

CLE Materials for

Confronting the Emerging Cyber Threat

January 15, 2016

- A. U.S. v. Shalon, et al. (2015)
- B. FTC v. Wyndham (2015)
- C. Remijas, et al., v. Neiman Marcus Group (2015)
- D. "Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme," Federal Bureau of Investigation (2015)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - X
:
UNITED STATES OF AMERICA :
:
-v.- :
:
GERY SHALON, :
a/k/a "Garri Shalelashvili," :
a/k/a "Gabriel," :
a/k/a "Gabi," :
a/k/a "Phillipe Mousset," :
a/k/a "Christopher Engeham," :
JOSHUA SAMUEL AARON, :
a/k/a "Mike Shields," and :
ZIV ORENSTEIN, :
a/k/a "Aviv Stein," :
a/k/a "John Avery," :
:
Defendants. :
:
- - - - - X

SEALED SUPERSEDING
INDICTMENT

333
S1 15 Cr. ~~555~~ (LTS)

The Grand Jury charges:

Relevant Persons and Entities

1. At all times relevant to this Indictment, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham" ("GERY SHALON"), the defendant, was a citizen and resident of Israel. At all relevant times, SHALON was the leader and self-described "founder" of a sprawling cybercriminal enterprise that encompassed all of the criminal schemes described herein. SHALON's cybercriminal enterprise operated through hundreds of

employees, co-conspirators and infrastructure in over a dozen countries.

2. At all times relevant to this Indictment, JOSHUA SAMUEL AARON, a/k/a "Mike Shields" ("JOSHUA AARON"), the defendant, was a United States citizen who, at relevant times, resided in the United States, Israel, and Russia. At the direction of GERY SHALON, the defendant, AARON engaged in computer hacking crimes and securities market manipulation schemes in the United States as set forth herein.

3. At all times relevant to this Indictment, ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein" ("ZIV ORENSTEIN"), the defendant, was a citizen and resident of Israel. At all relevant times, ORENSTEIN acted as a principal deputy to GERY SHALON, the defendant, in furtherance of their criminal schemes, opening bank and brokerage accounts under aliases, creating and maintaining shell companies, and managing payments to and from co-conspirators and others at SHALON's direction.

4. At all relevant times, Victim-1 was one of the world's largest financial institutions, with headquarters in New York, New York.

5. At all relevant times, Victim-2 was one of the world's largest financial services corporations, providing mutual fund,

online stock brokerage and other services, with headquarters in Boston, Massachusetts.

6. At all relevant times, Victim-3 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in Omaha, Nebraska.

7. At all relevant times, Victim-4 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in New York, New York.

8. At all relevant times, Victim-5 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in St. Louis, Missouri.

9. At all relevant times, Victim-6 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in Queens, New York.

10. At all relevant times, Victim-7 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in Charlotte, North Carolina.

11. At all relevant times, Victim-8 was one of the world's most widely circulated financial news publications, with headquarters in New York, New York.

12. At all relevant times, Victim-9 was a financial news publisher, with headquarters in Baltimore, Maryland.

13. At all relevant times, Victim-10 was a software development firm, with headquarters in Costa Rica and offices in the United States.

14. At all relevant times, Victim-11 was a software development firm, with headquarters in Curaçao.

15. At all relevant times, Victim-12 was a merchant risk intelligence firm, with headquarters in Bellevue, Washington.

Overview

16. From approximately 2012 to mid-2015, GERY SHALON, the defendant, orchestrated massive computer hacking crimes against U.S. financial institutions, financial services corporations, and financial news publishers, including the largest theft of customer data from a U.S. financial institution in history (the "U.S. Financial Sector Hacks"). Working with co-conspirators, including, at times, JOSHUA AARON, the defendant, SHALON directed network intrusions into Victims 1-9, among others, stealing personal information of over one hundred million customers of these companies. SHALON and his co-conspirators engaged in these crimes in furtherance of other criminal schemes, including securities market manipulation schemes that SHALON, AARON, and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendant, perpetrated in the United States. In particular, in an effort to artificially manipulate the price

of certain stocks publicly traded in the United States, SHALON and his co-conspirators sought to market the stocks, in a deceptive and misleading manner, to customers of the victim companies whose contact information they had stolen in the intrusions. SHALON and his co-conspirators generated tens of millions of dollars in unlawful proceeds from these schemes.

17. In addition to directing the U.S. Financial Sector Hacks, GERY SHALON, the defendant, directed computer network hacks and cyberattacks against numerous United States and foreign companies outside of the financial sector. As set forth below, SHALON and his co-conspirators engaged in these crimes in furtherance of large-scale criminal businesses that SHALON and ZIV ORENSTEIN, the defendant, operated in the United States and other countries. In particular, between approximately 2007 and July 2015, SHALON owned and operated unlawful internet gambling businesses in the United States and abroad; owned and operated multinational payment processors for illegal pharmaceutical suppliers, counterfeit and malicious software ("malware") distributors, and unlawful internet casinos; and owned and controlled Coin.mx, an illegal United States-based Bitcoin exchange that operated in violation of federal anti-money laundering laws. Nearly all of these schemes, like SHALON's securities market manipulation schemes, relied for their success

on computer hacking and other cybercrimes committed by SHALON and his co-conspirators.

18. Through their criminal schemes, between in or about 2007 and in or about July 2015, GERY SHALON and his co-conspirators earned hundreds of millions of dollars in illicit proceeds, of which SHALON concealed at least \$100 million in Swiss and other bank accounts.

19. GERY SHALON, JOSHUA AARON, and ZIV ORENSTEIN, the defendants, and their co-conspirators operated their criminal schemes, and laundered their vast criminal proceeds, through at least 75 shell companies and bank and brokerage accounts around the world. The defendants controlled these companies and accounts using aliases, and by fraudulently using approximately 200 purported identification documents, including over 30 false passports that purported to be issued by the United States and at least 16 other countries.

Execution of the U.S. Financial Sector Hacks

20. GERY SHALON, and JOSHUA AARON, the defendants, and their co-conspirators executed the U.S. Financial Sector Hacks using the following means and methods:

a. In furtherance of the conspiracy, using aliases, SHALON and, at SHALON's direction, certain co-conspirators not identified herein, procured computer network infrastructure,

including particular servers located in Egypt, the Czech Republic, South Africa, Brazil and elsewhere, to be used to gain unlawful access to companies' computer networks and to receive data stolen from those networks during the intrusions.

b. Also in furtherance of the conspiracy, at various times, SHALON directed a co-conspirator not identified herein ("CC-1") to execute network intrusions at particular companies in an effort to steal customer data as identified by SHALON. On at least one occasion, as set forth below, AARON identified the company to be hacked in furtherance of the conspiracy.

c. As a further part of the conspiracy, in connection with many of the network intrusions, AARON provided to SHALON, who provided to CC-1, AARON's own login credentials, and other information obtained by AARON, as a customer of many of the victim companies, in order for CC-1 to perform certain analysis of those victims' networks in connection with the intrusions.

d. Also in furtherance of the conspiracy, at SHALON's direction, CC-1 hacked into the victims' network servers, on which CC-1 typically caused a particular piece of malware to be installed. This malware provided CC-1 with persistent access to many of the victim companies' networks,

enabling CC-1 and SHALON to steal data from these victims repeatedly, sometimes over a period of many months.

e. As a further part of the conspiracy, as CC-1 engaged in particular network intrusions at SHALON's direction, CC-1 and SHALON discussed the nature of the data CC-1 was locating and stealing at SHALON's direction, various issues CC-1 encountered while hacking into the networks, and SHALON's receipt and use of the stolen data.

f. Also in furtherance of the conspiracy, after obtaining stolen customer data from victim companies, SHALON, AARON, and their co-conspirators used or sought to use the data in furtherance of their other criminal schemes, including securities market manipulation schemes they perpetrated with ZIV ORENSTEIN, the defendant, and others, as described below.

The 2012-2013 Hacks

21. Between approximately 2012 and late 2013, GERY SHALON, the defendant, and CC-1, working at times with JOSHUA AARON, the defendant, executed the hacks of the computer networks of Victims 4-9, stealing records relating to tens of millions of customers of these institutions. Among other things, in foreign-language electronic communications, during these hacks:

a. SHALON bragged about the size and scope of his securities market manipulation schemes, and described to CC-1

his use of the stolen data in furtherance of those schemes. For example:

i. As to a particular publicly traded stock for which SHALON, AARON and ORENSTEIN had manipulated trading in the United States, SHALON boasted that his sale of that stock for large profits was "a small step towards a large empire." As SHALON explained, "We buy them [i.e., stocks] very cheap, perform machinations, then play with them. . . ." When CC-1 asked, with respect to SHALON's ability to cause people in the United States to purchase stocks, if it really was "popular in America - buying stocks?," SHALON responded, "It's like drinking freaking vodka in Russia."

ii. SHALON indicated to CC-1 that SHALON intended to distribute "mailers," or promotions of particular stocks, to people whose contact information CC-1 had stolen from the victim companies.

iii. SHALON described contacting and lying to people whose personal information had been obtained in the hacks, in the course of tricking those people into buying stocks being deceptively touted by the defendants. In particular, SHALON explained, individuals acting at SHALON's direction lied to people about how their personal contact information had been

obtained, falsely claiming that the information was simply "in our investors' database."

b. SHALON and CC-1 discussed the risk of law enforcement detection of their activities. For example, CC-1 claimed, "[i]n Israel, you guys probably don't have to be afraid of the USA. . . meaning that even if there is some case, they won't be able to do anything"? SHALON responded, "[t]here is nothing to be afraid of in Israel. . . ." On another occasion, CC-1 suggested that SHALON "get[] a passport in another name. . . it will probably be safer?," to which SHALON responded that he was "doing it now."

c. SHALON and CC-1 discussed expanding the size and scope of their network intrusions to encompass thefts of material non-public information from the financial institutions and other firms they were hacking. For example, CC-1 noted, "the top managers in [Victim-5], can they have some interesting info in their mail [i.e., email]? Regarding working on the stock market, etc. It's a big company after all. mb [Maybe] they have some secrets. . . What do you think?" SHALON responded, "Yes, this is a very cool idea. Some *inside* [i.e., inside, or material non-public, information]. We need to think how we can do it."

d. AARON encouraged and participated in the conspiracy's hacking crimes in numerous ways. For example:

i. In furtherance of the schemes to hack Victims-4-8, AARON provided to SHALON, who in turn provided to CC-1, AARON's own login credentials, and in some instances, the login credentials of a friend of AARON's, as a customer of these companies, which CC-1 used in furtherance of efforts to hack into the victim company networks. In connection with the network intrusion of Victim-8, at SHALON's direction, AARON also provided to SHALON other information that AARON was able to obtain from Victim-8 online as a Victim-8 customer.

ii. AARON encouraged SHALON to orchestrate the hack of Victim-9. Thereafter, SHALON informed AARON of the successful completion of the Victim-9 hack, noting that they had obtained "probably 9 million unique" customer records of Victim-9. SHALON further told AARON, "we got what [yo]u wanted so now show me how we make out of it 100mil [i.e. \$100 million] a year," which AARON agreed to do.

The 2014 Hacks

22. In 2014, GERY SHALON, JOSHUA AARON and their co-conspirators orchestrated network intrusions into even bigger financial institutions, including Victims 1-3. In particular, in or about March 2014, GERY SHALON and JOSHUA AARON, the

defendants, and their co-conspirators began their efforts to hack into the computer networks of Victim-3. As part of that effort, they repeatedly attempted to access AARON's Victim-3 customer account from a particular Egypt-based computer server (the "Egypt Server"), but they were unable to do so because, after observing the attempts to access the account from this server, Victim-3 locked AARON's account for online access. In response, in furtherance of the hack, AARON called Victim-3 and, upon being notified that his account had been locked and asked by a customer service representative whether AARON had been traveling in Egypt in March 2014, AARON lied to the representative, and claimed that he had been in Egypt. In truth and in fact, and as AARON well knew, AARON had not been in Egypt, and was merely attempting to convince Victim-3 to allow AARON and his co-conspirators to access AARON's account online in furtherance of their efforts to hack into Victim-3.

23. Thereafter, in April 2014, SHALON and his co-conspirators unlawfully accessed the network of Victim-2 by exploiting the so-called "Heartbleed" vulnerability, which had, at that time, just been widely identified as a previously unrecognized security vulnerability that existed in computer network servers on a widespread basis. While they succeeded in gaining access to Victim-2's network, shortly after they did so,

Victim-2 recognized and repaired the Heartbleed vulnerability in its systems.

24. Beginning in June 2014, and ending in August 2014, SHALON, AARON and their co-conspirators executed the hack of Victim-1, during which they stole customer records of over 83 million customers of Victim-1. To hack into Victim-1's network, they used, among others, the Egypt Server, which they had rented from a third-party company for years under an alias frequently used by SHALON, AARON and their co-conspirators in the course of their criminal schemes. In August 2014, the day after the Victim-1 hack was first widely reported in the media, SHALON's co-conspirator abruptly canceled their longtime rental of the Egypt Server.

The Securities Market Manipulation Schemes

25. From in or about 2011 up to and including July 2015, GERY SHALON, JOSHUA AARON, and ZIV ORENSTEIN, the defendants, operated lucrative securities market manipulation schemes in the United States. In furtherance of their securities market manipulation scheme, among other things:

a. SHALON and AARON identified opportunities to partner with "promoters," including certain cooperating witnesses not identified herein ("CW-1" and "CW-2"), who identified companies whose stock would be targeted for

manipulation. In some instances, at the time SHALON and AARON partnered with the promoters, the companies identified by the promoters were already publicly traded, and in other instances, when they partnered with the promoters, SHALON and AARON worked with the promoters to cause the companies to become publicly traded in furtherance of the scheme. To do so, SHALON caused privately held companies to engage in "reverse mergers" with publicly traded shell corporations owned and controlled by SHALON.

b. Upon partnering with the promoters, SHALON, AARON and the promoters agreed upon the compensation SHALON and AARON would receive for their role in the scheme, which was typically either hundreds of thousands of dollars, or shares in the targeted stock that the defendants often sold for up to millions of dollars in profits per stock in the course of the scheme.

c. Also in furtherance of the securities fraud scheme, the promoters - along with, at certain times, SHALON and AARON - acquired control over all or substantially all of the free-trading shares of the targeted stock, that is, shares that the owner could trade without restriction on a national stock exchange or in the over-the-counter market. At certain times, when they acquired such shares, SHALON and AARON held the shares in particular U.S. brokerage accounts, which were frequently

held in the names of shell companies controlled by ORENSTEIN and which were managed in part at SHALON's direction by ORENSTEIN using numerous aliases, false passports and other false personal identification information.

d. As a further part of the scheme to defraud, after members of the conspiracy acquired control of a substantial portion of the free-trading shares of the targeted stock, SHALON, AARON and their co-conspirators artificially inflated the stock's price and trading volume through two primary fraudulent and deceptive means. First, certain members of the conspiracy typically executed pre-arranged manipulative trades to cause the stock's price to rise small amounts on successive days. Second, in connection with that trading, SHALON and AARON began disseminating materially misleading, unsolicited ("spam") messages by various means - including by email to up to millions of recipients per day - that falsely touted the stock in order to trick others into buying it. SHALON and AARON engaged in the U.S. Financial Sector Hacks in part to acquire email and mailing addresses, phone numbers and other contact information for potential victims to whom they could send such deceptive communications. As orchestrated by SHALON and AARON, these communications contained materially false and fraudulent statements including, for example, (i) that the stock's recent

trading activity reflected legitimate demand for the stock (when in truth and in fact, and as AARON and SHALON well knew, the trading activity was caused in whole or part by their co-conspirators' manipulative trading) and (ii) that the emails were being distributed and financed by certain third parties (when, in truth and in fact, and as the defendants well knew, the emails were being distributed and financed by SHALON, AARON and their co-conspirators, who controlled all or nearly all of the free-trading shares of the stock). In addition to fraudulently promoting the stocks by email, SHALON and AARON fraudulently marketed the stocks to potential U.S. victims by mail and phone.

e. Also in furtherance of the conspiracy, after causing the stock's price and trading volume to increase artificially during the days or weeks of the deceptive promotional campaign, members of the conspiracy (including the defendants, when they owned shares), began selling their shares in a coordinated fashion, often resulting in millions of dollars in profits per stock to members of the conspiracy. The co-conspirators' massive coordinated sales typically placed downward pressure on the stock's price and caused its trading volume to plummet, exposing unsuspecting investors to significant losses. SHALON, AARON and ORENSTEIN earned millions

of dollars in illicit profits this way. For example, among the dozens of publicly traded stocks for which they successfully manipulated trading, the defendants sold their holdings in a particular stock ("Stock-1") for over \$2 million at artificially inflated prices, soon after which Stock-1's price and liquidity plummeted.

f. As a further part of the scheme to defraud, after selling shares of the manipulated stock at artificially high prices or otherwise receiving compensation from promoters for their role in the scheme, SHALON, AARON, and ORENSTEIN laundered their criminal proceeds overseas, directing millions of dollars of their criminal profits to particular accounts in Cyprus for further distribution in part to a particular Cyprus-based shell company account owned by AARON and to other overseas shell company accounts beneficially owned and controlled by SHALON and other members of the conspiracy.

