# Fighting Account Takeover (ATO) Attacks
# through Big Data Analytics and Commercial Vendors

**By: Erin Tsai**

**MSBA 307**

## Table of Contents

## Table of Figures

## I. Executive Summary

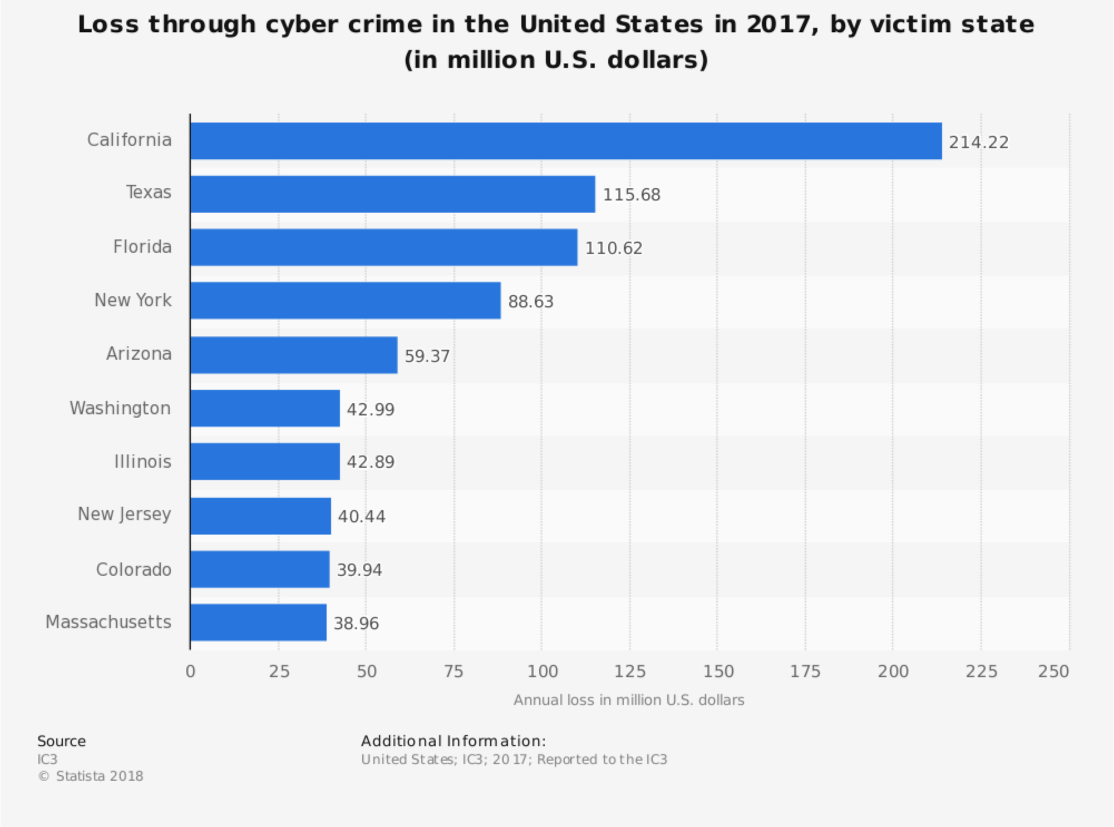
Our bank has experienced a significant increase in the number of new accounts enrolled. As a small local bank, we have to take into consideration security measures that we may not have considered in full before. Because of this, the risk for Account Takeover (ATO) attacks is extremely high. These types of attacks are particularly lucrative for cybercriminals.

Our current company has limited abilities with detecting large scale ATOs either at the point of unsuccessful login attempts or after the account has been compromised, stopping ATOs before any damage is done. Our websites are not yet set up to detect ATOs, and that needs to change in order to protect our clients, especially given the wave of new clients that have recently enrolled. Any ATO attack undetected can potentially cause a huge amount of negative media for our company and cause huge loss with respect to number of customers, retention of customers, and our brand.

