For those who do not want to deal with the decrypting of the passwords, one person has allegedly decrypted 367,000 accounts from the database and is selling them for \$400.

What should you do?

Now that the database dump is easily available for relatively nothing, the account credentials will be used in credential stuffing attacks.

A credential stuffing attack is when attackers compile usernames and passwords that were leaked from different company's data breaches and use those credentials to try and gain access to accounts at other sites. This type of attack works particularly well against users who use the same password at every site.

If your StockX password is also used at other sites, you should immediately change your passwords at all sites that it is used. By not doing so, you stand the risk of having those accounts compromised as well.

Related Articles:

[StockX Hack Exposes Personal Information of Customers](#)

[CafePress Data Breach Exposes Personal Info of 23 Million Users](#)

[Slack Resets Account Passwords Compromised During 2015 Hack](#)

[Steam Accounts Being Stolen Through Elaborate Free Game Scam](#)

[Google Estimates 1.5% of Web Logins Exposed in Data Breaches](#)

[DATA BREACH](#) [DATA DUMP](#) [HACK](#) [STOCKX](#)

LAWRENCE ABRAMS

Lawrence Abrams is the creator and owner of BleepingComputer.com. Lawrence's area of expertise includes malware removal and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

[< PREVIOUS ARTICLE](#)[NEXT ARTICLE >](#)

Post a Comment**Community Rules**

You need to login in order to post a comment

Login

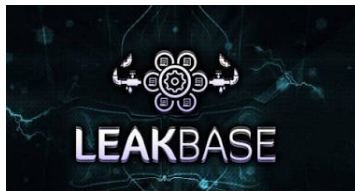
Not a member yet? [Register Now](#)

You may also like:



**Future Branches
Conference - Topics &
Speakers - Get Agenda**

Ad [futurebranches.wbresearch.com](#)



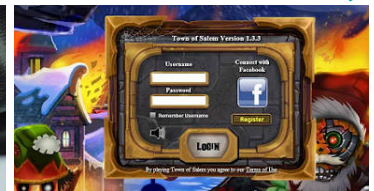
**Leakbase.pw Hacked
Password Service Goes
Dark**

[bleepingcomputer.com](#)



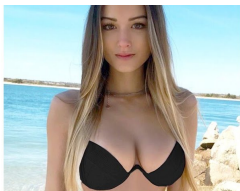
**Police Say To Carry
This**

Ad [trysafepersonalalarm.com](#)



**27% of Passwords
From Town of Salem
Breach Already...**

[bleepingcomputer.com](#)



2019 Sexiest Bikinis

Ad [Bikini Clearance Sale](#)



**Hacker Wants \$50K
From Hacker Forum or
He'll Share Stolen...**

[bleepingcomputer.com](#)



**Microsoft Bug is
Deactivating Windows
10 Pro Licenses and...**

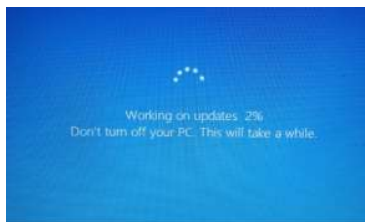
[bleepingcomputer.com](#)



**FBI Seize Dee
For Taking
Commissions**

[bleepingcomputer.com](#)

POPULAR STORIES



**Microsoft Confirms
Windows 10 1903 Update
Error 0x80073701,
Working on Fix**



Steam Accounts Being Stolen Through Elaborate Free Game Scam

NEWSLETTER SIGN UP

To receive periodic
updates and news
from
BleepingComputer,
please use the form
below.

Submit

Exhibit 23

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?