The Unlawful Internet Gambling Schemes, Hacks and Cyberattacks

26. In addition to operating U.S. securities market manipulation schemes, from at least in or about 2007 up to and including in or about July 2015, GERY SHALON and ZIV ORENSTEIN, the defendants, and their co-conspirators operated lucrative, unlawful internet casinos in the United States and elsewhere through hundreds of employees in multiple countries. In the

United States, SHALON, ORENSTEIN and their co-conspirators knowingly operated, among others, at least 12 unlawful internet casinos (the "Casino Companies") which, through their websites, offered real-money casino gambling in violation of federal law and the laws of numerous states, including New York State. Similar to the manner in which they marketed their fraudulent stock promotions, SHALON, ORENSTEIN and their co-conspirators knowingly marketed the Casino Companies to U.S. customers through, among other things, email promotions distributed on a massive scale. Through the Casino Companies, SHALON, ORENSTEIN, and their co-conspirators generated hundreds of millions of dollars in unlawful income, at a minimum, earning up to millions of dollars in profits per month.

27. In furtherance of his unlawful internet gambling schemes, GERY SHALON, the defendant, and his co-conspirators engaged in massive hacks and cyberattacks against other internet gambling businesses to steal customer information, secretly review executives' emails, and cripple rival businesses. In particular, in or about 2012, SHALON orchestrated network intrusions of competitors in order to steal his competitors' customer databases and other information. SHALON separately directed "distributed denial of service," or DDOS, attacks, against competitors to temporarily shut down their businesses in

response to perceived misconduct by them directed at SHALON's casinos.

28. Also in furtherance of his unlawful internet gambling businesses, GERY SHALON, the defendant, orchestrated network intrusions of Victim-10 and Victim-11, software development companies that provided operating software to SHALON's internet casinos and other such casinos around the world. In doing so, SHALON sought to, and did, secretly obtain access to the email accounts of senior executives at both companies, reading their emails on an ongoing basis, a fact SHALON ultimately admitted to at least one of the executives whose emails he had been secretly reading. SHALON monitored company executives' emails in order to ensure that the companies' work with SHALON's competitors did not, in SHALON's view, compromise the success of SHALON's unlawful internet gambling businesses.

The Illicit Payment Processing Scheme and Hack

29. From at least in or about 2011 until in or about July 2015, GERY SHALON and ZIV ORENSTEIN, the defendants, and their co-conspirators operated IDPay and Todur, multinational payment processors for criminals who sought to receive payments by credit and debit card in furtherance of their unlawful schemes. Through these payment processors, SHALON, ORENSTEIN and their co-conspirators knowingly processed credit and debit card

payments for, at a minimum, unlawful pharmaceutical distributors, purveyors of counterfeit and malicious purported "anti-virus" computer software, their own unlawful internet casinos, and an illegal United States-based Bitcoin exchange owned by SHALON. In doing so, SHALON, ORENSTEIN and their co-conspirators knowingly processed hundreds of millions of dollars in transactions for criminal schemes, for which they earned a percentage of every transaction, amounting to over \$18 million in illicit profits.

30. As GERY SHALON and ZIV ORENSTEIN, the defendants, well knew, banks and credit card issuers in the United States and elsewhere were largely unwilling to process payment transactions for illegal activities such as internet gambling, the sale of counterfeit pharmaceuticals, the distribution of counterfeit and malicious software, and running an unlicensed Bitcoin exchange. For that reason, to open and operate bank accounts in numerous countries, including Azerbaijan, through which they processed unlawful credit and debit card transactions, SHALON, ORENSTEIN, and their co-conspirators variously lied to financial institutions about the nature of their business and colluded with corrupt international bank officials who willfully ignored its criminal nature in order to profit from, as a co-conspirator

described it to SHALON, their payment processing "casino/soft[ware]/pharma[ceutical] cocktail."

31. Furthermore, to deceive U.S. banks and credit card issuers into authorizing their illicit credit and debit card payment transactions, GERY SHALON and ZIV ORENSTEIN, the defendants, and their co-conspirators deliberately misidentified and miscoded those transactions, in violation of bank and credit card company rules and regulations. For example, through their payment processing scheme, SHALON, ORENSTEIN and their co-conspirators arranged for money received from United States gamblers to be disguised as payments to phony online non-gambling merchants, such as wedding dress and pet supply stores, in order to trick U.S. and other financial institutions into allowing the transactions to be completed.

32. At relevant times, in an effort to ensure compliance with their regulations, major United States credit card companies monitored and investigated merchant activity that appeared to be in furtherance of criminal schemes or otherwise designed to circumvent their regulations. In the course of that work, credit card companies repeatedly identified bank accounts which were receiving credit and debit card payments for illicit pharmaceuticals and other criminal goods and services, and which, unbeknownst to the credit card companies, were operated

by GERY SHALON and ZIV ORENSTEIN, the defendants, in furtherance of their unlawful payment processing scheme. In so doing, the credit card companies imposed millions of dollars in penalties on the financial institutions through which SHALON and ORENSTEIN processed these unlawful credit and debit card payments, and SHALON and ORENSTEIN, in turn, paid those amounts to the financial institutions to cover the penalties.

33. To avoid further financial penalties and processing shutdowns, and to evade law enforcement detection of their illicit payment processing scheme, GERY SHALON and ZIV ORENSTEIN, the defendants, (1) worked continuously to obtain new bank accounts, and establish new phony merchants, to replace those that were periodically shut down by banks and credit card companies for engaging in unlawful activity; (2) monitored credit card transactions processed through their payment processing business to attempt to discern which, if any, were undercover transactions made on behalf of credit card companies attempting to identify unlawful merchants; and (3) lied repeatedly to banks that discovered illicit transactions conducted in their accounts by pretending they were surprised and otherwise unaware of the illicit nature of the transactions, a deceit that SHALON and ORENSTEIN discussed openly with each other and co-conspirators.

34. The efforts of GERY SHALON and ZIV ORENSTEIN, the defendants, to evade detection of their criminal payment processing activity went beyond the defensive measures described above. Beginning in or about 2012, SHALON and his co-conspirators hacked into the computer networks of Victim-12, a U.S. company which assessed merchant risk and compliance for credit card issuers and others, including by detecting merchants that accepted credit card payments for unlawful goods or services. Thereafter, on an ongoing basis, SHALON and his co-conspirators monitored Victim-12's detection efforts, including reading emails of Victim-12 employees, so they could take steps to evade detection by Victim-12 of their unlawful payment processing scheme. In particular, through their unlawful intrusion into Victim-12's network, SHALON and his co-conspirators determined which credit and debit card numbers Victim-12 employees were using to make undercover purchases of illicit goods in the course of their effort to detect unlawful merchants. Upon identifying those credit and debit card numbers, SHALON and his co-conspirators blacklisted the numbers from their payment processing business, automatically declining any transaction for which payment was offered through one of those credit or debit card numbers.

The Unlawful Bitcoin Exchange

35. In addition to the other unlawful schemes set forth above, from in or about 2013 to in or about July 2015, GERY SHALON, the defendant, knowingly owned Coin.mx, a Bitcoin exchange service, which was operated by co-conspirators in the United States at SHALON's direction in violation of federal anti-money laundering ("AML") registration and reporting laws and regulations. Through Coin.mx, SHALON and his co-conspirators enabled their customers to exchange cash for Bitcoins, charging a fee for their service. In total, between approximately October 2013 and July 2015, Coin.mx exchanged millions of dollars for Bitcoins on behalf of its customers.

36. GERY SHALON, the defendant, and his co-conspirators engaged in substantial efforts to evade detection of their unlawful Bitcoin exchange scheme by operating through a phony front-company, "Collectables Club," and maintaining a corresponding phony "Collectables Club" website. In doing so, they sought to trick the major financial institutions through which they operated into believing their unlawful Bitcoin exchange business was simply a members-only association of individuals who discussed, bought, and sold collectable items, such as stamps and sports memorabilia. In approximately 2014, in an effort to evade potential scrutiny from these institutions

and others, SHALON's co-conspirators acquired control of a federal credit union (the "Credit Union"), installed co-conspirators on the Credit Union's Board of Directors, and transferred Coin.mx's banking operations to the Credit Union, which SHALON's co-conspirators operated, at least until early 2015, as a captive bank for their unlawful business.

Statutory Allegations

COUNT ONE

(Conspiracy to Commit Computer Hacking: U.S. Financial Sector Hacks)

37. The allegations contained in paragraphs 1-24 of this Indictment are repeated and realleged as if fully set forth herein.

38. From at least in or about 2012, up to and including at least July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, computer hacking, in violation of Title 18, United States Code, Sections 1030(a)(2)(A) and 1030(a)(2)(C).

39. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendants, and others known and unknown, would and did intentionally access a computer without authorization and exceed authorized access, and thereby obtain information contained in a financial record of a financial institution, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in violation of the laws of the United States, to wit, the securities and wire fraud crimes charged in Counts Four through Thirteen of this Indictment, and the value of the information obtained was greater than \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(A) and 1030(c)(2)(B).

40. It was a further part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendants, and others known and unknown, would and did intentionally access a computer without authorization and exceed authorized access, and thereby did obtain information from a protected computer, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in

violation of the laws of the United States, to wit, the securities and wire fraud crimes charged in Counts Four through Thirteen of this Indictment, and the value of the information obtained was greater than \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B).

Overt Acts

41. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about June 2012, JOSHUA AARON, the defendant, provided information regarding Victim-9's websites and servers to GERY SHALON, the defendant.

b. In at least in or about June 2012, SHALON caused the unauthorized access to, and theft of customer data from, the computer network of Victim-9.

c. In or about October 2012, AARON provided login credentials for a Victim-5 account to SHALON.

d. In or about November 2012, AARON provided login credentials for a Victim-7 account to SHALON.

e. In or about November 2012, AARON provided login credentials for a Victim-4 account to SHALON.

f. In or about November 2012, AARON provided login credentials for a Victim-6 account to SHALON.

g. In or about December 2012, SHALON caused the unauthorized access to, and theft of customer data from, Victim-6, including by wire communications through the Southern District of New York.

h. In or about August 2013, SHALON caused the unauthorized access to, and theft of customer data from, the computer network of Victim-8.

i. On or about August 30, 2013, while hacking into Victim-8's computer network, CC-1 told SHALON, in electronic communications, in substance, that CC-1 had located 10 million email addresses of Victim-8 customers.

j. During at least in or about September 2013 to in or about February 2014, SHALON caused the unauthorized access to, and theft of customer data from, the computer network of Victim-5.

k. During at least in or about September 2013 to in or about November 2013, SHALON caused the unauthorized access to, and theft of customer data from, the computer network of Victim-7.

l. In or about December 2013, SHALON caused the unauthorized access to, and theft of customer data from, the computer network of Victim-4.

m. On or about December 7, 2013, while hacking into Victim-4's computer network, CC-1 told SHALON, in electronic communications, in substance, that CC-1 had located 15 million email addresses of Victim-4 customers.

n. In or about April 2014, SHALON, the defendant, caused Victim-2's computer network to be accessed without authorization.

o. From in or about June 2014, to in or about August 2014, SHALON caused the unauthorized access to, and theft of customer data from, the computer network of Victim-1.

(Title 18, United States Code, Section 371).

COUNT TWO

(Computer Hacking: Victim-1)

The Grand Jury further charges:

42. The allegations contained in paragraphs 1-25 and 41 of this Indictment are repeated and realleged as if fully set forth herein.

43. From at least in or about June 2014, up to and including at least in or about August 2014, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe

Mousset," a/k/a "Christopher Engeham," and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendants, and others known and unknown, willfully and knowingly, did intentionally access a computer without authorization and exceed authorized access, and thereby obtain information contained in a financial record of a financial institution and from a protected computer, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in violation of the laws of the United States, to wit, the securities and wire fraud crimes charged in Counts Four through Thirteen of this Indictment, and the value of the information obtained was greater than \$5,000, to wit, SHALON and AARON worked with others to hack into the computer network of Victim-1 and steal personal information of tens of millions of Victim-1 customers in furtherance of fraud schemes perpetrated by SHALON and AARON.

(Title 18, United States Code, Sections 1030(a)(2)(A),
1030(c)(2)(B), and 2.)

COUNT THREE

(Computer Hacking: Victim-8)

The Grand Jury further charges:

44. The allegations contained in paragraphs 1-25 and 41 of this Indictment are repeated and realleged as if fully set forth herein.

45. From at least in or about late 2013, up to and including in or about May 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendants, and others known and unknown, willfully and knowingly, did intentionally access a computer without authorization and exceed authorized access, and thereby obtain information contained in a financial record of a financial institution and from a protected computer, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in violation of the laws of the United States, to wit, the securities and wire fraud crimes charged in Counts Four through Thirteen of this Indictment, and the value of the information obtained was greater than \$5,000, to wit, SHALON and AARON worked with others to hack into the computer network of Victim-8 and steal personal information of millions of Victim-8 customers in furtherance of fraud schemes perpetrated by SHALON and AARON.

(Title 18, United States Code, Sections 1030(a)(2)(C),
1030(c)(2)(B), and 2.)

COUNT FOUR

(Conspiracy to Commit Securities Fraud)

The Grand Jury further charges:

46. The allegations contained in paragraphs 1-25 and 41 of this Indictment are repeated and realleged as if fully set forth herein.

47. From at least in or about 2011, up to and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate and agree together and with each other to commit an offense against the United States, to wit, securities fraud, in violation of Title 15, United States Code, Section 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

48. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, and others known and unknown, willfully and knowingly, directly and

indirectly, by the use of means and instrumentalities of interstate commerce, and of the mails, and of facilities of national securities exchanges, would and did use and employ, in connection with the purchase and sale of securities, manipulative and deceptive devices and contrivances in contravention of Title 17, Code of Federal Regulations, Section 240.10b-5, by (a) employing devices, schemes, and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon purchasers and sellers, all in violation of Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, to wit, by email and telephone communications from overseas to New York, New York and elsewhere, the defendants engaged in a scheme to artificially manipulate the price and trading volume of numerous stocks publicly traded in the United States.

Overt Acts

49. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others,

were committed in the Southern District of New York and elsewhere:

a. In or about mid-2011, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," the defendant, caused a brokerage account to be opened under an alias and using a copy of a false passport sent to a securities brokerage firm ("Firm-1") in Arizona.

b. On or about June 12, 2011, by email from outside the United States to a securities brokerage firm located in New York, New York ("Firm-2"), ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendant, opened an account at Firm-2 in the name "Entersa Limited" using an alias and a false passport (the "Firm-2 Entersa Account").

c. On or about June 26, 2011, in order to obtain trading authority over an account in the name "Entersa Limited" ("the Firm-1 Entersa Account") for JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendant, SHALON informed Firm-1 by email that "Mike Shields" was an "advisor" to Entersa.

d. In or about early January 2012, AARON transferred 2.5 million shares of Stock-1 into the Firm-2 Entersa Account in New York, New York.

e. In or about late January 2012, SHALON and AARON caused spam emails touting Stock-1, including false statements about the cause of the increase in Stock-1's trading volume, to be widely disseminated to recipients throughout the United States.

f. From on or about January 30, 2012 to on or about February 13, 2012, Entersa's Stock-1 holdings at Firm-2, located in New York, New York, were liquidated and, at the direction of AARON, Firm-2 wired over \$1.1 million in proceeds to a bank account in Cyprus in the name of Entersa ("the Entersa Cyprus Account").

g. In or about late 2011, AARON discussed with CW-2, by telephone, the manner in which AARON wanted CW-2 to manipulate the price of a particular publicly traded stock ("Stock-2").

h. In or about February 2012, SHALON and AARON met with CW-1 in person in Kiev, Ukraine, in furtherance of schemes to manipulate the price and sales of the publicly traded stock of at least two companies ("Stock-3" and "Stock-4").

i. In or about October 2012, AARON caused spam emails touting Stock-3, including false statements that Stock-3's trading volume was increasing due to investors "becoming

aware of the great story behind [Stock-3]," to be widely disseminated.

j. In or about mid-2011, at SHALON's direction, another individual not charged herein wired over \$80,000 of SHALON and AARON's compensation for the unlawful manipulation of the price and trading volume of a particular publicly traded stock ("Stock 5") from the Entersa Cyprus Account to a bank account maintained by AARON in Cyprus in the name of "Warmkal Trading Limited" ("AARON's Warmkal Account").

k. In or about June 2011, by email and telephone, AARON informed a representative of Firm-2 in New York, New York that email promotional campaigns run by AARON and others had resulted in substantial trading volume in ten particular publicly traded stocks (not including Stocks 1-7) on particular dates.

l. In or about May 2014, ORENSTEIN, by email, sent to SHALON and AARON two documents signed in the name of an alias used by SHALON, AARON, and ORENSTEIN, which effected a transfer of shares of a particular publicly traded stock ("Stock-6").

m. In or about May 2014, ORENSTEIN, by email, sent to SHALON and AARON documents signed in the name of an individual - in fact, an alias used by the defendants - in which

this purported individual accepted a position on the Board of Directors of the company traded publicly as Stock-7.

n. In or about May 2015, in furtherance of the scheme to manipulate Stock-7, a particular brokerage firm in the United States received a form signed in the name of the purported account owner - in fact, an alias used by the defendants - appointing "Mike Shields," that is, AARON, as agent and attorney-in-fact for the account.

(Title 18, United States Code, Section 371.)

COUNT FIVE

(Conspiracy to Commit Wire Fraud: Securities Market Manipulation Scheme)

The Grand Jury further charges:

50. The allegations contained in paragraphs 1-25, 41, and 49 of this Indictment are repeated and realleged as if fully set forth herein.

51. From at least in or about 2011, up to and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, and others known and unknown, willfully and knowingly, combined, conspired, confederated and agreed

together and with each other to violate Title 18, United States Code, Section 1343.

52. It was a part and an object of the conspiracy that the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, SHALON, AARON and ORENSTEIN perpetrated schemes to manipulate the price and trading volume of numerous publicly traded stocks, and in doing so, exchanged emails with Firm-2 in New York, New York from overseas and caused Firm-2 to send wire transfers to, and receive wire transfers from, an overseas bank account.

(Title 18, United States Code, Section 1349.)