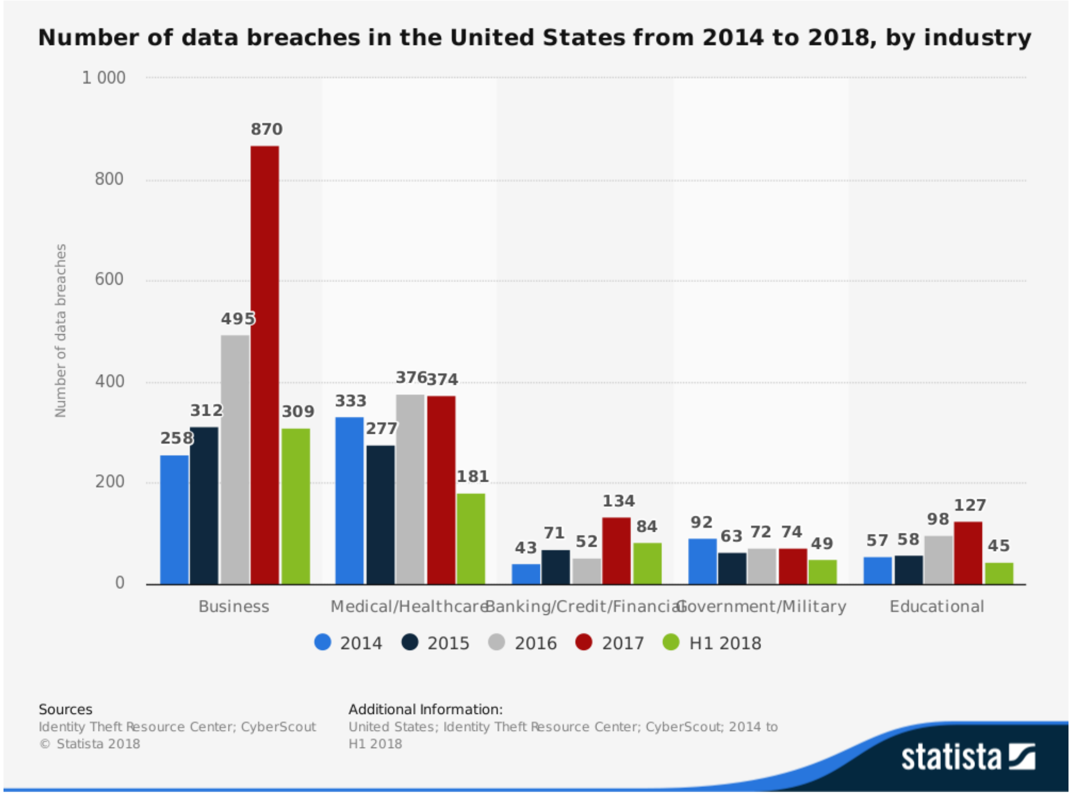
After thorough research regarding the vendors that provide for ATO protection, I have come up with the following proposition. We go through our log files frequently, to find ATO attacks through use of queries to identify when coding has been modified, or if there are IP addresses with many failed login attempts. Additionally, we must have a plan for when we do identify ATO attacks. But furthermore, to increase security, we should also combine that with use of a commercial vendor, which I have suggested Netacea is the commercial vendor we go with. Netacea integrates directly into our website, and offers advanced behavioral machine learning so that it can predict when the login attempts are fraudulent. This will be extremely beneficial in protecting our client's information and money, and protecting our brand.

## II. Problem Statement

Cybercrime continues to be an increasing problem throughout the United States. The loss in California through cybercrime is the highest in California as compared to the other states. It is almost twice as much as the next highest state in Texas. This is alarming, especially considering the high risk our bank faces with respect to cyber crimes.



Thankfully, as compared to other businesses, banks have a much lower number of data breaches. However, it is still alarming because the number of breaches occurring every year increases. The data below only shows the first half of 2018. Therefore, as we look at banking/credit/financial industry numbers for the first half of 2018, which is currently at 84, if that only covers half the year, presuming an equal number for the remainder of the year, we would be looking at a total of 168 for the year of 2018, which is still an increase from 2017.



Number of data breaches in the United States from 2014 to 2018, by industry

Sources
Identity Theft Resource Center; CyberScout
© Statista 2018

Additional Information:
United States; Identity Theft Resource Center; CyberScout; 2014 to H1 2018

The Federal Financial Institutions Examination Council (FFIEC) have identified resources to assist in enhancing cybersecurity and protecting client information. (FFIEC, 2018). Banks such as ours have to meet the set of standards set forth by the FFIEC. We can utilize the resources available on the FFIEC website to identify gaps and ensure compliance with the guidelines.

Additionally, because there is cause of concern with respect to ATOs given the increased prevalence of cybercrime, which includes ATO attacks, due to the increased in number of new accounts enrolled, we are seeking a good solution to not only detect ATO attacks, but also prevent them before they occur.