Generate secure, unique passwords for every account

Learn more at 1Password.com (<https://1password.com/haveibeenpwned/>)

Why 1Password? (/1Password)

397

pwned websites

8,418,474,549

pwned accounts

99,584

pastes

121,023,090

paste accounts

Largest breaches

EXHIBIT 23



verifications.io

772,904,991 Collection #1 accounts (/PwnedWebsites#Collection1)763,117,241 Verifications.io accounts (/PwnedWebsites#VerificationsIO)711,477,622 Onliner Spambot accounts
(/PwnedWebsites#OnlinerSpambot)593,427,119 Exploit.In accounts (/PwnedWebsites#ExploitIn)457,962,538 Anti Public Combo List accounts (/PwnedWebsites#AntiPublic)393,430,309 River City Media Spam List accounts
(/PwnedWebsites#RiverCityMedia)359,420,698 MySpace accounts (/PwnedWebsites#MySpace)234,842,089 NetEase accounts (/PwnedWebsites#NetEase)164,611,595 LinkedIn accounts (/PwnedWebsites#LinkedIn)161,749,950 Dubsmash accounts (/PwnedWebsites#Dubsmash)

Recently added breaches

39,721,127 Chegg accounts (/PwnedWebsites#Chegg)749,161 Cracked.to accounts (/PwnedWebsites#CrackedTO)6,840,339 StockX accounts (/PwnedWebsites#StockX)137,272,116 Canva accounts (/PwnedWebsites#Canva)23,205,290 CafePress accounts (/PwnedWebsites#CafePress)4,007,909 Club Penguin Rewritten (July 2019) accounts
(/PwnedWebsites#ClubPenguinRewrittenJul2019)368,507 Anime-Planet accounts (/PwnedWebsites#AnimePlanet)408,795 EpicNPC accounts (/PwnedWebsites#EpicNPC)1,604,957 Clash of Kings accounts (/PwnedWebsites#ClashOfKings)1,410,899 Snail accounts (/PwnedWebsites#Snail)

A troyhunt.com project (<https://www.troyhunt.com>)



(<https://www.facebook.com/troyahunt>)



(<https://twitter.com/troyhunt>)

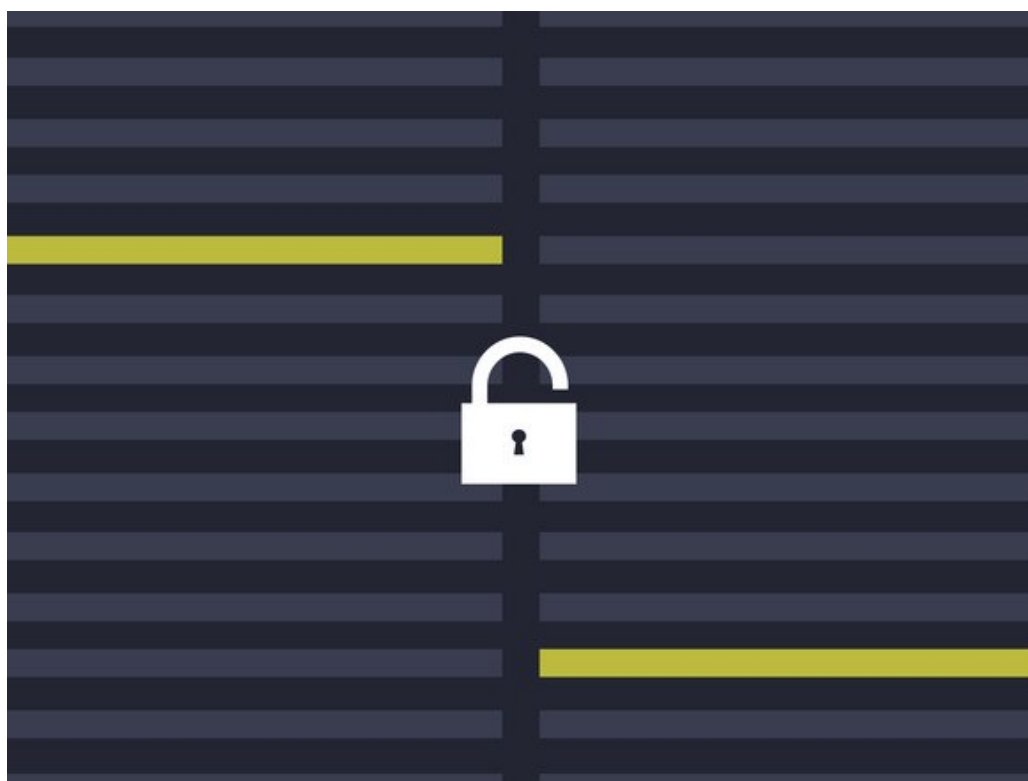


(<https://www.troyhunt.com/contact/>)

Exhibit 24

LILY HAY NEWMAN SECURITY 02.17.19 07:00 AM

HACKER LEXICON: WHAT IS CREDENTIAL STUFFING?