COUNTS SIX THROUGH TWELVE
(Securities Fraud)

The Grand Jury further charges:

53. The allegations contained in paragraphs 1-25, 41 and 49 of this Indictment are repeated and realleged as if fully set forth herein.

54. On or about the dates set forth below, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, willfully and knowingly, directly and indirectly, by the use of means and instrumentalities of interstate commerce, and the mails and facilities of national securities exchanges, did use and employ, and cause to be used and employed, in connection with the purchase and sale of securities, manipulative and deceptive devices and contrivances in contravention of Title 17, Code of Federal Regulations, Section 240.10b-5, by (a) employing devices, schemes, and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, to wit, in or about the time periods set forth below, the defendants participated in schemes to manipulate the price and trading volume of the following publicly traded securities:

COUNT	SECURITY	APPROXIMATE TIME PERIOD
SIX	Stock-1	October 2011 to April 2012
SEVEN	Stock-2	August 2011 to March 2012
EIGHT	Stock-3	December 2011 to October 2012
NINE	Stock-4	March 2012 to August 2012
TEN	Stock-5	March 2012 to September 2012
ELEVEN	Stock-6	March 2014 to December 2014
TWELVE	Stock-7	April 2014 to July 2015

(Title 15, United States Code, Sections 78j(b) & 78ff; Title 17, Code of Federal Regulations, Section 240.10b-5, and Title 18, United States Code, Section 2.)

COUNT THIRTEEN
(Wire Fraud)

The Grand Jury further charges:

55. The allegations contained in paragraphs 1-25, 41, and 49 of this Indictment are repeated and realleged as if fully set forth herein.

56. From at least in or about 2011, up to and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, SHALON, AARON and ORENSTEIN perpetrated schemes to manipulate the price and trading volume of numerous publicly traded stocks, and in doing so, exchanged emails from overseas with Firm-2, located in New

York, New York, and caused Firm-2 to send wire transfers to, and receive wire transfers from, an overseas bank account.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT FOURTEEN

(Identification Document Fraud Conspiracy)

The Grand Jury further charges:

57. The allegations contained in paragraphs 1-25, 41, and 49 of this Indictment are repeated and realleged as if fully set forth herein.

58. From at least in or about 2011, up to and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, together with others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, identification document fraud, in violation of Title 18, United States Code, Sections 1028(a)(2), 1028(a)(3), and 1028(a)(7).

59. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN,

a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, and others known and unknown, willfully and knowingly would and did transfer an identification document, authentication feature, and a false identification document, in and affecting interstate and foreign commerce, knowing that such document and feature was stolen and produced without lawful authority, in violation of Title 18, United States Code, Section 1028(a)(2).

60. It was further a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, and others known and unknown, willfully and knowingly would and did possess with intent to use unlawfully and transfer unlawfully five and more identification documents, authentication features, and false identification documents, in and affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1028(a)(3).

61. It was further a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the

defendants, and others known and unknown, willfully and knowingly would and did transfer, possess, and use, without lawful authority, a means of identification of another person with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of federal law, in violation of Title 18, United States Code, Section 1028(a)(7).

Overt Acts

62. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about March 29, 2011, to open the Firm-1 Entersa account using an alias, ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendant, emailed to Firm-1 a copy of a purported passport of the United Kingdom ("False Name-1 UK Passport").

b. In or about June 2011, to obtain trading authority for JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendant, over the Firm-1 Entersa account, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and AARON caused Firm-1 to receive false personal identification information, including a fake

Florida driver's license and a Social Security Number belonging to another person.

c. In or about June 2011, to open an account at Firm-1, SHALON caused Firm-1 to receive a false purported passport of France.

d. On or about June 12, 2011, to open the Firm-2 Entersa account, ORENSTEIN sent an email from outside the United States to Firm-2 in New York, New York, containing a false purported passport of the United Kingdom, which bore a different name than that of the False Name-1 UK Passport (the "False Name-2 UK Passport").

e. On or about August 4, 2011, by email, AARON provided the False Name-2 UK Passport to Firm-1.

f. On or about March 1, 2011, working with SHALON, ORENSTEIN provided a copy of a fake United States passport to a financial institution in Azerbaijan.

g. On or about July 21, 2013, ORENSTEIN sent an email to a co-conspirator not identified herein instructing the co-conspirator to alter the name, identification information, picture, and signature of a purported Latvian passport.

h. On or about October 9, 2014, ORENSTEIN caused a brokerage firm in the United States to receive a purported identification document from the Ukraine in a particular name

("False Name-3"), a purported Serbian passport in a particular name ("False Name-4") and documents purportedly executed by False Name-3 and False Name-4 appointing "Mike Shields," that is, AARON, as agent and attorney-in-fact for accounts held in False Name-3 and False Name-4.

(Title 18, United States Code, Sections 1028(f) and 2.)

COUNT FIFTEEN

(Aggravated Identity Theft)

The Grand Jury further charges:

63. The allegations contained in paragraphs 1-25, 41, 49, and 62 of this Indictment are repeated and realleged as if fully set forth herein.

64. From in or about mid-2011 until in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, willfully and knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Section 1028A(c), to wit, SHALON AARON, and ORENSTEIN used numerous means of identification of other individuals, and the Social Security Number of another person, to commit the securities and

wire fraud crimes charged in Counts Four through Thirteen of this Indictment.

(Title 18, United States Code, Sections 1028A and 2.)

COUNT SIXTEEN

(Unlawful Internet Gambling Enforcement Act Conspiracy)

The Grand Jury further charges:

65. The allegations contained in paragraphs 1, 3, 13-14, 17-19, and 26-28 of this Indictment are repeated and realleged as if fully set forth herein.

66. From at least in or about 2007, up through and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, together with others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, violations of Title 31, United States Code, Section 5363.

67. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, unlawfully, willfully,

and knowingly, with persons engaged in the business of betting and wagering, would and did knowingly accept, in connection with the participation of another person in unlawful internet gambling, to wit, gambling in violation of New York Penal Law Sections 225.00 and 225.05 and the laws of other states where the gambling businesses operated, credit, and the proceeds of credit, extended to and on behalf of such other person, including credit extended through the use of a credit card, and an electronic fund transfer and the proceeds of an electronic fund transfer from and on behalf of such other person, and a check, draft and similar instrument which is drawn by and on behalf of such other person and is drawn on and payable at and through any financial institution, in violation of Title 31 United States Code, Sections 5363 and 5366.

Overt Acts

68. In furtherance of the conspiracy and to effect the illegal object thereof, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. On or about October 1, 2007, by email, SHALON informed another individual that his internet casino "is one of the only casinos accepting players worldwide including the United States."

b. On or about January 13, 2010, by email, SHALON arranged to send advertisements promoting SHALON's internet casinos by U.S. mail to up to one hundred thousand U.S. residents in over 30 states, including the Southern District of New York.

c. On or about December 8, 2013, ORENSTEIN, by email, informed SHALON that "casino turnover" for the month of October 2013 was \$78,910,099, which was "almost no change" from a given month approximately one year earlier, July 2012, when monthly "casino turnover" was \$75,259,052.

d. On or about December 8, 2013, by email, ORENSTEIN informed SHALON of the monthly salary cost for approximately 270 employees of their casino business in Ukraine and Hungary.

e. On or about November 17, 2014, by email, ORENSTEIN attempted to address problems experienced by United States-based players making deposits to gamble at one of SHALON's internet casinos.

f. On or about January 28, 2015, by email, SHALON approved of a promotion to be sent to United States-based players for one of SHALON's internet casinos.

g. In or about June 2015, ORENSTEIN informed SHALON, by email, that casino "profits" for the month of February 2015 were \$7,288,828.

h. Between approximately June 26, 2015, and July 7, 2015, in the Southern District of New York and elsewhere, a federal law enforcement agent, acting in an undercover capacity, gambled at one of SHALON's internet casinos with real money.

(Title 18, United States Code, Section 371.)

COUNT SEVENTEEN

(Unlawful Internet Gambling Enforcement Act)

The Grand Jury further charges:

69. The allegations contained in paragraphs 1, 3, 13-14, 17-19, 26-28, and 68 of this Indictment are repeated and realleged as if fully set forth herein.

70. From in or about 2007 up to and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, persons engaged in the business of betting and wagering and persons aiding and abetting persons in the business

of betting and wagering, did knowingly accept, in connection with the participation of another person in unlawful internet gambling, to wit, gambling through the Casino Companies in violation of New York Penal Law Sections 225.00 and 225.05 and the laws of other states where the Casino Companies operated, credit, and the proceeds of credit, extended to and on behalf of such other person, including credit extended through the use of a credit card, and an electronic fund transfer and the proceeds of an electronic fund transfer from and on behalf of such other person, and a check, draft and similar instrument which was drawn by and on behalf of such other person and was drawn on and payable at and through any financial institution.

(Title 31, United States Code, Sections 5363 and 5366; Title 18
United States Code, Section 2.)

COUNT EIGHTEEN

(Operation of an Illegal Gambling Business)

The Grand Jury further charges:

71. The allegations contained in paragraphs 1, 3, 13-14, 17-19, 26-28, and 68 of this Indictment are repeated and realleged as if fully set forth herein.

72. From at least in or about 2007 up to and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a

"Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, willfully, and knowingly did conduct, finance, manage, supervise, direct, and own all and part of an illegal gambling business, namely a business that engaged in and facilitated online casino gambling, in violation of New York State Penal Law Sections 225.00 and 225.05 and the law of other states in which the business operated, and which business involved five and more persons who conducted, financed, managed, supervised, directed, and owned all and part of that business, and which business had been and had remained in substantially continuous operation for a period in excess of thirty days and had gross revenues of \$2,000 in a single day, to wit, the defendants operated and aided and abetted the operation of the Casino Companies.

(Title 18, United States Code, Sections 1955 and 2.)

COUNT NINETEEN

(Conspiracy to Commit Wire Fraud: Unlawful Payment Processing)

The Grand Jury further charges:

73. The allegations contained in paragraphs 1, 3, 15, 17-19, and 29-34 of this Indictment are repeated and realleged as if fully set forth herein.

74. From at least in or about 2011, up to and including on or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a

"Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

75. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, the defendants participated in a scheme involving wire communications to deceive financial institutions and other financial intermediaries into processing and authorizing

payments to and from (i) the Casino Companies and United States gamblers, (ii) distributors of unlicensed pharmaceuticals around the world, (iii) purveyors of counterfeit and malicious purported anti-virus software in the United States, and (iv) Coin.mx, an unlicensed United States-based Bitcoin exchange, by disguising the transactions to create the false appearance that they were unrelated to gambling, unlicensed pharmaceutical distribution, sales of counterfeit and malicious software, and the exchange of money for Bitcoins, respectively, and thereby to obtain money of, or under the custody and control of, those financial institutions and intermediaries.

(Title 18, United States Code, Section 1349.)

COUNT TWENTY

(Conspiracy to Operate an Unlicensed Money Transmitting Business)

The Grand Jury further charges:

76. The allegations contained in paragraphs 1, 17-19, and 35-36 of the Indictment are repeated and realleged as if fully set forth herein.

77. From at least in or about April 2013 to at least in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," the defendant, and others known and

unknown, unlawfully, willfully and knowingly, did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate Title 18, United States Code, Section 1960.

78. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," the defendant, and others known and unknown, unlawfully, willfully and knowingly would and did conduct, control, manage, supervise, direct, and own all and part of an unlicensed money transmitting business, to wit, Coin.mx, d/b/a "Collectables Club," d/b/a "Currency Enthusiasts" ("Coin.mx") in violation of Title 18, United States Code, Section 1960.

Overt Acts

79. In furtherance of the conspiracy and to effect the illegal object thereof, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," the defendant, and others known and unknown, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. On or about November 22, 2013, SHALON agreed with a co-conspirator not named herein to miscode credit card

transactions processed on behalf of Coin.mx in an effort to avoid detection of the unlawful Coin.mx scheme by credit card issuers.

b. From in or about December 2013, through at least in or about November 2014, in an effort to promote Coin.mx and expand its customer base, a co-conspirator not identified herein exchanged numerous emails with a company in the Southern District of New York.

c. In or about August 2014, in the Southern District of New York, a co-conspirator not identified herein opened a bank account for use by Coin.mx.

d. In September 2014, SHALON met with certain co-conspirators not identified herein and discussed the operation of Coin.mx.

e. From in or about November 2014, through at least in or about December 2014, a co-conspirator not named herein exchanged numerous emails from the Southern District of New York with individuals outside the Southern District of New York in furtherance of their efforts to secure bank accounts through which Coin.mx could operate unlawfully.

(Title 18, United States Code, Section 371.)

COUNT TWENTY-ONE

(Operation of an Unlicensed Money Transmitting Business)

The Grand Jury further charges:

80. The allegations contained in paragraphs 1, 3, 17-19 35-36, and 79 of the Indictment are repeated and realleged as if fully set forth herein.

81. From at least in or about April 2013 to at least in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," the defendant, willfully and knowingly did conduct, control, manage, supervise, direct, and own all or part of an unlicensed money transmitting business affecting interstate and foreign commerce, to wit, Coin.mx, an internet-based Bitcoin exchange business, which failed to comply with the money transmitting business registration requirements set forth in federal law and regulations.

(Title 18, United States Code, Sections 1960 and 2.)

COUNT TWENTY-TWO

(Money Laundering Conspiracy: Securities Market
Manipulation Scheme)

The Grand Jury further charges:

82. The allegations contained in paragraphs 1-25, 41, 49, and 62 of this Indictment are repeated and realleged as if fully set forth herein.

83. From at least 2011, up to and including in or about July 2015, in the Southern District of New York and elsewhere, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to violate Title 18, United States Code, Section 1956(a)(1)(B)(i) and 1957(a).

84. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, in an offense involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions represented the proceeds of some form of unlawful activity, willfully and knowingly would and did conduct and attempt to conduct such financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, the proceeds of the wire fraud and securities fraud offenses charged in Counts Four through Thirteen of this Indictment,

knowing that the transaction was designed in whole or in part to conceal and disguise the nature, the location, the source, the ownership and the control or the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

85. It was a further part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, within the United States and involving United States persons, in an offense involving and affecting interstate and foreign commerce, willfully and knowingly would and did engage and attempt to engage in monetary transactions in criminally derived property of a value greater than \$10,000 that was derived from specified unlawful activity, to wit, the proceeds of the wire fraud and securities fraud offenses charged in Counts Four through Thirteen of this Indictment, in violation of Title 18, United States Code, Section 1957.

Overt Acts

86. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about February 5, 2012, JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendant, by email instructed Firm-2, located in New York, New York, to wire \$241,000 from the Entersa Firm-2 account to the Entersa Cyprus Account.

b. On or about February 8, 2012, by email, AARON instructed Firm-2, in New York, New York, to wire \$191,000 from the Entersa Firm-2 account to the Entersa Cyprus Account.

c. On or about February 13, 2012, by email, AARON instructed Firm-2 to wire \$542,000 from the Entersa Firm-2 account to the Entersa Cyprus Account.

d. On or about August 1, 2011, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," the defendant, instructed an individual not identified herein to transfer \$27,560 from the Entersa Cyprus Account to Aaron's Warmkal Account.

e. On or about June 12, 2011, by email from outside the United States to Firm-2, ZIV ORENSTEIN, a/k/a "Aviv Stein,"

a/k/a "John Avery," the defendant, opened the Firm-2 Entersa using an alias and a false passport.

(Title 18, United States Code, Section 1956(h).)

COUNT TWENTY-THREE

(Money Laundering Conspiracy: Unlawful Internet Gambling and Payment Processing)

The Grand Jury further charges:

87. The allegations contained in paragraphs 1, 3, 13-14, 17-19, 26-32, and 68 of this Indictment are repeated and realleged as if fully set forth herein.

88. From at least 2011, up to and including in or about July 2015, in the Southern District of New York and elsewhere, "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to violate Title 18, United States Code, Section 1956(a)(1)(B)(i) and 1957(a).

89. It was a part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, in an offense

involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions represented the proceeds of some form of unlawful activity, willfully and knowingly would and did conduct and attempt to conduct such financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, the proceeds of the gambling and wire fraud offenses charged in Counts Sixteen through Nineteen of this Indictment, knowing that the transaction was designed in whole or in part to conceal and disguise the nature, the location, the source, the ownership and the control or the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

90. It was a further part and an object of the conspiracy that GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendants, and others known and unknown, within the United States and involving United States persons, in an offense involving and affecting interstate and foreign commerce, willfully and knowingly would and did engage and attempt to engage in monetary transactions in criminally derived property of a value greater than \$10,000 that was derived from specified

unlawful activity, to wit, the proceeds of the gambling and wire fraud offenses charged in Counts Sixteen through Nineteen of this Indictment.

Overt Acts

91. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about 2013, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," the defendant, caused millions of dollars in unlawful profits from the operation of his payment processing business to be sent from bank accounts in Azerbaijan to a Swiss bank account owned and controlled by SHALON in the name of another shell company.

b. On or about June 26, 2015, after an undercover law enforcement agent in the Southern District of New York gambled at one of SHALON's internet casinos using a debit card, SHALON and his co-conspirators caused the agent's debit card statement falsely to reflect that the money spent by that agent through the casino website was for a purchase at "houses4petz.com," a phony merchant.

c. Throughout in or about 2012 and 2013, SHALON and ZIV ORENSTEIN, a/k/a "John Avery," a/k/a "Aviv Stein," the defendant, caused millions of dollars in unlawful gambling proceeds and profits to be sent to, from and between Cyprus-based bank accounts in the names of shell companies, including shell companies controlled by SHALON and ORENSTEIN using aliases and false identification.

(Title 18, United States Code, Section 1956(h).)