## III. <u>Key requirements to address the problem</u>

Our key requirements to address the problem is to ensure that the cost needed to utilize these vendors and to place heightened security measures will be worth the gain. Another key requirement we need to consider is the time it will take to implement the programs and to ensure proper function, and minimal error.

With all programs and software, there will be some error. There will always be false positives that occur. Our goal is to minimize the number of false positives, creating unnecessary alarm to customers. At the same time, we want to be able to provide the security that our clients deserve when they bank with us.

## IV. Key research findings

### *a. Current Trends in ATO Fraud*

As of 2017, the number of account takeover fraud has increased significantly, approximately 45% from 2016. (Andreea, 2018.) The loss that online retailers suffered reached 3.3 billion dollars. Several methods are utilized to obtain banking credentials, such as fake websites that mimic the actual bank websites, malware and viruses to compromise a system, or using social engineering to find security credentials or other user data. *Id.* Data breaches have been a huge problem in 2017, and these data breaches lead to more ATO attacks. *Id.* "Advanced security features, such as biometric authentication devices, are being built directly into smartphones that consumers use every day, giving companies new tools in the fight against fraudsters." *Id.*

Because of the increased numbers of account takeover fraud, we must be vigilant in fighting these issues and determining when there is unauthorized access in our clients' bank accounts. We can use information such as behavior patterns to fight ATO fraud. For instance, we can review login attempts from different devices, switching operating systems, changing passwords, multiple failed login attempts, strange device configurations like using VPNs. *Id.*

### *b. Big Data Analytics*

First and foremost, we should consider what we can do in-house, specifically, to address the issues of ATOs. We have data from logins from our clients. We can review the log files to help us in obtaining insight on how attacks are happening. How can we utilize that data to detect ATOs and prevent ATOs in the future?

I would propose that our Cyber Security Department review log files and identify possible attacks that have already occurred. We will contact clients if it seems that their account has been compromised. Is it an issue with respect to how easy their password is? Should we be changing our requirements for passwords to make it more difficult to hack? We would have to check for things like SQL Injection attacks, Directory Traversal, and to mark Hosts with multiple failed attempts. (*See* Talabis, Mcpherson, et al. 2015). We can also use haversine distances to identify potential unauthorized users. For instance, if we note that there are IP addresses with multiple failed attempts or IP addresses with extremely high haversine distances, we can find out if it is because of a hacker, or if it is because our client is having issues remembering their user credentials. We should have a plan on how to deal with the issues, while also being able to filter the results so that we are not overwhelmed with calling every single person for every single hit. Sometimes, there will be false positives when we review the log files, and we must be careful not to cause too many problems for our clients. If we do identify that the IP address is indeed someone attempting to hack into the account, we can put them on a blacklist to prevent them from further access. Having a black list of IP addresses we believe are high risk and have been attempting to gain data from our bank is useful, but it is only a reactive method, which is noted on Netacea's page. (Netacea, 2018c.) We should also do more to focus on the preventative side.

### *c. Commercial Vendors*

Different vendors have different approaches to the problem. With a two-factor authentication or a multifactor authentication method, the chances of an ATO will be lower. However, with too many multi-factor authentication, email link confirmation, SMS codes, Captchas, or other forms of additional layers of security, the experience becomes increasingly frustrating for the client.

Sift Science suggests that with each user, there can be a risk score, and if the score is low, then there would be less Captchas or codes required, but if the score is high, then it may require multiple authentication attempts. (Sift Science, 2018.) As such, they calculate scores based on user browsing patterns, network and IP data, location history, and device information. *Id.* Their end goal is to ensure a balance between increasing security for the clients, but at the same time, minimizing user frustration.

Iovation, a TransUnion company, utilizes technology to match the identity of the user with a matching device fingerprints. (Iovation, 2018.) Clients can indicate which devices they want to associate with their accounts. Because it uses the matching device's fingerprints, it has one more step then just purely a username or password. Moreover, fingerprints biologically unique, making it much harder for a cybercriminal to obtain access. Utilizing biometric data seems to be an up and coming trend with respect to cyber security. “Biometric authentication uses the unique physical characteristics of a person to confirm that they are who they say they are, and is being increasingly used to confirm online purchases, payments, and bank transactions.” (Kennedy, 2018.) I believe this would only be minimally effective.