Attackers take a massive trove of usernames and passwords and try to "stuff" those credentials into the login page of other digital services. EMILY WAITE

EXHIBIT 24

YOU MAY HAVE noticed this happening more and more lately: Online accounts get taken over in droves, but the companies insist that their systems haven't been compromised. It's maddening, but in many cases, technically they're right. The real culprit is a hacker technique known as "credential stuffing."

usernames and passwords (often from a corporate megabreach) and try to "stuff" those credentials into the login page of other digital services. Because people often reuse the same username and password across multiple sites, attackers can often use one piece of credential info to unlock multiple accounts. In the last few weeks alone, Nest, Dunkin' Donuts, OkCupid, and the video platform DailyMotion have all seen their users fall victim to credential stuffing.

"With all of the massive credential dumps that have happened over the past few years, credential stuffing has become a serious threat to online services," says Crane Hassold, a threat intelligence manager at the digital fraud defense firm Agari. "Most people don't change their passwords regularly, so even older credential dumps can be used with relative success. And since password reuse is rampant, cybercriminals will generally test a set of credentials against numerous different websites."

Credential Craze

Credential stuffing has been a problem for years now, as troves of credentials from seminal breaches like LinkedIn and Dropbox in 2012 and Myspace in 2013 have been used—to great effect!—in countless credential stuffing campaigns. But one trend in particular has fueled a recent rise in successful campaigns.

Recently hackers have posted more gigantic, aggregated credential collections that comprise multiple data breaches. One of the most wild recent examples is known as Collection #1-5, a "breach of breaches" that totaled 2.2 billion unique username and password combinations, all available to download in plaintext—for free.

LEARN MORE

THE WIRED GUIDE TO DATA BREACHES

recently, immediately after that news came out, says Shuman Ghosemajumder, chief technical officer at the corporate digital fraud defense firm Shape Security. “In fact, we saw some of the largest credential stuffing attacks across several customers in just that week. And that makes sense because you’ve got all these plaintext usernames and passwords available through a torrent. It democratizes credential stuffing.”

The Collection credentials are mostly a few years old, meaning many were already in broad circulation and not worth much. But over the last week, another outlandish trove has provided exactly the type of fresh, high-quality credentials hackers cherish. Posted on the Dream Market dark web marketplace, the collection includes a total of roughly 841 million records, released in three batches, from 32 web services, including MyFitnessPal, MyHeritage, Whitepages, and the file-sharing platform Ge.tt. The first part of the dump costs about \$20,000 in bitcoin, the second about \$14,500, and the third roughly \$9,350. A few of the breaches don’t include passwords, and some that do are protected by cryptographic scrambling that buyers will need to decode, but overall these are top-shelf troves ripe for use in credential stuffing.

Hot Stuff

As you’ve probably guessed, credential stuffing relies on automation; hackers aren’t literally typing in hundreds of millions of credential pairs across hundreds of sites by hand. Credential stuffing attacks also can’t try massive numbers of logins on a site with all the tries coming from the same IP address, because web services have basic rate-limiting protections in place to block floods of activity that could be destabilizing.

So hackers use credential stuffing tools, available on malicious platforms, to incorporate “proxy lists” to bounce the requests around the web and make them look like they’re coming from all different IP addresses. They can also manipulate properties of the login requests to make it look like they come from a diverse array of browsers, because most websites will flag large amounts of traffic all coming from the same type of browser as suspicious. Credential

Captchas.

Credential stuffing campaigns ultimately try to get the malicious requests to blend into the noise of all the legitimate logins happening on a service at any given time, or “simulate the activity of a large population of humans,” as Shape Security’s Ghosemajumder puts it.

It also requires patience; Shape estimates that typically attackers find matches between their test credentials and an account on the platform they are attacking 0.1 to 2 percent of the time. This is why attackers need hundreds of thousands or millions of credential pairs to make credential stuffing attacks worth it. And once they’ve gotten into some accounts, attackers still need a way to monetize what they find there—either by stealing more personal data, money, gift card balances, credit card numbers, and so on—to make the whole thing worthwhile.