FORFEITURE ALLEGATIONS

92. As a result of committing one or more of the offenses alleged in Counts One through Three of this Indictment, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham", and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B) any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses alleged in Counts One through Three and, pursuant to Title 18, United States Code, Section 1030(i), any interest in any personal property that was used or intended to be used to commit or facilitate the commission of the offenses alleged in Counts One through Three, and any property, real or personal, constituting or derived from any proceeds obtained

directly or indirectly as a result of the offenses alleged in Counts One through Three.

93. As a result of committing one or more of the offenses charged in Counts Four through Thirteen, and Eighteen through Twenty, of this Indictment, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, any and all property, real and personal, which constitutes or is derived from proceeds traceable to the offenses alleged in Counts Four through Thirteen, and Eighteen through Twenty.

94. As a result of committing the offense alleged in Count Fourteen of this Indictment, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," JOSHUA SAMUEL AARON, a/k/a "Mike Shields," and ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery," the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting or derived from proceeds obtained directly or indirectly as a result of the offense

alleged in Count Fourteen and, pursuant to Title 18, United States Code, Section 1028(b)(5), any personal property used or intended to be used to commit the offense alleged in Count Fourteen.

95. As a result of committing one or more of the offenses alleged in Counts Twenty One through Twenty Three of this Indictment, GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," and JOSHUA SAMUEL AARON, a/k/a "Mike Shields," the defendants, shall forfeit to the United States pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in the offenses alleged in Counts Twenty One through Twenty Three, or any property traceable to such property.

Substitute Assets Provision

96. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 982(b), Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461, to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981, 982, 1028 & 1030;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)


FOREPERSON


PREET BHARARA
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

GERY SHALON,
a/k/a "Garri Shalelashvili," a/k/a
"Gabriel," a/k/a "Gabi," a/k/a "Phillipe
Mousset," a/k/a "Christopher Engeham,"
JOSHUA SAMUEL AARON,
a/k/a "Mike Shields," and
ZIV ORENSTEIN,
a/k/a "Aviv Stein," a/k/a "John Avery,"

Defendants.

SEALED SUPERSEDING INDICTMENT

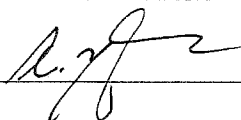
S1 15 Cr. 333 (LTS)

(15 U.S.C. §§ 78j(b) & 78ff; 17 C.F.R. §
240.10b-5; 18 U.S.C. §§ 371, 1030, 1343,
1349, 1028(f), 1028A, 1955, 1956, 1960 &
2, 31 U.S.C. §§ 5363 & 5366)

PREET BHARARA

United States Attorney.

TRUE BILL



FOREPERSON

10/22/15 - Filed Sealed Superseding Indictment
cc

J. Pak.
USMD

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 14-3514

FEDERAL TRADE COMMISSION

v.

WYNDHAM WORLDWIDE CORPORATION,
a Delaware Corporation
WYNDHAM HOTEL GROUP, LLC,
a Delaware limited liability company;
WYNDHAM HOTELS AND RESORTS, LLC,
a Delaware limited liability company;
WYNDHAM HOTEL MANAGEMENT INCORPORATED,
a Delaware Corporation

Wyndham Hotels and Resorts, LLC,
Appellant

On Appeal from the United States District Court
for the District of New Jersey
(D.C. Civil Action No. 2-13-cv-01887)
District Judge: Honorable Esther Salas

Argued March 3, 2015

Before: AMBRO, SCIRICA, and ROTH, Circuit Judges

(Opinion filed: August 24, 2015)

Kenneth W. Allen, Esquire
Eugene F. Assaf, Esquire (Argued)
Christopher Landau, Esquire
Susan M. Davies, Esquire
Michael W. McConnell, Esquire
Kirkland & Ellis
655 15th Street, N.W., Suite 1200
Washington, DC 20005

David T. Cohen, Esquire
Ropes & Gray
1211 Avenue of the Americas
New York, NY 10036

Douglas H. Meal, Esquire
Ropes & Gray
800 Boylston Street, Prudential Tower
Boston, MA 02199

Jennifer A. Hradil, Esquire
Justin T. Quinn, Esquire
Gibbons
One Gateway Center
Newark, NJ 07102

Counsel for Appellants

Jonathan E. Nuechterlein
General Counsel
David C. Shonka, Sr.
Principal Deputy General Counsel
Joel R. Marcus, Esquire (Argued)
David L. Sieradzki, Esquire
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Counsel for Appellee

Sean M. Marotta, Esquire
Catherine E. Stetson, Esquire
Harriet P. Pearson, Esquire
Bret S. Cohen, Esquire
Adam A. Cooke, Esquire
Hogan Lovells US LLP
555 Thirteenth Street, N.W.
Columbia Square
Washington, DC 20004

Kate Comerford Todd, Esquire
Steven P. Lehotsky, Esquire
Sheldon Gilbert, Esquire
U.S. Chamber Litigation Center, Inc.
1615 H Street, N.W.
Washington, DC 20062

Banks Brown, Esquire
McDermott Will & Emery LLP
340 Madison Ave.
New York, NY 10713

Karen R. Harned, Esquire
National Federation of Independent Business
Small Business Legal Center
1201 F Street, N.W., Suite 200
Washington, DC 20004

Counsel for Amicus Appellants
Chamber of Commerce of the USA;
American Hotel & Lodging Association;
National Federation of Independent Business.

Cory L. Andrews, Esquire
Richard A. Samp, Esquire
Washington Legal Foundation
2009 Massachusetts Avenue, N.W.
Washington, DC 20036

John F. Cooney, Esquire
Jeffrey D. Knowles, Esquire
Mitchell Y. Mirviss, Esquire
Leonard L. Gordon, Esquire
Randall K. Miller, Esquire
Venable LLC
575 7th Street, N.W.
Washington, DC 20004

Counsel for Amicus Appellants
Electronic Transactions Association,
Washington Legal Foundation

Scott M. Michelman, Esquire
Jehan A. Patterson, Esquire
Public Citizen Litigation Group

1600 20th Street, N.W.
Washington, DC 20009

Counsel for Amicus Appellees
Public Citizen Inc.; Consumer Action;
Center for Digital Democracy.

Marc Rotenberg, Esquire
Alan Butler, Esquire
Julia Horwitz, Esquire
John Tran, Esquire
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009

Catherine N. Crump, Esquire
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004

Chris Jay Hoofnagle, Esquire
Samuelson Law, Technology & Public Policy Clinic
U.C. Berkeley School of Law
Berkeley, CA 94720

Justin Brookman, Esquire
G.S. Hans, Esquire
Center for Democracy & Technology
1634 I Street N.W. Suite 1100
Washington, DC 20006

Lee Tien, Esquire
Electronic Frontier Foundation

815 Eddy Street
San Francisco, CA 94109

Counsel for Amicus Appellees
Electronic Privacy Information Center,
American Civil Liberties Union,
Samuelson Law, Technology & Public Policy Clinic,
Center for Democracy & Technology,
Electronic Frontier Foundation

OPINION OF THE COURT

AMBRO, Circuit Judge

The Federal Trade Commission Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45(a). In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement.

On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation’s computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over \$10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham’s conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham’s motion to dismiss, and we granted interlocutory appeal on two issues:

whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision.¹ We affirm the District Court.

I. Background

A. Wyndham's Cybersecurity

Wyndham Worldwide is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries.² Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes. Wyndham “manage[s]” these systems and requires the hotels to “purchase and configure” them to its own specifications. Compl. at ¶ 15, 17. It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels.

¹ On appeal, Wyndham also argues that the FTC fails the pleading requirements of an unfairness claim. As Wyndham did not request and we did not grant interlocutory appeal on this issue, we decline to address it.

² In addition to Wyndham Worldwide, the defendant entities are Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LCC, and Wyndham Hotel Management, Inc. For convenience, we refer to all defendants jointly as Wyndham.

The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, “taken together, unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.” *Id.* at ¶ 24. This claim is fleshed out as follows.

1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text.

2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain “remote access to at least one hotel’s system,” which was developed by Micros Systems, Inc., the user ID and password were both “micros.” *Id.* at ¶ 24(f).

3. Wyndham failed to use “readily available security measures”—such as firewalls—to “limit access between [the] hotels’ property management systems, . . . corporate network, and the Internet.” *Id.* at ¶ 24(a).

4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented “adequate information security policies and procedures.” *Id.* at ¶ 24(c). Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham’s network even though “default user IDs and passwords were enabled . . . , which were easily available to hackers through simple Internet searches.” *Id.* And, because it failed to maintain an “adequate[] inventory [of] computers connected to [Wyndham’s] network [to] manage the devices,” it was unable to identify the source of at least one of the cybersecurity attacks. *Id.* at ¶ 24(g).

5. Wyndham failed to “adequately restrict” the access of third-party vendors to its network and the servers of Wyndham-branded hotels. *Id.* at ¶ 24(j). For example, it did not “restrict[] connections to specified IP addresses or grant[] temporary, limited access, as necessary.” *Id.*

6. It failed to employ “reasonable measures to detect and prevent unauthorized access” to its computer network or to “conduct security investigations.” *Id.* at ¶ 24(h).

7. It did not follow “proper incident response procedures.” *Id.* at ¶ 24(i). The hackers used similar methods in each attack, and yet Wyndham failed to monitor its network for malware used in the previous intrusions.

Although not before us on appeal, the complaint also raises a deception claim, alleging that since 2008 Wyndham has published a privacy policy on its website that overstates the company’s cybersecurity.

We safeguard our Customers’ personally identifiable information by using industry standard practices. Although “guaranteed security” does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such [i]nformation consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for

encrypting data. This protects confidential information—such as credit card numbers, online forms, and financial data—from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain “fire walls” and other appropriate safeguards

Id. at ¶ 21. The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data.

B. The Three Cybersecurity Attacks

As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham’s network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first broke into the local network of a hotel in Phoenix, Arizona, which was connected to Wyndham’s network and the Internet. They then used the brute-force method—repeatedly guessing users’ login IDs and passwords—to access an administrator account on Wyndham’s network. This enabled them to obtain consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to a domain in Russia.

In March 2009, hackers attacked again, this time by accessing Wyndham’s network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered “memory-scraping malware” used in the previous attack on more than thirty hotels’ computer systems. *Id.* at ¶ 34. The FTC asserts that, due to Wyndham’s “failure to monitor [the network] for

the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months.” *Id.* In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.

Hackers in late 2009 breached Wyndham’s cybersecurity a third time by accessing an administrator account on one of its networks. Because Wyndham “had still not adequately limited access between . . . the Wyndham-branded hotels’ property management systems, [Wyndham’s network], and the Internet,” the hackers had access to the property management servers of multiple hotels. *Id.* at ¶ 37. Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems of 28 hotels.

The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least \$10.6 million in fraud loss. It further states that consumers suffered financial injury through “unreimbursed fraudulent charges, increased costs, and lost access to funds or credit,” *Id.* at ¶ 40, and that they “expended time and money resolving fraudulent charges and mitigating subsequent harm.” *Id.*

C. Procedural History

The FTC filed suit in the U.S. District Court for the District of Arizona in June 2012 claiming that Wyndham engaged in “unfair” and “deceptive” practices in violation of § 45(a). At Wyndham’s request, the Court transferred the case to the U.S. District Court for the District of New Jersey.

Wyndham then filed a Rule 12(b)(6) motion to dismiss both the unfair practice and deceptive practice claims. The District Court denied the motion but certified its decision on the unfairness claim for interlocutory appeal. We granted Wyndham’s application for appeal.

II. Jurisdiction and Standards of Review

The District Court has subject-matter jurisdiction under 28 U.S.C. §§ 1331, 1337(a), and 1345. We have jurisdiction under 28 U.S.C. § 1292(b).

We have plenary review of a district court’s ruling on a motion to dismiss for failure to state a claim under Rule 12(b)(6). *Farber v. City of Paterson*, 440 F.3d 131, 134 (3d Cir. 2006). In this review, “we accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief.” *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 374 n.7 (3d Cir. 2002).

III. FTC’s Regulatory Authority Under § 45(a)

A. Legal Background

The Federal Trade Commission Act of 1914 prohibited “unfair methods of competition in commerce.” Pub. L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)). Congress “explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase ‘unfair methods of competition’ . . . by enumerating the particular practices to which it was intended to apply.” *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239–40 (1972) (citing S. Rep. No. 63-597, at 13 (1914)); *see also* S. Rep. No. 63-597, at 13 (“The committee gave *careful consideration* to

the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce It concluded that . . . there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others.” (emphasis added)). The takeaway is that Congress designed the term as a “flexible concept with evolving content,” *FTC v. Bunte Bros.*, 312 U.S. 349, 353 (1941), and “intentionally left [its] development . . . to the Commission,” *Atl. Ref. Co. v. FTC*, 381 U.S. 357, 367 (1965).

After several early cases limited “unfair methods of competition” to practices harming competitors and not consumers, *see, e.g., FTC v. Raladam Co.*, 283 U.S. 643 (1931), Congress inserted an additional prohibition in § 45(a) against “unfair or deceptive acts or practices in or affecting commerce,” Wheeler-Lea Act, Pub. L. No. 75-447, § 5, 52 Stat. 111, 111 (1938).

For the next few decades, the FTC interpreted the unfair-practices prong primarily through agency adjudication. But in 1964 it issued a “Statement of Basis and Purpose” for unfair or deceptive advertising and labeling of cigarettes, 29 Fed. Reg. 8324, 8355 (July 2, 1964), which explained that the following three factors governed unfairness determinations:

- (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes

substantial injury to consumers (or competitors or other businessmen).

Id. Almost a decade later, the Supreme Court implicitly approved these factors, apparently acknowledging their applicability to contexts other than cigarette advertising and labeling. *Sperry*, 405 U.S. at 244 n.5. The Court also held that, under the policy statement, the FTC could deem a practice unfair based on the third prong—substantial consumer injury—without finding that at least one of the other two prongs was also satisfied. *Id.*

During the 1970s, the FTC embarked on a controversial campaign to regulate children's advertising through the unfair-practices prong of § 45(a). At the request of Congress, the FTC issued a second policy statement in 1980 that clarified the three factors. FTC Unfairness Policy Statement, Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Senate Comm. on Commerce, Sci., and Transp. (Dec. 17, 1980), *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) [hereinafter 1980 Policy Statement]. It explained that public policy considerations are relevant in determining whether a particular practice causes substantial consumer injury. *Id.* at 1074–76. Next, it “abandoned” the “theory of immoral or unscrupulous conduct . . . altogether” as an “independent” basis for an unfairness claim. *Int'l Harvester Co.*, 104 F.T.C. at 1061 n.43; 1980 Policy Statement, *supra* at 1076 (“The Commission has . . . never relied on [this factor] as an independent basis for a finding of unfairness, and it will act in the future only on the basis of the [other] two.”). And finally, the Commission explained that “[u]njustified consumer injury is the primary focus of the FTC Act” and that such an injury “[b]y itself . . . can be sufficient to warrant a finding of unfairness.” 1980 Policy Statement, *supra* at 1073. This “does not mean that every consumer injury is legally ‘unfair.’” *Id.* Indeed,

[t]o justify a finding of unfairness the injury must satisfy three tests. [1] It must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided.

Id.

In 1994, Congress codified the 1980 Policy Statement at 15 U.S.C. § 45(n):

The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695. Like the 1980 Policy Statement, § 45(n) requires substantial injury that is not reasonably avoidable by consumers and that is not outweighed by the benefits to consumers or competition. It also acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive.

B. Plain Meaning of Unfairness

Wyndham argues (for the first time on appeal) that the three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions of an unfair practice and that the plain meaning of the word “unfair” imposes independent requirements that are not met here. Arguably, § 45(n) may not identify all of the requirements for an unfairness claim. (While the provision forbids the FTC from declaring an act unfair “unless” the act satisfies the three specified requirements, it does not answer whether these are the *only* requirements for a finding of unfairness.) Even if so, some of Wyndham’s proposed requirements are unpersuasive, and the rest are satisfied by the allegations in the FTC’s complaint.

First, citing *FTC v. R.F. Keppel & Brother, Inc.*, 291 U.S. 304 (1934), Wyndham argues that conduct is only unfair when it injures consumers “through unscrupulous or unethical behavior.” Wyndham Br. at 20–21. But *Keppel* nowhere says that unfair conduct must be unscrupulous or unethical. Moreover, in *Sperry* the Supreme Court rejected the view that the FTC’s 1964 policy statement required unfair conduct to be “unscrupulous” or “unethical.” 405 U.S. at 244 n.5.³

³ *Id.* (“[Petitioner] argues that . . . [the 1964 statement] commits the FTC to the view that misconduct in respect of the third of these criteria is not subject to constraint as ‘unfair’ absent a concomitant showing of misconduct according to the first or second of these criteria. But all the FTC said in the [1964] statement . . . was that ‘[t]he wide variety of decisions interpreting the elusive concept of unfairness *at least* makes clear that a method of selling violates Section 5 if it is exploitive or inequitable and if, in addition to being morally objectionable, it is seriously

Wyndham points to no subsequent FTC policy statements, adjudications, judicial opinions, or statutes that would suggest any change since *Sperry*.

Next, citing one dictionary, Wyndham argues that a practice is only “unfair” if it is “not equitable” or is “marked by injustice, partiality, or deception.” Wyndham Br. at 18–19 (citing *Webster’s Ninth New Collegiate Dictionary* (1988)). Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

We recognize this analysis of unfairness encompasses some facts relevant to the FTC’s deceptive practices claim. But facts relevant to unfairness and deception claims frequently overlap. *See, e.g., Am. Fin. Servs. Ass’n v. FTC*, 767 F.2d 957, 980 n.27 (D.C. Cir. 1985) (“The FTC has determined that . . . making unsubstantiated advertising claims may be both an unfair and a deceptive practice.”); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1367 (11th Cir. 1988) (“[A] practice may be both deceptive and unfair . . .”).⁴ We cannot completely disentangle the two

detrimental to consumers or others.” (emphasis and some alterations in original, citation omitted)).

⁴ The FTC has on occasion described deception as a subset of unfairness. *See Int’l Harvester Co.*, 104 F.T.C. at 1060 (“The Commission’s unfairness jurisdiction provides a more general basis for action against acts or practices which cause significant consumer injury. This part of our jurisdiction is

theories here. The FTC argued in the District Court that consumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had published a

broader than that involving deception, and the standards for its exercise are correspondingly more stringent. . . . [U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset.”); *Figgie Int’l*, 107 F.T.C. 313, 373 n.5 (1986) (“[U]nfair practices are not always deceptive but deceptive practices are always unfair.”); *Orkin Exterminating Co.*, 108 F.T.C. 263, 363 n.78 (1986). So have several FTC staff members. See, e.g., J. Howard Beales, Director of the Bureau of Consumer Protection, FTC, Marketing and Public Policy Conference, The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003) (“Although, in the past, they have sometimes been viewed as mutually exclusive legal theories, Commission precedent incorporated in the statutory codification makes clear that deception is properly viewed as a subset of unfairness.”); Neil W. Averitt, *The Meaning of “Unfair Acts or Practices” in Section 5 of the Federal Trade Commission Act*, 70 Geo. L.J. 225, 265–66 (1981) (“Although deception is generally regarded as a separate aspect of section 5, in its underlying rationale it is really just one specific form of unfair consumer practice [For example, the] Commission has held that it is deceptive for a merchant to make an advertising claim for which he lacks a reasonable basis, regardless of whether the claim is eventually proven true or false Precisely because unsubstantiated ads are deceptive in this manner, . . . they also affect the exercise of consumer sovereignty and thus constitute an unfair act or practice.”).

misleading privacy policy that overstated its cybersecurity. Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant at 5, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887) ("Consumers could not take steps to avoid Wyndham's unreasonable data security [before providing their personal information] because Wyndham falsely told consumers that it followed 'industry standard practices.'"); see JA 203 ("On the reasonable avoidable part, . . . consumers certainly would not have known that Wyndham had unreasonable data security practices in this case We also allege that in [Wyndham's] privacy policy they deceive consumers by saying we do have reasonable security data practices. That is one way consumers couldn't possibly have avoided providing a credit card to a company."). Wyndham did not challenge this argument in the District Court nor does it do so now. If Wyndham's conduct satisfies the reasonably avoidable requirement at least partially because of its privacy policy—an inference we find plausible at this stage of the litigation—then the policy is directly relevant to whether Wyndham's conduct was unfair.⁵

Continuing on, Wyndham asserts that a business “does not treat its customers in an ‘unfair’ manner when the business *itself* is victimized by criminals.” Wyndham Br. at

⁵ No doubt there is an argument that consumers could not reasonably avoid injury even absent the misleading privacy policy. See, e.g., James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. Ill. J.L. Tech. & Pol'y. 1 (arguing that consumers may care about data privacy, but be unable to consider it when making credit card purchases). We have no occasion to reach this question, as the parties have not raised it.

21 (emphasis in original). It offers no reasoning or authority for this principle, and we can think of none ourselves. Although unfairness claims “usually involve actual and completed harms,” *Int’l Harvester*, 104 F.T.C. at 1061, “they may also be brought on the basis of likely rather than actual injury,” *id.* at 1061 n.45. And the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs. 15 U.S.C. § 45(n) (“[An unfair act or practice] causes or is *likely to cause* substantial injury” (emphasis added)). More importantly, that a company’s conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms. See Restatement (Second) of Torts § 449 (1965) (“If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby.”); *Westfarm Assocs. v. Wash. Suburban Sanitary Comm’n*, 66 F.3d 669, 688 (4th Cir. 1995) (“Proximate cause may be found even where the conduct of the third party is . . . criminal, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable.”). For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks.

Finally, Wyndham posits a *reductio ad absurdum*, arguing that if the FTC’s unfairness authority extends to Wyndham’s conduct, then the FTC also has the authority to “regulate the locks on hotel room doors, . . . to require every store in the land to post an armed guard at the door,” Wyndham Br. at 23, and to sue supermarkets that are “sloppy about sweeping up banana peels,” Wyndham Reply Br. at 6. The argument is alarmist to say the least. And it invites the

tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a).

We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of "unfair."

C. Subsequent Congressional Action

Wyndham next argues that, even if cybersecurity were covered by § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity. A recent amendment to the Fair Credit Reporting Act directed the FTC and other agencies to develop regulations for the proper disposal of consumer data. *See* Pub. L. No. 108-159, § 216(a), 117 Stat. 1952, 1985-86 (2003) (codified as amended at 15 U.S.C. § 1681w). The Gramm-Leach-Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information. *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436-37 (1999) (codified as amended at 15 U.S.C. § 6801(b)). And the Children's Online Privacy Protection Act ordered the FTC to promulgate regulations requiring children's websites, among other things, to provide notice of "what information is collected from children . . . , how the operator uses such information, and the operator's disclosure practices for such information." Pub. L. No. 105-277, § 1303, 112 Stat. 2681, 2681-730-732 (1998) (codified as amended at 15 U.S.C. § 6502).⁶ Wyndham contends these "tailored grants of

⁶ Wyndham also points to a variety of cybersecurity bills that Congress has considered and not passed. "[S]ubsequent legislative history . . . is particularly dangerous ground on

substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field.” Wyndham Br. at 25. Citing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000), Wyndham concludes that Congress excluded cybersecurity from the FTC’s unfairness authority by enacting these measures.

We are not persuaded. The inference to congressional intent based on post-enactment legislative activity in *Brown & Williamson* was far stronger. There, the Food and Drug Administration had repeatedly disclaimed regulatory authority over tobacco products for decades. *Id.* at 144. During that period, Congress enacted six statutes regulating tobacco. *Id.* at 143–44. The FDA later shifted its position, claiming authority over tobacco products. The Supreme Court held that Congress excluded tobacco-related products from the FDA’s authority in enacting the statutes. As tobacco products would necessarily be banned if subject to the FDA’s regulatory authority, any interpretation to the contrary would contradict congressional intent to regulate rather than ban tobacco products outright. *Id.* 137–39; *Massachusetts v. EPA*, 549 U.S. 497, 530–31 (2007). Wyndham does not argue that recent privacy laws *contradict* reading corporate cybersecurity into § 45(a). Instead, it merely asserts that Congress had no reason to enact them if the FTC could already regulate cybersecurity through that provision. Wyndham Br. at 25–26.

We disagree that Congress lacked reason to pass the recent legislation if the FTC already had regulatory authority over some cybersecurity issues. The Fair Credit Reporting

which to rest an interpretation of a prior statute when it concerns . . . a proposal that does not become law.” *Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990).

Act requires (rather than authorizes) the FTC to issue regulations, 15 U.S.C. § 1681w (“The Federal Trade Commission . . . *shall* issue final regulations requiring” (emphasis added)); *id.* § 1681m(e)(1)(B) (“The [FTC and other agencies] *shall* jointly . . . prescribe regulations requiring each financial institution” (emphasis added)), and expands the scope of the FTC’s authority, *id.* § 1681s(a)(1) (“[A] violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce . . . and shall be subject to enforcement by the [FTC] . . . irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the [FTC] Act.”). The Gramm-Leach-Bliley Act similarly requires the FTC to promulgate regulations, *id.* § 6801(b) (“[The FTC] shall establish appropriate standards for the financial institutions subject to [its] jurisdiction”), and relieves some of the burdensome § 45(n) requirements for declaring acts unfair, *id.* § 6801(b) (“[The FTC] shall establish appropriate standards . . . to protect against unauthorized access to or use of . . . records . . . which could result in substantial harm *or inconvenience to any customer.*” (emphasis added)). And the Children’s Online Privacy Protection Act required the FTC to issue regulations and empowered it to do so under the procedures of the Administrative Procedure Act, *id.* § 6502(b) (citing 5 U.S.C. § 553), rather than the more burdensome Magnuson-Moss procedures under which the FTC must usually issue regulations, 15 U.S.C. § 57a. Thus none of the recent privacy legislation was “inexplicable” if the FTC already had some authority to regulate corporate cybersecurity through § 45(a).

Next, Wyndham claims that the FTC’s interpretation of § 45(a) is “inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here.” Wyndham Br. at 28. Yet again we disagree. In two of the

statements cited by Wyndham, the FTC clearly said that some cybersecurity practices are “unfair” under the statute. *See Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 2358081, at *6 (June 15, 2011) (statement of Edith Ramirez, Comm’r, FTC) (“[T]he Commission enforces the FTC Act’s proscription against unfair . . . acts . . . in cases where a business[’s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.”); *Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 1971214, at *7 (May 4, 2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection) (same).

In the two other cited statements, given in 1998 and 2000, the FTC only acknowledged that it cannot require companies to adopt “fair information practice policies.” *See* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 34 (2000) [hereinafter *Privacy Online*]; *Privacy in Cyberspace: Hearing Before the Subcomm. on Telecomms., Trade & Consumer Prot. of the H. Comm. on Commerce*, 1998 WL 546441 (July 21, 1998) (statement of Robert Pitofsky, Chairman, FTC). These policies would protect consumers from far more than the kind of “substantial injury” typically covered by § 45(a). In addition to imposing some cybersecurity requirements, they would require companies to give notice about what data they collect from consumers, to permit those consumers to decide how the data is used, and to permit them to review and correct inaccuracies. *Privacy Online*, *supra* at 36–37. As the FTC explained in the District Court, the primary concern driving the adoption of these policies in the late 1990s was that “companies . . . were capable of *collecting* enormous amounts of information about consumers, and people were suddenly realizing this.” JA 106 (emphasis added). The FTC

thus could not require companies to adopt broad fair information practice policies because they were “just collecting th[e] information, and consumers [were not] injured.” *Id.*; *see also* Order Denying Respondent LabMD’s Motion to Dismiss, No. 9357, slip op. at 7 (Jan. 16, 2014) [hereinafter *LabMD Order* or *LabMD*] (“[T]he sentences from the 1998 and 2000 reports . . . simply recognize that the Commission’s existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern (such as aspects of children’s online privacy)” (emphasis in original)). Our conclusion is this: that the FTC later brought unfairness actions against companies whose inadequate cybersecurity resulted in consumer harm is not inconsistent with the agency’s earlier position.

Having rejected Wyndham’s arguments that its conduct cannot be unfair, we assume for the remainder of this opinion that it was.

IV. Fair Notice

A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained “fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.” *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (internal quotation marks omitted). Wyndham claims that, notwithstanding whether its conduct was unfair under § 45(a),

the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow.⁷

A. Legal Standard

The level of required notice for a person to be subject to liability varies by circumstance. In *Bouie v. City of Columbia*, the Supreme Court held that a “judicial construction of a criminal statute” violates due process if it is “unexpected and indefensible by reference to the law which had been expressed prior to the conduct in issue.” 378 U.S. 347, 354 (1964) (internal quotation marks omitted); *see also* *Rogers v. Tennessee*, 532 U.S. 451, 457 (2001); *In re Surrick*, 338 F.3d 224, 233–34 (3d Cir. 2003). The precise meaning of “unexpected and indefensible” is not entirely clear, *United States v. Lata*, 415 F.3d 107, 111 (1st Cir. 2005), but we and our sister circuits frequently use language implying that a conviction violates due process if the defendant could not reasonably foresee that a court might adopt the new interpretation of the statute.⁸

⁷ We do not read Wyndham’s briefing as raising a meaningful argument under the “discriminatory enforcement” prong. A few sentences in a reply brief are not enough. *See* Wyndham Reply Br. at 26 (“To provide the notice required by due process, a statement must in some sense declare what conduct the law proscribes and thereby constrain enforcement discretion Here, the consent decrees at issue . . . do not limit the Commission’s enforcement authority in any way.” (citation omitted)).

⁸ *See Ortiz v. N.Y.S. Parole*, 586 F.3d 149, 159 (2d Cir. 2009) (holding that the “unexpected and indefensible” standard “requires only that the law . . . not lull the potential defendant

The fair notice doctrine extends to civil cases, particularly where a penalty is imposed. *See Fox Television Stations, Inc.*, 132 S. Ct. at 2317–20; *Boutilier v. INS*, 387 U.S. 118, 123 (1967). “Lesser degrees of specificity” are allowed in civil cases because the consequences are smaller than in the criminal context. *San Filippo v. Bongiovanni*, 961 F.2d 1125, 1135 (3d Cir. 1992). The standards are especially lax for civil statutes that regulate economic activities. For those statutes, a party lacks fair notice when the relevant standard is “so vague as to be no rule or standard at all.”

into a *false sense of security*, giving him *no reason even to suspect* that his conduct *might* be within its scope.” (emphases added)); *In re Surrick*, 338 F.3d at 234 (“[We] reject [the] contention that . . . nothing in the history of [the relevant provision] had stated *or even foreshadowed* that reckless conduct *could* violate it. Indeed, in view of the foregoing, the [state court’s] decision . . . was neither ‘unexpected’ nor ‘indefensible’ by reference to the law which had been expressed prior to the conduct in issue.” (emphases added)); *Warner v. Zent*, 997 F.2d 116, 125 (6th Cir. 1993) (“‘The underlying principle is that no man shall be held criminally responsible for conduct which *he could not reasonably understand* to be proscribed.’” (emphasis added) (quoting *United States v. Harriss*, 347 U.S. 612, 617 (1954))); *id.* at 127 (“It was *by no means unforeseeable* . . . that the [court] would [construe the statute as it did].” (emphasis added)); *see also Lata*, 415 F.3d at 112 (“[S]omeone in [the defendant’s] position *could not reasonably be surprised* by the sentence he eventually received We reserve for the future the case . . . in which a sentence is imposed . . . that is *higher than any that might realistically have been imagined* at the time of the crime” (emphases added)).

CMR D.N. Corp. v. City of Phila., 703 F.3d 612, 631–32 (3d Cir. 2013) (internal quotation marks omitted).⁹

A different set of considerations is implicated when agencies are involved in statutory or regulatory interpretation. Broadly speaking, agencies interpret in at least three contexts. One is where an agency administers a statute without any special authority to create new rights or obligations. When disputes arise under this kind of agency interpretation, the courts give respect to the agency’s view to the extent it is persuasive, but they retain the primary responsibility for construing the statute.¹⁰ As such, the

⁹ See also *Bongiovanni*, 961 F.2d at 1138; *Boutilier*, 387 U.S. at 123; *Leib v. Hillsborough Cnty. Pub. Transp. Comm’n*, 558 F.3d 1301, 1310 (11th Cir. 2009); *Ford Motor Co. v. Tex. Dep’t of Transp.*, 264 F.3d 493, 507 (5th Cir. 2001); *Columbia Nat’l Res., Inc. v. Tatum*, 58 F.3d 1101, 1108 (6th Cir. 1995).

¹⁰ See *Skidmore v. Swift & Co.*, 323 U.S. 134, 140 (1944) (“[The agency interpretation is] not controlling upon the courts by reason of [its] authority [but is a] body of experience and informed judgment to which courts . . . may properly resort for guidance.”); *Christenson v. Harris Cnty.*, 529 U.S. 576, 587 (2000) (“[Agency interpretations are] entitled to respect under [*Skidmore*], but only to the extent that [they] have the power to persuade.” (internal quotation marks omitted)); see also Peter L. Strauss, “*Deference*” is Too Confusing—Let’s Call Them “Chevron Space” and “Skidmore Weight”, 112 Colum. L. Rev. 1143, 1147 (2012) (“*Skidmore* . . . is grounded in a construct of the agency as responsible expert, arguably possessing special knowledge of

standard of notice afforded to litigants about the meaning of the statute is not dissimilar to the standard of notice for civil statutes generally because the court, not the agency, is the ultimate arbiter of the statute's meaning.

The second context is where an agency exercises its authority to fill gaps in a statutory scheme. There the agency is primarily responsible for interpreting the statute because the courts must defer to any reasonable construction it adopts. *See Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837 (1984). Courts appear to apply a more stringent standard of notice to civil regulations than civil statutes: parties are entitled to have “ascertainable certainty” of what conduct is legally required by the regulation. *See Chem. Waste Mgmt., Inc. v. EPA*, 976 F.2d 2, 29 (D.C. Cir. 1992) (*per curiam*) (denying petitioners’ challenge that a recently promulgated EPA regulation fails fair notice principles); *Nat’l Oilseed Processors Ass’n. v. OSHA*, 769 F.3d 1173, 1183–84 (D.C. Cir. 2014) (denying petitioners’ challenge that a recently promulgated OSHA regulation fails fair notice principles).

The third context is where an agency interprets the meaning of its own regulation. Here also courts typically must defer to the agency’s reasonable interpretation.¹¹ We

the statutory meaning a court should consider in *reaching its own judgment*.” (emphasis added)).