Stuff It

The best way to protect against credential stuffing attacks is to use unique passwords for each of your digital accounts—ideally by using a password manager—and turn on two-factor authentication when it’s available. But it’s not entirely on you. Companies, too, are increasingly attempting to detect and block credential stuffing attempts. And some like Google (which also owns Nest) have started initiatives to proactively check whether users’ account credentials have been compromised in breaches and trigger password resets if they discover a match. But the trick is to do all of this without blocking or hindering legitimate activity.

One strategy companies can deploy is to track logins that ultimately result in fraud, then blacklist the associated IP address. Over time, this can erode the effectiveness of the proxy lists attackers rely on to mask their mass login

more difficult and potentially costly for hackers to carry out the attacks.

Services whose users are mainly in specific geographic regions can also establish geofences, blocking proxy traffic that comes in from elsewhere in the world. Once again, though, attackers can ultimately adapt to this restriction as well by switching to using proxy IPs within those areas.

A recent credential stuffing attack against the productivity and project management service [Basecamp](#) helps illustrate the problem. The company reported recently that it had faced 30,000 malicious login attempts from a diverse set of IP addresses in a single hour. The company began blocking the IPs as quickly as possible, but needed to implement a Captcha to ultimately end the attack. When the barrage died down, Basecamp found that the attackers had only succeeded in penetrating 124 accounts; the company quickly reset those account passwords to revoke the attackers' access.

Many companies aren't as prepared to handle the scale of the credential stuffing threat. Shape Security's Ghosemajumder says that it's pretty typical at this point for corporate clients to see 90 percent of their logins come from malicious attacks. He has even worked with customers who deal with credential stuffing in 99.9 percent of login attempts to their service. And while credential dumps from leaks and breaches are the primary fuel for these attacks, criminals can also diversify their approach by using credential pairs gathered from phishing attacks.

"Most credential stuffing uses information obtained from the major data breaches," Agari's Hassold says. "But over the past few years there has been a shift in the credential phishing landscape to target generic account credentials that are then 'stuffed' into a number of different websites."

Though it is frustrating when companies insist that they haven't been breached and deny responsibility for protecting their users from credential stuffing

defending against this threat. As Basecamp's CEO and co-founder David Heinemeier Hansson put it after the service's recent incident, "Our ops team will continue to monitor and fight any future attacks. ... But if someone has your username and password, and you don't have 2FA protection, there are limits to how effective this protection can be."

For such a simple technique, credential stuffing is frustratingly difficult to quash. So keep your passwords as diverse as possible and use two-factor whenever you can. And complain loudly on social media about any web service that isn't offering it.

More Great WIRED Stories

- A scary map shows how climate change will alter cities
- Strava has a new way to build routes with a finger swipe
- What happens if Russia cuts itself off from the internet
- Ride with the guy who builds roller coasters in his yard
- *Captain Marvel* has the best movie site since *Space Jam*
- 🔍 Looking for the latest gadgets? Check out our latest buying guides and best deals all year round
- ✉️ Want more? Sign up for our daily newsletter and never miss our latest and greatest stories

RELATED VIDEO

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

FOLLOW US ON TWITTER



Visit WIRED Photo for our unfiltered take on photography, photographers, and photographic journalism [wired.com/category/photo](https://www.wired.com/category/photo)

FOLLOW

SUBSCRIBE

ADVERTISE

SITE MAP

PRESS CENTER

FAQ

ACCESSIBILITY HELP

CUSTOMER CARE

CONTACT US

[SUBSCRIBE](#)[NEWSLETTER](#)[WIRED STAFF](#)[JOBS](#)[RSS](#)

CNMN Collection

© 2018 Condé Nast. All rights reserved.

Use of and/or registration on any portion of this site constitutes acceptance of our [User Agreement](#) (updated 5/25/18) and [Privacy Policy and Cookie Statement](#) (updated 5/25/18). [Your California Privacy Rights](#). The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast. [Ad Choices](#).

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Claims StockX Failed to Prevent, Attempted to Cover Up Data Breach](#)