¹¹ *See Auer v. Robbins*, 519 U.S. 452, 461 (1997) (“Because the salary-basis test is a creature of the Secretary’s own regulations, his interpretation of it is . . . controlling unless plainly erroneous or inconsistent with the regulation.” (internal quotation marks omitted)); *Decker v. Nw. Env’tl. Def. Ctr.*, 133 S. Ct. 1326, 1337 (2013) (“When an agency

and several of our sister circuits have stated that private parties are entitled to know with “ascertainable certainty” an agency’s interpretation of its regulation. *Sec’y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008); *Dravo Corp. v. Occupational Safety & Health Rev. Comm’n*, 613 F.2d 1227, 1232–33 (3d Cir. 1980).¹² Indeed,

interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation.” (internal quotation marks omitted)); *Martin v. Occupational Safety & Health Rev. Comm’n*, 499 U.S. 144, 150–51 (1991) (“In situations in which the meaning of [regulatory] language is not free from doubt, the reviewing court should give effect to the agency’s interpretation so long as it is reasonable.” (alterations in original, internal quotations omitted)); *Columbia Gas Transp., LLC v. 1.01 Acres, More or Less in Penn Twp.*, 768 F.3d 300, 313 (3d Cir. 2014) (“[A]s an agency interpretation of its own regulation, it is deserving of deference.” (citing *Decker*)).

¹² See also *Wis. Res. Prot. Council v. Flambeau Mining Co.*, 727 F.3d 700, 708 (7th Cir. 2013); *AJP Const., Inc. v. Sec’y of Labor*, 357 F.3d 70, 75–76 (D.C. Cir. 2004) (quoting *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995)); *Tex. Mun. Power Agency v. EPA*, 89 F.3d 858, 872 (D.C. Cir. 1996); *Ga. Pac. Corp. v. Occupational Safety & Health Rev. Comm’n*, 25 F.3d 999, 1005 (11th Cir. 1994); *Diamond Roofing Co. v. Occupational Safety & Health Rev. Comm’n*, 528 F.2d 645, 649 (5th Cir. 1976). In fact, the Supreme Court applied *Skidmore* to an interpretation by an agency of a regulation it adopted instead of deferring to that interpretation because the latter would have “seriously undermine[d] the principle that agencies should provide regulated parties fair

“the due process clause prevents . . . deference from validating the application of a regulation that fails to give fair warning of the conduct it prohibits or requires.” *AJP Const., Inc.*, 357 F.3d at 75 (internal quotation marks omitted).

A higher standard of fair notice applies in the second and third contexts than in the typical civil statutory interpretation case because agencies engage in interpretation differently than courts. See Frank H. Easterbook, *Judicial Discretion in Statutory Interpretation*, 57 Okla. L. Rev. 1, 3 (2004) (“A judge who announces deference is approving a shift in interpretive method, not just a shift in the identity of the decider, as if a suit were being transferred to a court in a different venue.”). In resolving ambiguity in statutes or regulations, courts generally adopt the *best* or *most reasonable* interpretation. But, as the agency is often free to adopt *any reasonable construction*, it may impose higher legal obligations than required by the best interpretation.¹³

warning of the conduct [a regulation] prohibits or requires.” *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 & n.15 (2012) (second alteration in original, internal quotation marks omitted) (citing *Dravo*, 613 F.2d at 1232–33 and the “ascertainable certainty” standard).

¹³ See *Nat’l Cable & Telecomms. Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 980 (2005) (“If a statute is ambiguous, and if the implementing agency’s construction is reasonable, *Chevron* requires a federal court to accept the agency’s construction of the statute, even if the agency’s reading differs from what the court believes is the best statutory interpretation.”); *Decker*, 133 S. Ct. at 1337 (“It is well established that an agency’s interpretation need not be the only possible reading of a regulation—or even the best one—

Furthermore, courts generally resolve statutory ambiguity by applying traditional methods of construction. Private parties can reliably predict the court's interpretation by applying the same methods. In contrast, an agency may also rely on technical expertise and political values.¹⁴ It is harder to predict how an agency will construe a statute or regulation at some unspecified point in the future, particularly when that interpretation will depend on the "political views of

to prevail. When an agency interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation." (internal quotation marks omitted)); *Auer*, 519 U.S. at 462–63 ("[The rule that Fair Labor Standards Act] exemptions are to be narrowly construed against . . . employers . . . is a rule governing judicial interpretation of statutes and regulations, not a limitation on the Secretary's power to resolve ambiguities in his own regulations. A rule requiring the Secretary to construe his own regulations narrowly would make little sense, since he is free to write the regulations as broadly as he wishes, subject only to the limits imposed by the statute." (internal quotation marks omitted)).

¹⁴ See *Garfias-Rodriguez v. Holder*, 702 F.3d 504, 518 (9th Cir. 2012) (rejecting the applicability of the judicial retroactivity test to a new Board of Immigration Appeals' interpretation because the "decision fill[ed] a statutory gap and [was] an exercise [of the agency's] policymaking function"); Easterbrook, *supra* at 3 ("Judges in their own work forswear the methods that agencies employ" to interpret statutes, which include relying on "political pressure, the President's view of happy outcomes, cost-benefit studies . . . and the other tools of policy wonks . . .").

the President in office at [that] time.” Strauss, *supra* at 1147.¹⁵

Wyndham argues it was entitled to “ascertainable certainty” of the FTC’s interpretation of what specific cybersecurity practices are required by § 45(a). Yet it has contended repeatedly—no less than seven separate occasions in *this* case—that there is no FTC rule or adjudication about cybersecurity that merits deference here. The necessary implication, one that Wyndham itself has explicitly drawn on two occasions noted below, is that federal courts are to interpret § 45(a) in the first instance to decide whether Wyndham’s conduct was unfair.

Wyndham’s argument has focused on the FTC’s motion to dismiss order in *LabMD*, an administrative case in which the agency is pursuing an unfairness claim based on allegedly inadequate cybersecurity. *LabMD Order, supra*. Wyndham first argued in the District Court that the *LabMD Order* does not merit *Chevron* deference because “self-serving, litigation-driven decisions . . . are entitled to no deference at all” and because the opinion adopted an impermissible construction of the statute. Wyndham’s

¹⁵ See also *Brand X Internet Servs.*, 545 U.S. at 981 (“[T]he agency . . . must consider varying interpretations and the wisdom of its policy on a continuing basis . . . in response to . . . a change in administrations.” (internal quotation marks omitted, first omission in original)); *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 59 (1983) (Rehnquist, J., dissenting in part) (“A change in administration brought about by the people casting their votes is a perfectly reasonable basis for an executive agency’s reappraisal of the costs and benefits of its . . . regulations.”).

January 29, 2014 Letter at 1–2, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887).

Second, Wyndham switched gears in its opening brief on appeal to us, arguing that *LabMD* does not merit *Chevron* deference because courts owe no deference to an agency’s interpretation of the “boundaries of Congress’ statutory delegation of authority to the agency.” Wyndham Br. at 19–20.

Third, in its reply brief it argued again that *LabMD* does not merit *Chevron* deference because it adopted an impermissible construction of the statute. Wyndham Reply Br. at 14.

Fourth, Wyndham switched gears once more in a Rule 28(j) letter, arguing that *LabMD* does not merit *Chevron* deference because the decision was nonfinal. Wyndham’s February 6, 2015 Letter (citing *LabMD, Inc. v. FTC*, 776 F.3d 1275 (11th Cir. 2015)).

Fifth, at oral argument we asked Wyndham whether the FTC has decided that cybersecurity practices are unfair. Counsel answered: “No. I don’t think consent decrees count, I don’t think the 2007 brochure counts, and I don’t think *Chevron* deference applies. So are . . . they asking this federal court in the first instance . . . [?] I think the answer to that question is yes” Oral Arg. Tr. at 19.

Sixth, due to our continuing confusion about the parties’ positions on a number of issues in the case, we asked for supplemental briefing on certain questions, including whether the FTC had declared that cybersecurity practices can be unfair. In response, Wyndham asserted that “the FTC has not declared unreasonable cybersecurity practices ‘unfair.’” Wyndham’s Supp. Memo. at 3. Wyndham

explained further: “It follows from [our] answer to [that] question that the FTC is asking the federal courts to determine in the first instance that unreasonable cybersecurity practices qualify as ‘unfair’ trade practices under the FTC Act.” *Id.* at 4.

Seventh, and most recently, Wyndham submitted a Rule 28(j) letter arguing that *LabMD* does not merit *Chevron* deference because it decided a question of “deep economic and political significance.” Wyndham’s June 30, 2015 Letter (quoting *King v. Burwell*, 135 S. Ct. 2480 (2015)).

Wyndham’s position is unmistakable: the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret § 45(a) in the first instance to decide whether it prohibits the alleged conduct here. The implication of this position is similarly clear: if the federal courts are to decide whether Wyndham’s conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply. The relevant question is not whether Wyndham had fair notice of the *FTC’s interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires.

Indeed, at oral argument we asked Wyndham whether the cases cited in its brief that apply the “ascertainable certainty” standard—all of which involve a court reviewing an agency adjudication¹⁶ or at least a court being asked to

¹⁶ See *Fox Television Stations, Inc.*, 132 S. Ct. 2307 (vacating an FCC adjudication for lack of fair notice of an agency interpretation); *PMD Produce Brokerage Corp. v. USDA*, 234

defer to an agency interpretation¹⁷—apply where the court is to decide the meaning of the statute in the first instance.¹⁸ Wyndham’s counsel responded, “I think it would, your Honor. I think if you go to *Ford Motor* [*Co. v. FTC*, 673 F.2d 1008 (9th Cir. 1981)], I think that’s what was happening there.” Oral Arg. Tr. at 61. But *Ford Motor* is readily distinguishable. Unlike Wyndham, the petitioners there did not bring a fair notice claim under the Due Process Clause. Instead, they argued that, per *NLRB v. Bell Aerospace Co.*, 416 U.S. 267 (1974), the FTC abused its discretion by proceeding through agency adjudication rather than

F.3d 48 (D.C. Cir. 2000) (vacating the dismissal of an administrative appeal issued by a Judicial Officer in the Department of Agriculture because the agency’s Rules of Practice failed to give fair notice of the deadline for filing an appeal); *Gen. Elec. Co.*, 53 F.3d 1324 (vacating an EPA adjudication for lack of fair notice of the agency’s interpretation of a regulation); *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374 (1965) (reviewing an FTC adjudication that found liability).

¹⁷ See *In re Metro-East Mfg. Co.*, 655 F.2d 805, 810–12 (7th Cir. 1981) (declining to defer to an agency’s interpretation of its own regulation because the defendant could not have known with ascertainable certainty the agency’s interpretation).

¹⁸ We asked, “All of your cases on fair notice pertain to an agency’s *interpretation* of its own regulation or the statute that governs that agency. Does this fair notice doctrine apply where it is a *court* announcing an *interpretation* of a *statute* in the first instance?” Oral Arg. Tr. at 60 (emphases added).

rulemaking.¹⁹ More importantly, the Ninth Circuit was reviewing an agency adjudication; it was not interpreting the meaning of the FTC Act in the first instance.

In addition, our understanding of Wyndham's position is consistent with the District Court's opinion, which concluded that the FTC has stated a claim under § 45(a) based on the Court's interpretation of the statute and without any reference to *LabMD* or any other agency adjudication or

¹⁹ To the extent Wyndham could have raised this argument, we do not read its briefs to do so. Indeed, its opening brief appears to repudiate the theory. Wyndham Br. at 38–39 (“The district court below framed the fair notice issue here as whether ‘the FTC must formally promulgate regulations before bringing its unfairness claim.’ With all respect, that characterization of Wyndham’s position is a straw man. Wyndham has never disputed the general principle that administrative agencies have discretion to regulate through either rulemaking or adjudication. *See, e.g., [Bell Aerospace Co., 416 U.S. at 290–95]*. Rather, Wyndham’s point is only that, however an agency chooses to proceed, it must provide regulated entities with constitutionally requisite fair notice.” (internal citations omitted)). Moreover, the Supreme Court has explained that where “it is doubtful [that] any generalized standard could be framed which would have more than marginal utility[, the agency] has reason to . . . develop[] its standards in a case-by-case manner.” *Bell Aerospace Co.*, 416 U.S. at 294. An agency’s “judgment that adjudication best serves this purpose is entitled to great weight.” *Id.* Wyndham’s opening brief acknowledges that the FTC has given this rationale for proceeding by adjudication, Wyndham Br. at 37–38, but, the company offers no ground to challenge it.

regulation. *See FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 621–26 (D.N.J. 2014).

We thus conclude that Wyndham was not entitled to know with ascertainable certainty the FTC’s interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute. If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham’s liability, we leave to that time a fuller exploration of the level of notice required. For now, however, it is enough to say that we accept Wyndham’s forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency’s interpretation of the statute.

B. Did Wyndham Have Fair Notice of the Meaning of § 45(a)?

Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham’s briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under § 45(a). Wyndham argues instead it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim.

To begin with, Wyndham’s briefing focuses on the FTC’s failure to give notice of its interpretation of the statute and does not meaningfully argue that the statute itself fails fair notice principles. We think it imprudent to hold a 100-

year-old statute unconstitutional as applied to the facts of this case when we have not expressly been asked to do so.

Moreover, Wyndham is entitled to a relatively low level of statutory notice for several reasons. Subsection 45(a) does not implicate any constitutional rights here. *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982). It is a civil rather than criminal statute.²⁰ *Id.* at 498–99. And statutes regulating economic activity receive a “less strict” test because their “subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action.” *Id.* at 498.

In this context, the relevant legal rule is not “so vague as to be ‘no rule or standard at all.’” *CMR D.N. Corp.*, 703 F.3d at 632 (quoting *Boutilier*, 387 U.S. at 123). Subsection 45(n) asks whether “the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis, *Pa. Funeral Dirs. Ass’n v. FTC*, 41 F.3d 81, 89–92 (3d Cir. 1992); *Am. Fin. Servs. Ass’n*, 767 F.2d at 975, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that

²⁰ While civil statutes containing “quasi-criminal penalties may be subject to the more stringent review afforded criminal statutes,” *Ford Motor Co.*, 264 F.3d at 508, we do not know what remedy, if any, the District Court will impose. And Wyndham’s briefing does not indicate what kinds of remedies it is exposed to in this proceeding.

would arise from investment in stronger cybersecurity. We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. *Cf. Nash v. United States*, 229 U.S. 373, 377 (1913) (“[T]he law is full of instances where a man’s fate depends on his estimating rightly, that is, as the jury subsequently estimates it, some matter of degree.”). Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.

What appears to us is that Wyndham’s fair notice claim must be reviewed as an as-applied challenge. *See United States v. Mazurie*, 419 U.S. 544, 550 (1975); *San Filippo*, 961 F.2d at 1136. Yet Wyndham does not argue that its cybersecurity practices survive a reasonable interpretation of the cost-benefit analysis required by § 45(n). One sentence in Wyndham’s reply brief says that its “view of what data-security practices are unreasonable . . . is not necessarily the same as the FTC’s.” Wyndham Reply Br. at 23. Too little and too late.

Wyndham’s as-applied challenge falls well short given the allegations in the FTC’s complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, Compl. at ¶ 24(a), did not restrict specific IP addresses *at all*, *id.* at ¶ 24(j), did not use *any* encryption for certain customer files, *id.* at ¶ 24(b), and did not require some users to change their default or factory-setting passwords *at all*, *id.* at ¶ 24(f). Wyndham did not respond to this argument in its reply brief.

Wyndham's as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis. That said, we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis.

Several other considerations reinforce our conclusion that Wyndham's fair notice challenge fails. In 2007 the FTC issued a guidebook, *Protecting Personal Information: A Guide for Business*, FTC Response Br. Attachment 1 [hereinafter *FTC Guidebook*], which describes a "checklist[]" of practices that form a "sound data security plan." *Id.* at 3. The guidebook does not state that any particular practice is required by § 45(a),²¹ but it does counsel against many of the specific practices alleged here. For instance, it recommends that companies "consider encrypting sensitive information that is stored on [a] computer network . . . [, c]heck . . . software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches." *Id.* at 10. It recommends using "a firewall to protect [a] computer from hacker attacks while it is connected to the Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through

²¹ For this reason, we agree with Wyndham that the guidebook could not, on its own, provide "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices fail § 45(n). But as we have already explained, this is not the relevant question.

the firewall and what they will be allowed to see . . . to allow only trusted employees with a legitimate business need to access the network.” *Id.* at 14. It recommends “requiring that employees use ‘strong’ passwords” and cautions that “[h]ackers will first try words like . . . the software’s default password[] and other easy-to-guess choices.” *Id.* at 12. And it recommends implementing a “breach response plan,” *id.* at 16, which includes “[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information,” *id.* at 23.

As the agency responsible for administering the statute, the FTC’s expert views about the characteristics of a “sound data security plan” could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis.

Before the attacks, the FTC also filed complaints and entered into consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. FTC Br. at 47 n.16. The agency published these materials on its website and provided notice of proposed consent orders in the Federal Register. Wyndham responds that the complaints cannot satisfy fair notice principles because they are not “adjudications on the merits.”²² Wyndham Br. at 41. But even where the “ascertainable certainty” standard applies to fair notice claims, courts regularly consider materials that are neither regulations nor “adjudications on the merits.” *See, e.g., United States v.*

²² We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).

Lachman, 387 F.3d 42, 57 (1st Cir. 2004) (noting that fair notice principles can be satisfied even where a regulation is vague if the agency “provide[d] a sufficient, publicly accessible statement” of the agency’s interpretation of the regulation); *Beverly Healthcare-Hillview*, 541 F.3d at 202 (citing *Lachman* and treating an OSHA opinion letter as a “sufficient, publicly accessible statement”); *Gen. Elec. Co.*, 53 F.3d at 1329. That the FTC commissioners—who must vote on whether to issue a complaint, 16 C.F.R. § 3.11(a); ABA Section of Antitrust Law, *FTC Practice and Procedure Manual* 160–61 (2007)—believe that alleged cybersecurity practices fail the cost-benefit analysis of § 45(n) certainly helps companies with similar practices apprehend the possibility that their cybersecurity could fail as well.²³

²³ We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC’s only answer was that “if you’re a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things.” Oral Arg. Tr. at 51. We also asked whether the FTC has “informed the public that it needs to look at complaints and consent decrees for guidance,” and the Commission could offer no examples. *Id.* at 52. But Wyndham does not appear to argue it was unaware of the consent decrees and complaints; it claims only that they did not give notice of what the law requires. Wyndham Reply Br. at 25 (“The fact that the FTC publishes these materials on its website and provides notice in the Federal Register, moreover, is immaterial—the problem is not that Wyndham lacked notice *of the consent decrees* [which

Wyndham next contends that the individual allegations in the complaints are too vague to be relevant to the fair notice analysis. Wyndham Br. at 41–42. It does not, however, identify any specific examples. And as the Table below reveals, the individual allegations were specific and similar to those here in at least one of the four or five²⁴ cybersecurity-related unfair-practice complaints that issued prior to the first attack.

Wyndham also argues that, even if the individual allegations are not vague, the complaints “fail to spell out what specific cybersecurity practices . . . actually triggered the alleged violation, . . . provid[ing] only a . . . description of certain alleged problems that, ‘*taken together*,’” fail the cost-benefit analysis. Wyndham Br. at 42 (emphasis in original). We part with it on two fronts. First, even if the complaints do not specify which allegations, in the Commission’s view, form the necessary and sufficient conditions of the alleged violation, they can still help companies apprehend the possibility of liability under the statute. Second, as the Table below shows, Wyndham cannot argue that the complaints fail to give notice of the necessary and sufficient conditions of an

reference the complaints] but that consent decrees [and presumably complaints] by their nature do not give notice *of what Section 5 requires*.” (emphases in original, citations and internal quotations omitted)).

²⁴ The FTC asserts that five such complaints issued prior to the first attack in April 2008. See FTC Br. at 47–48 n.16. There is some ambiguity, however, about whether one of them issued several months later. See Complaint, *TJX Co.*, No. C-4227 (FTC 2008) (stating that the complaint was issued on July 29, 2008). We note that this complaint also shares significant parallels with the allegations here.

alleged § 45(a) violation when all of the allegations in at least one of the relevant four or five complaints have close corollaries here. *See* Complaint, *CardSystems Solutions, Inc.*, No. C-4168 (FTC 2006) [hereinafter CCS].

Table: Comparing CSS and Wyndham Complaints

	CSS	Wyndham
1	Created unnecessary risks to personal information by storing it in a vulnerable format for up to 30 days, CSS at ¶ 6(1).	Allowed software at hotels to store payment card information in clear readable text, Compl. at ¶ 24(b).
2	Did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks; did not implement simple, low-cost and readily available defenses to such attacks, CSS at ¶ 6(2)–(3).	Failed to monitor network for the malware used in a previous intrusion, Compl. at ¶ 24(i), which was then reused by hackers later to access the system again, <i>id.</i> at ¶ 34.
3	Failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network, CSS at ¶ 6(4).	Did not employ common methods to require user IDs and passwords that are difficult for hackers to guess. <i>E.g.</i> , allowed remote access to a hotel’s property management system that used default/factory setting passwords, Compl. at ¶ 24(f).

4	Did not use readily available security measures to limit access between computers on its network and between those computers and the Internet, CSS at ¶ 6(5).	Did not use readily available security measures, such as firewalls, to limit access between and among hotels' property management systems, the Wyndham network, and the Internet, Compl. at ¶ 24(a).
5	Failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations, CSS at ¶ 6(6).	Failed to employ reasonable measures to detect and prevent unauthorized access to computer network or to conduct security investigations, Compl. at ¶ 24(h).

In sum, we have little trouble rejecting Wyndham's fair notice claim.

V. Conclusion

The three requirements in § 45(n) may be necessary rather than sufficient conditions of an unfair practice, but we are not persuaded that any other requirements proposed by Wyndham pose a serious challenge to the FTC's claim here. Furthermore, Wyndham repeatedly argued there is no FTC interpretation of § 45(a) or (n) to which the federal courts must defer in this case, and, as a result, the courts must interpret the meaning of the statute as it applies to Wyndham's conduct in the first instance. Thus, Wyndham cannot argue it was entitled to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform. Instead, the company can only claim that it lacked fair notice of the meaning of the statute itself—a

theory it did not meaningfully raise and that we strongly suspect would be unpersuasive under the facts of this case.

We thus affirm the District Court's decision.

In the
United States Court of Appeals
For the Seventh Circuit

No. 14-3122

HILARY REMIJAS, on behalf of herself and all others similarly
situated, *et al.*,

Plaintiffs-Appellants,

v.

NEIMAN MARCUS GROUP, LLC,

Defendant-Appellee.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 14 C 1735 — **James B. Zagel**, *Judge*.

ARGUED JANUARY 23, 2015 — DECIDED JULY 20, 2015

Before WOOD, *Chief Judge*, and KANNE and TINDER, *Circuit Judges*.

WOOD, *Chief Judge*. Sometime in 2013, hackers attacked Neiman Marcus, a luxury department store, and stole the credit card numbers of its customers. In December 2013, the company learned that some of its customers had found fraudulent charges on their cards. On January 10, 2014, it announced to the public that the cyberattack had occurred

and that between July 16, 2013, and October 30, 2013, approximately 350,000 cards had been exposed to the hackers' malware. In the wake of those disclosures, several customers brought this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), seeking various forms of relief. The district court stopped the suit in its tracks, however, ruling that both the individual plaintiffs and the class lacked standing under Article III of the Constitution. This resulted in a dismissal of the complaint without prejudice. See *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 102 (1998) (standing to sue is a threshold jurisdictional question); *Hernandez v. Conriv Realty Assocs.*, 182 F.3d 121, 122 (2d Cir. 1999) ("[W]here federal subject matter jurisdiction does not exist, federal courts do not have the power to dismiss with prejudice"). We conclude that the district court erred. The plaintiffs satisfy Article III's requirements based on at least some of the injuries they have identified. We thus reverse and remand for further proceedings.

I

In mid-December 2013, Neiman Marcus learned that fraudulent charges had shown up on the credit cards of some of its customers. Keeping this information confidential at first (according to plaintiffs, so that the breach would not disrupt the lucrative holiday shopping season), it promptly investigated the reports. It discovered potential malware in its computer systems on January 1, 2014. Nine days later, it publicly disclosed the data breach and sent individual notifications to the customers who had incurred fraudulent charges. The company also posted updates on its website. Those messages confirmed several aspects of the attack: some card numbers had been exposed to the malware, but

other sensitive information such as social security numbers and birth dates had not been compromised; the malware attempted to collect card data between July 16, 2013, and October 30, 2013; 350,000 cards were potentially exposed; and 9,200 of those 350,000 cards were known to have been used fraudulently. Notably, other companies had also suffered cyberattacks during that holiday season.

At that point, Neiman Marcus notified all customers who had shopped at its stores between January 2013 and January 2014 and for whom the company had physical or email addresses, offering them one year of free credit monitoring and identity-theft protection. On February 4, 2014, Michael Kingston, the Senior Vice President and Chief Information Officer for the Neiman Marcus Group, testified before the United States Senate Judiciary Committee. He represented that “the customer information that was potentially exposed to the malware was payment card account information” and that “there is no indication that social security numbers or other personal information were exposed in any way.”

These disclosures prompted the filing of a number of class-action complaints. They were consolidated in a First Amended Complaint filed on June 2, 2014, by Hilary Remijas, Melissa Frank, Debbie Farnoush, and Joanne Kao. They sought to represent themselves and the approximately 350,000 other customers whose data may have been hacked. The complaint relies on a number of theories for relief: negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws. It raises claims that exceed \$5,000,000, and minimal diversity of citizenship exists, because Remijas is a citizen of Illinois, Frank is a citi-

zen of New York, and Farnoush and Kao are citizens of California, while the Neiman Marcus Group LLC, once ownership is traced through several intermediary LLCs, is owned by NM Mariposa Intermediate Holdings Inc., a Delaware corporation with its principal place of business in Texas. The district court's jurisdiction (apart from the Article III issue to which we will turn) was therefore proper under 28 U.S.C. § 1332(d)(2).

Remijas alleged that she made purchases using a Neiman Marcus credit card at the department store in Oak Brook, Illinois, in August and December 2013. Frank alleged that she and her husband used a joint debit card account to make purchases at a Neiman Marcus store on Long Island, New York, in December 2013; that on January 9, 2014, fraudulent charges appeared on her debit card account; that, several weeks later, she was the target of a scam through her cell phone; and that her husband received a notice letter from Neiman Marcus about the breach. Farnoush alleged that she also incurred fraudulent charges on her credit card after she used it at Neiman Marcus in 2013. Finally, Kao made purchases on ten separate occasions at a Neiman Marcus store in San Francisco in 2013 and received notifications in January 2014 from her bank as well as Neiman Marcus that her debit card had been compromised.

Citing Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), Neiman Marcus moved to dismiss the complaint for lack of standing and for failure to state a claim. On September 16, 2014, the district judge granted the motion exclusively on standing grounds, and the plaintiffs filed their notice of appeal nine days later. This created a slight problem with appellate jurisdiction, because the district judge never set

out his judgment in a separate document as required by Rule 58(a). Nonetheless, we have confirmed that there is a final judgment for purposes of 28 U.S.C. § 1291 and our jurisdiction is secure. (This step would not be necessary if the district court had taken the simple additional step described in Rule 58(a); we once again urge the district courts to do so, for the sake of both the parties and the appellate court.) Here, the district court clearly evidenced its intent in its opinion that this was the final decision in the case, and the clerk recorded the dismissal in the docket. *Bankers Trust Co. v. Mallis*, 435 U.S. 381, 387–88 (1978); see also *Kaplan v. Shure Bros.*, 153 F.3d 413, 417 (7th Cir. 1998). As neither party has called to our attention anything that would defeat finality nor do we see anything, we are free to proceed.

II

We review a district court’s dismissal for lack of Article III standing *de novo*. *Reid L. v. Ill. State Bd. of Educ.*, 358 F.3d 511, 515 (7th Cir. 2004). Under Rule 12(b)(1), “the district court must accept as true all material allegations of the complaint, drawing all reasonable inferences therefrom in the plaintiff’s favor, unless standing is challenged as a factual matter.” *Id.* “The plaintiffs, as the parties invoking federal jurisdiction, bear the burden of establishing the required elements of standing.” *Id.* (citation omitted); see *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). In order to have standing, a litigant must “prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision.” *Hollingsworth v. Perry*, 133 S. Ct. 2652, 2661 (2013) (citing *Lujan*, 504 U.S. at 560–61).

These plaintiffs must allege that the data breach inflicted concrete, particularized injury on them; that Neiman Marcus caused that injury; and that a judicial decision can provide redress for them. We first address these requirements of Article III standing, and then briefly comment on Neiman Marcus's argument that, alternatively, the complaint should be dismissed for failure to state a claim.

A

The plaintiffs point to several kinds of injury they have suffered: 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information. (We note that these allegations go far beyond the complaint about a website's publication of inaccurate information, in violation of the Fair Credit Reporting Act, that is before the Supreme Court in *Spokeo, Inc. v. Robins*, No. 13-1339, *cert. granted* 135 S. Ct. 1892 (2015).) The plaintiffs also allege that they have standing based on two imminent injuries: an increased risk of future fraudulent charges and greater susceptibility to identity theft. We address the two alleged imminent injuries first and then the four asserted actual injuries.

Allegations of future harm can establish Article III standing if that harm is "certainly impending," but "allegations of possible future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (citation omitted). Here, the complaint alleges that everyone's personal data has already been stolen; it alleges that the 9,200 who already

have incurred fraudulent charges have experienced harm. Those victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges. The complaint also alleges a concrete risk of harm for the rest. The question is whether these allegations satisfy *Clapper's* requirement that injury either already have occurred or be "certainly impending."

As for the 9,200 (including Frank and Farnoush), the plaintiffs concede that they were later reimbursed and that the evidence does not yet indicate that their identities (as opposed to the data) have been stolen. But as we already have noted, there are identifiable costs associated with the process of sorting things out. Neiman Marcus challenges the standing of these class members, but we see no merit in that point. What about the class members who contend that unreimbursed fraudulent charges and identity theft may happen in the future, and that these injuries are likely enough that immediate preventive measures are necessary? Neiman Marcus contends that this is too speculative to serve as injury-in-fact. It argues that all of the plaintiffs would be reimbursed for fraudulent charges because (it asserts) that is the common practice of major credit card companies. The plaintiffs disagree with the latter proposition; they contend that they, like all consumers subject to fraudulent charges, must spend time and money replacing cards and monitoring their credit score, and that full reimbursement is not guaranteed. (It would not be enough to review one's credit card statements carefully every month, because the thieves might—and often do—acquire new credit cards unbeknownst to the victim.) This reveals a material factual dispute on such mat-

ters as the class members' experiences and both the content of, and the universality of, bank reimbursement policies.

Clapper does not, as the district court thought, foreclose any use whatsoever of future injuries to support Article III standing. In *Clapper*, the Supreme Court decided that human rights organizations did not have standing to challenge the Foreign Intelligence Surveillance Act (FISA) because they could not show that their communications with suspected terrorists *were* intercepted by the government. The plaintiffs only suspected that such interceptions might have occurred. This, the Court held, was too speculative to support standing. In so ruling, however, it did not jettison the "substantial risk" standard. To the contrary, it stated that "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." 133 S. Ct. at 1150 n.5 (2013) (citation omitted).

In a data breach case similar to ours, a district court persuasively applied these principles, including *Clapper's* recognition that a substantial risk will sometimes suffice to support Article III standing. "Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both 'highly attenuated' and 'highly speculative,' the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real." *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, at *8 (N.D. Cal. Sept. 4, 2014) (citing *Clapper*, 133 S. Ct. at 1148). Our case is much the same. The plaintiffs allege that the

hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information. Whereas in *Clapper*, “there was no evidence that any of respondents’ communications either had been or would be monitored,” in our case there is “no need to speculate as to whether [the Neiman Marcus customers’] information has been stolen and what information was taken.” *Id.* (citing *Clapper*, 133 S. Ct. at 1148). Like the *Adobe* plaintiffs, the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an “objectively reasonable likelihood” that such an injury will occur. *Clapper*, 133 S. Ct. at 1147.

Requiring the plaintiffs “to wait for the threatened harm to materialize in order to sue” would create a different problem: “the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not ‘fairly traceable’ to the defendant’s data breach.” *In re Adobe Sys.*, 2014 WL 4379916, at *8 n.5. Neiman Marcus has made just that argument here. The point is best understood as a challenge to the causation requirement of standing, to which we turn shortly.

At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store’s database and steal consumers’ private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities. The plaintiffs are also careful to say that only 9,200 cards have experienced fraudulent charges *so far*; the complaint asserts that fraudulent charges and identity theft can occur long after a data breach. It cites a Government Ac-

countability Office Report that finds that “stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.” U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007). (This suggests that on remand the district court may wish to look into length of time that a victim is truly at risk; the GAO suggests at least one year, but more data may shed light on this question.) We recognize that the plaintiffs may eventually not be able to provide an adequate factual basis for the inference, but they had no such burden at the pleading stage. Their allegations of future injury are sufficient to survive a 12(b)(1) motion.

In addition to the alleged future injuries, the plaintiffs assert that they have already lost time and money protecting themselves against future identity theft and fraudulent charges. Mitigation expenses do not qualify as actual injuries where the harm is not imminent. *Clapper*, 133 S. Ct. at 1152 (concluding that “costs that they have incurred to avoid [injury]” are insufficient to confer standing). Plaintiffs “cannot manufacture standing by incurring costs in anticipation of non-imminent harm.” *Id.* at 1155. “If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.” *Id.* at 1151.

Once again, however, it is important not to overread *Clapper*. *Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place. An affected

customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring. It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than *de minimis*. For instance, Experian offers credit monitoring for \$4.95 a month for the first month, and then \$19.95 per month thereafter. See <http://www.experian.com/consumer-products/credit-monitoring.html>. That easily qualifies as a concrete injury. It is also worth noting that our analysis is consistent with that in *Anderson v. Hannaford Bros. Co.*, where the First Circuit held before *Clapper* that the plaintiffs sufficiently alleged mitigation expenses—namely, the fees for replacement cards and monitoring expenses—because under Maine law, a plaintiff may “recover for costs and harms incurred during a reasonable effort to mitigate, regardless of whether the harm is non-physical.” 659 F.3d 151, 162 (1st Cir. 2011).

For the sake of completeness, we comment briefly on the other asserted injuries. They are more problematic. We need not decide whether they would have sufficed for standing on their own, but we are dubious. The plaintiffs argue, for example, that they overpaid for the products at Neiman Marcus because the store failed to invest in an adequate security system. In some situations, we have held that financial injury in the form of an overcharge can support Article III standing. See *In re Aqua Dots Products Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011) (“The plaintiffs’ loss is financial: they

paid more for the toys than they would have, had they known of the risks the beads posed to children. A financial injury creates standing.”) (citations omitted). District courts have applied this approach to comparable situations. See, e.g., *Chicago Faucet Shoppe, Inc. v. Nestle Waters N. Am. Inc.*, No. 12 C 08119, 2014 WL 541644, at *3 (N.D. Ill. Feb. 11, 2014) (citing *Aqua Dots*); *Muir v. Playtex Products, LLC*, 983 F. Supp. 2d 980, 986 (N.D. Ill. 2013) (holding that a claim that consumer would not have purchased product or not have paid a premium price for the product is sufficient injury to establish standing).

Importantly, many of those cases involve products liability claims against defective or dangerous products. See, e.g., *Lipton v. Chattem, Inc.* No. 11 C 2952, 2012 WL 1192083, at *3–4 (N.D. Ill. Apr. 10, 2012). Our case would extend that idea from a particular product to the operation of the entire store: plaintiffs allege that they would have shunned Neiman Marcus had they known that it did not take the necessary precautions to secure their personal and financial data. They appear to be alleging some form of unjust enrichment as well: Neiman Marcus sold its products at premium prices, but instead of taking a portion of the proceeds and devoting it to cybersecurity, the company pocketed too much. This is a step that we need not, and do not, take in this case. Plaintiffs do not allege any defect in any product they purchased; they assert instead that patronizing Neiman Marcus inflicted injury on them. Compare *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012) (reasoning that the plaintiff had financial injury from paying higher premiums in light of defendant’s failure to implement security policies). That allegation takes nothing away from plaintiffs’ more concrete alle-

gations of injury, but it is not necessary to support their standing.

The plaintiffs also allege that they have a concrete injury in the loss of their private information, which they characterize as an intangible commodity. Under this theory, persons who had unauthorized credit charges would have standing even if they were automatically reimbursed, their identities were not stolen, and they could not show that there was a substantial risk of lack of reimbursement or further use of their information. This assumes that federal law recognizes such a property right. Plaintiffs refer us to no authority that would support such a finding. We thus refrain from supporting standing on such an abstract injury, particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value.

The plaintiffs counter that recently-enacted state statutes make this right to personal information concrete enough for standing. They are correct to the extent they suggest that “the actual or threatened injury required under Article III can be satisfied solely by virtue of an invasion of a recognized state-law right.” *Scanlan v. Eisenberg*, 669 F.3d 838, 845 (7th Cir. 2012) (citation omitted). The plaintiffs argue that Neiman Marcus violated California and Illinois’s Data Breach Acts by impermissibly delaying the notifications of the data breach. That may be (we express no opinion on the point), but even if it is, the violation does not help the plaintiffs. Neither of those statutes provides the basis for finding an injury for Article III standing. As for California law, a delay in notification is not a cognizable injury, *Price v. Starbucks Corp.*, 192 Cal. App. 4th 1136, 1143 (Cal. Ct. App. 2011), and the Illinois Consumer Fraud Act requires “actual damages.”

People ex rel. Madigan v. United Constr. of Am., Inc., 981 N.E.2d 404, 411 (Ill. App. Ct. 2012). None of the other state-law claims has been discussed by the parties, and so we too do not address them.

To sum up, we refrain from deciding whether the overpayment for Neiman Marcus products and the right to one's personal information might suffice as injuries under Article III. The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft do. These injuries are sufficient to satisfy the first requirement of Article III standing.

B

Injury-in-fact is only one of the three requirements for Article III standing. Plaintiffs must also allege enough in their complaint to support the other two prerequisites: causation and redressability. As the Supreme Court put it in *Clapper*, plaintiffs must "show[] that the defendant's actual action has caused the substantial risk of harm." 133 S. Ct. at 1150, n.5. Neiman Marcus argues that these plaintiffs cannot show that their injuries are traceable to the data incursion at the company rather than to one of several other large-scale breaches that took place around the same time. This argument is reminiscent of *Summers v. Tice*, 199 P.2d 1, 5 (Cal. 1948), in which joint liability was properly pleaded when, during a quail hunt on the open range, the plaintiff was shot, but he did not know which defendant had shot him. Under those circumstances, the Supreme Court of California held, the burden shifted to the defendants to show who was responsible. Neiman Marcus apparently rejects such a rule, but we think that this debate has no bearing on standing to sue;

at most, it is a legal theory that Neiman Marcus might later raise as a defense.

The fact that Target or some other store *might* have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are "fairly traceable" to the data breach at Neiman Marcus. See *In re Target Corp. Data Sec. Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2014 WL 7192478, at *2 (D. Minn. Dec. 18, 2014) ("Plaintiffs' allegations plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct. This is sufficient at this stage to plead standing. Should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue."). If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then "the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J. concurring) (citing *Summers*, 199 P.2d at 3-4). It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk. Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level. See *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

With respect to standing, Neiman Marcus finally argues that the plaintiffs' injuries cannot be redressed by a judicial decision because they already have been reimbursed for the fraudulent charges. That may be true for the fraudulent

charges (the plaintiffs do not allege that any of those charges went unreimbursed), but it is not true for the mitigation expenses or the future injuries. Although some credit card companies offer some customers “zero liability” policies, under which the customer is not held responsible for any fraudulent charges, that practice defeats neither injury-in-fact nor redressability. The “zero liability” feature is a business practice, not a federal requirement. Under 15 U.S.C. § 1643, a consumer’s liability for the unauthorized use of her credit card may not exceed \$50 if she does not report the loss before the credit card is used. If she notifies the card issuer before any use, she is not responsible for any charges she did not authorize. Debit cards (used by several of the named plaintiffs) receive less protection than credit cards; the former are covered under the Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq.*, and the latter under the Truth in Lending Act as amended by the Fair Credit Billing Act, 15 U.S.C. § 1601 *et seq.* If a person fails to report to her bank that money has been taken from her debit card account more than 60 days after she receives the statement, there is no limit to her liability and she could lose all the money in her account. In any event, as we have noted, reimbursement policies vary. For the plaintiffs, a favorable judicial decision could redress any injuries caused by less than full reimbursement of unauthorized charges.

C

Neiman Marcus attempts to argue in the alternative that the plaintiffs failed to state a claim upon which relief can be granted. FED. R. CIV. P. 12(b)(6). Their problem is that the district court did not reach this ground, and that the ground on which it resolved the case (Article III standing) necessarily

resulted in a dismissal without prejudice. A dismissal under Rule 12(b)(6), in contrast, is a dismissal with prejudice. If Neiman Marcus had wanted this additional relief, it needed to file a cross-appeal. See *Jennings v. Stephens*, 135 S. Ct. 793, 798 (2015) (“[A]n appellee who does not cross-appeal may not attack the decree with a view either to enlarging his own rights thereunder or of lessening the rights of his adversary.”) (citation and quotation marks omitted). Since it did not, the question whether this complaint states a claim on which relief can be granted is not properly before us.

We therefore conclude that the plaintiffs have adequately alleged standing under Article III. The district court’s judgment is REVERSED and the case is REMANDED for further proceedings consistent with this opinion.



New York Field Office

[Home](#) • [New York](#) • [Press Releases](#) • 2015 • [Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme](#)

Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme

More Than 150,000 Press Releases Stolen from Three Major Newswire Companies, Used to Generate Approximately \$30 Million in Illegal Trading Profits

U.S. Attorney's Office

August 11, 2015

Eastern District of New York

(718) 254-7000

NEWARK, NJ—Nine people were charged in two indictments unsealed today in Brooklyn, New York, and Newark federal court with an international scheme to hack into three business newswires and steal yet-to-be published press releases containing non-public financial information that was then used to make trades that allegedly generated approximately \$30 million in illegal profits.

U.S. Attorney Paul J. Fishman, District of New Jersey, and Acting U.S. Attorney Kelly T. Currie, Eastern District of New York, announced the indictments today, along with U.S. Secretary of Homeland Security Jeh Johnson; U.S. Secret Service Director Joseph P. Clancy; FBI Assistant Director-in-Charge Diego Rodriguez, New York Field Office; and U.S. Securities Exchange Commission (SEC) Chair Mary Jo White. The SEC also unsealed a civil complaint today charging the nine indicted defendants and several other individuals and entities.

The indictments unsealed today charge the defendants with hacking into the newswires and stealing confidential information about companies traded on the NASDAQ and NYSE in what is the largest scheme of its kind ever prosecuted. The defendants allegedly stole approximately 150,000 confidential press releases from the servers of the newswire companies. They then traded ahead of more than 800 stolen press releases before their public release, generating millions of dollars in illegal profits.

"The defendants were a well-organized group that allegedly robbed the newswire companies and their clients and cheated the securities markets and the investing public by engaging in an unprecedented hacking and trading scheme," U.S. Attorney Fishman said. "The defendants launched a series of sophisticated and relentless cyber attacks against three major newswire companies, stole highly confidential information and used to enrich themselves at the expense of public companies and their shareholders."

"As alleged, the defendants and their co-conspirators formed an alliance of hackers and securities industry professionals to systematically steal valuable inside information and profit by trading ahead of authorized disclosures to the investing public," stated Acting United States Attorney Currie.

"Today's sweeping indictments are the result of a cutting edge investigation by law enforcement to combat twenty-first century criminal schemes."

"Today's announcement is a testament to the countless hours of hard work and dedication by law enforcement and other personnel across government, including the Secret Service investigative team. In today's day and age, criminals are using computers instead of guns to steal money and threaten the safety and security of our cyber networks," Secretary Johnson said. "In matters of cybersecurity, the Department of Homeland Security has a major law enforcement role, and our work to counter cyber threats is a critical priority for the Secret Service because of the substantial threat it poses to this nation's financial infrastructure."

The 23-count District of New Jersey indictment charges five defendants—Ivan Turchynov, 27; Oleksandr Ieremenko, 24; and Pavel Dubovoy, 32; all of Ukraine, and Arkadiy Dubovoy, 51, and Igor Dubovoy, 28, of Alpharetta, Georgia—with wire fraud conspiracy, securities fraud conspiracy, wire fraud, securities fraud, and money laundering conspiracy. Turchynov and Ieremenko are additionally charged with computer fraud conspiracy, computer fraud, and aggravated identity theft.

The Eastern District of New York indictment charges four defendants: Vitaly Korchevsky, 50, of Glen Mills, Pennsylvania; Vladislav Khalupsky, 45, of Brooklyn, New York; and Odessa, Ukraine; Leonid Momotok, 47, of Suwanee, Georgia; and Alexander Garkusha, 47, of Cummings and Alpharetta, Georgia, with wire fraud conspiracy, securities fraud conspiracy, securities fraud, and money laundering conspiracy.

Earlier today, the government seized 17 bank and brokerage accounts containing more than \$6.5 million of alleged criminal proceeds. The government also took steps to restrain 12 properties, a shopping center located in Pennsylvania, an apartment building located in Georgia, and a houseboat, all worth more than \$5.5 million.

Five of the nine defendants named above were arrested this morning: Arkadiy Dubovoy, Igor

New York Field Office Links

New York Home

Contact Us

- Overview
- Territory/Jurisdiction

News and Outreach

- Press Room | Stories
- In Your Community

About Us

- Our People & Capabilities
- What We Investigate
- Our Partnerships
- New York History

Wanted by the FBI - New York

FBI Jobs

Five of the nine defendants named above were arrested this morning. Arkadiy Dubovoy, Igor Dubovoy, Momotok, and Garkusha were all arrested at their homes in Georgia, and are scheduled to appear this afternoon before U.S. Magistrate Judge Alan J. Berman in federal court in Atlanta, Georgia. Korchevsky was arrested at his home in Glenn Mills, Pennsylvania, and is scheduled to appear this afternoon before U.S. Magistrate Judge Linda K. Caracappa in federal court in Philadelphia, Pennsylvania. Turchynov, Ieremenko, Pavel Dubovoy, and Khalupsky remain in Ukraine, and international arrest warrants were issued today for their arrests.

According to the indictments:

Between February 2010 and August 2015, Turchynov and Ieremenko, computer hackers based in Ukraine, gained unauthorized access into the computer networks of Marketwired L.P., PR Newswire Association LLC (PRN), and Business Wire. They used a series of sophisticated cyber attacks to gain access to the computer networks. The hackers moved through the computer networks and stole press releases about upcoming announcements by public companies concerning earnings, gross margins, revenues, and other confidential and material financial information.

At one point, one of the hackers sent an online chat message in Russian to another individual stating, "I'm hacking prnewswire.com." In another online chat, Ieremenko told Turchynov that he had compromised the log-in credentials of 15 Business Wire employees.

The hackers shared the stolen press releases with traders Arkadiy Dubovoy, Korchevsky, Momotok, Igor Dubovoy, Pavel Dubovoy, Khalupsky, Garkusha, and others, using overseas computer servers that they controlled. In a series of e-mails, the hackers even shared "instructions" on how to access and use an overseas server where they shared the stolen releases with the traders, and the access credentials and instructions were distributed amongst the traders. In an e-mail sent by one of the traders, the instructions for accessing the overseas server suggested that users conceal their Internet Protocol address when accessing the server as a precaution to avoid detection. The traders created "shopping lists" or "wish lists" for the hackers listing desired upcoming press releases from Marketwired and PRN for publicly traded companies. Trading data obtained over the course of the investigation showed that, after one of the shopping lists or wish lists was sent, the traders and others traded ahead of several of the press releases listed on it.

The traders generally traded ahead of the public distribution of the stolen releases, and their activities shadowed the hackers' capabilities to exfiltrate stolen press releases. In order to execute their trades before the releases were made public, the traders sometimes had to execute trades in extremely short windows of time between when the hackers illegally accessed and shared information and when the press releases were disseminated to the public by the newswires, usually shortly after the close of the markets. Frequently, all of this activity occurred on the same day. Thus, the trading data often showed a flurry of trading activity around a stolen press release just prior to its public release. The defendants' illegal trading resulted in gains of more than \$30 million, of which Korchevsky accounted for more than \$17 million and Arkadiy Dubovoy accounted for more than \$11 million.

The traders traded on stolen press releases containing material nonpublic information about publicly traded companies that included, among hundreds of others: Align Technology Inc.; Caterpillar Inc.; Hewlett Packard; Home Depot; Panera Bread Co.; and Verisign Inc.

The traders paid the hackers for access to the overseas servers based, in part, on a percentage of the money the traders made from their illegal trading activities. The hackers and traders used foreign shell companies to share in the illegal trading profits.

"This is the story of a traditional securities fraud scheme with a twist—one that employed a contemporary approach to a conventional crime. In this case the defendants allegedly traded on nonpublic information, ultimately benefitting from more than \$30 million in illegal profits over the course of three years," Assistant Director-in-Charge Rodriguez said. "But just as criminals continue to develop relationships with one another in order to advance their objectives, the law enforcement community has developed a collaborative approach to fighting these types of crimes."

"Cyber cases such as this are a vital part of the Secret Service's integrated mission," Joseph P. Clancy, Director of the U.S. Secret Service, said. "This is yet another example of the successful investigative work being done in coordination with our partners in the global law enforcement community."

The wire fraud conspiracy and substantive wire fraud counts with which all defendants are charged carry a maximum potential penalty of 20 years in prison and a \$250,000 fine, or twice the gain or loss from the offense. The securities fraud conspiracy count with which all defendants are charged carries a maximum potential penalty of five years in prison and a \$250,000 fine, or twice the gain or loss from the offense. The substantive securities fraud counts with which all defendants are charged carry a maximum potential penalty of 20 years in prison and a \$5 million fine, or twice the gain or loss from the offense. The money laundering conspiracy count with which all defendants are charged carries a maximum potential penalty of 20 years in prison and a \$500,000 fine, or twice the value of the funds involved in the illegal transfers. The computer fraud counts with which the alleged hackers are charged carry a maximum potential penalty of five years' imprisonment and a \$250,000 fine, or twice the gain or loss from the offense. The aggravated identity theft counts with which the hackers are charged carry a mandatory consecutive term of imprisonment of 24 months.

U.S. Attorney Fishman and Acting U.S. Attorney Currie credited special agents of the U.S. States Secret Service, Criminal Investigations, under the direction of Director Clancy, and the Newark Field Office under the direction of Special Agent in Charge Carl Agnelli; and special agents of the FBI, New York Field Office, under the direction of Assistant Director Diego Rodriguez, for the investigation leading to today's arrests and indictments. They thanked the U.S. Securities and Exchange Commission, for its significant cooperation and assistance in the investigation and the newswires, which cooperated with law enforcement over the course of the investigation.

In the District of New Jersey, the government is represented by Assistant U.S. Attorneys Andrew S.

In the District of New York, the government is represented by Assistant U.S. Attorneys Jonathan S. Pak, Daniel V. Shapiro, and David M. Eskew of the Economic Crimes Unit, Computer Hacking & Intellectual Property Section, Assistant U.S. Attorney Svetlana M. Eisenberg of the Office's Civil Division, and Special Assistant U.S. Attorney Sarah Devlin of the Asset Forfeiture and Money Laundering Unit.

In the Eastern District of New York, the government's case is being prosecuted by the Business and Securities Fraud Section and the National Security and Cybercrime Section. Assistant U.S. Attorneys Christopher A. Ott, Christopher L. Nasson, and Richard M. Tucker are in charge of the prosecution. Assistant U.S. Attorneys Brian D. Morris and Tanisha Payne of the Office's Civil Division are responsible for the forfeiture of assets.

The charges and allegations contained in the indictments are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

The charges were brought in connection with the President's Financial Fraud Enforcement Task Force. The task force was established to wage an aggressive, coordinated, and proactive effort to investigate and prosecute financial crimes. With more than 20 federal agencies, 94 U.S. Attorneys' Offices, and state and local partners, it is the broadest coalition of law enforcement, investigatory, and regulatory agencies ever assembled to combat fraud. Since its formation, the task force has made great strides in facilitating increased investigation and prosecution of financial crimes; enhancing coordination and cooperation among federal, state, and local authorities; addressing discrimination in the lending and financial markets; and conducting outreach to the public, victims, financial institutions, and other organizations. Since fiscal year 2009, the Justice Department has filed over 18,000 financial fraud cases against more than 25,000 defendants. For more information on the task force, please visit www.StopFraud.gov.

- Remarks Prepared for ADIC Diego Rodriguez Concerning International Hacking Ring, Insider Trading Scheme

Follow the FBI's New York Office on Twitter. Sign up for our e-mail alerts to receive the latest information from the FBI's New York Office on breaking news, arrests, and fugitives.

This content has been reproduced from its original source.

Close