After some research, I believe some of our best options would be with Netacea and Shape Security.

Netacea has a product called bot management. It can identify approved visitors, and if they are not previously approved, then there are more security measures taken against the attempts. (Netacea, 2018b.) Netacea detects and prevents ATOs by “identifying credential stuffing, account hijacking, password cracking, and brute force attacks.” (Netacea, 2018a.) It uses advanced behavioral machine learning to identify and prevent account takeovers by modeling account behavior to detect anomalies and to gain insight into new attack vectors. *Id.* Netacea also utilizes Captcha that does not require JavaScript, there are no complex or repetitive navigation links, so that the flow is easy for the clients, and it is easily integrated into the website. (Netacea, 2018c.) Additionally, it has a quick attack detection and response ability. This is a step up from Iovation as it uses behavioral machine learning in addition to adding a second level of protection in login attempts.

One of the major benefits of Netacea is that they have a free trial, which would be extremely beneficial for our company. Since we are still a relatively small bank, having a free trial before we launch into a full length contract would be extremely beneficial for us. Additionally, their ability to integrate directly to our website easily is very helpful in our transition.

ShapeSecurity is one of the most well-known companies that offer ATO protection. Many of the top banks in the United States use Shape Security. (Shape Security, 2018). It prides itself on “eliminating bots, fraudulent activity, and unwanted automation for over 20 of the consumer brands in the Fortune 500.” (Anderson, 2018.) It uses a huge amount of data and its artificial intelligence platform to detect and shut down automated attacks in real-time. *Id.*

However, with Shape Security, there would be a high cost involved. There is a licensing cost, of which I would suggest the perpetual license so that we can pay one upfront fee as opposed to a subscription. (ItQlick, 2018.) Naturally, a subscription would likely cost less initially since we would be paying on a monthly basis. However, because this is better viewed as a long term plan, it will end up being cheaper if we pay for a perpetual license. If cost is a huge problem, we could always go with the commercial open source, so that the software is free of cost and there is no upfront license fee. However, then all ongoing maintenance, upgrading, customization must be done in house. *Id.* This is something we can consider, as long our Cyber Security Department can handle it. There are various fees with respect to cost of customization, data migration, and cost of training. However, this may be something we must bear as an initial cost regardless of what vendor we choose.

## V. Conclusion

Based on my research of the various vendors, I recommend that we utilize a combination of being more proactive with the data we already have, and using the data to detect ATO attacks that have already occurred, in combination with a commercial vendor such as Netacea. Our data analytics of the log files from our current clients' login attempts will give us insight as to how cybercriminals have been able to compromise our security measures initially, so that we can place additional safety measures to prevent further issues.

As a preventative measure, we can also utilize a vendor to complement our in-house team. Although ShapeSecurity is one of the most popular companies amongst top banks, my primary concern with going with ShapeSecurity is cost. I would suggest Netacea over Shape Security because Netacea also has the behavioral machine learning aspect that I believe we could really use in our company, but they offer a free trial so we can first determine if the benefits justify the cost.

Based on the above analysis, I am requesting an approval for the plan to proceed with implementing timed review of log files through use of Big Data Analytics, along with implementation of the ATO fraud prevention through Netacea, initially through the free trial.

## VI. References

Anderson, Dan. (2018, Nov. 5). *Shape Security Raises $26 Million to Prevent Attacks From Committing Online Fraud.* https://pulse2.com/shape-security-26-million/

Andreea, Nita. (2017, Dec. 19). *Web Fraud Prevention and Online Authentication Market Guide 2017/2018.* https://www.thepaypers.com/reports/web-fraud-prevention-and-online-authentication-market-guide-2017-2018/r770429

Federal Financial Institutions Examination Council. (Nov. 5, 2018) *Cybersecurity Awareness.* https://www.ffiec.gov/cybersecurity.htm

Iovation. (2018). Account Takeover Fraud (ATO) Detection & Prevention – Stop Account Takeover with iovation. https://www.iovation.com/fraud-detection-prevention/account-takeover-fraud

ITQlick. (2018, Apr. 25). *2018 Shape Security Pricing Guide.* https://www.itqlick.com/shape-security/pricing

Kennedy, Mark. (2018, June 29). *Banking on the future with biometric innovation.* https://www.thepaypers.com/expert-opinion/banking-on-the-future-with-biometric-innovation/773774

Netacea. (2018a). *Account Takeover Detection & Prevention.* https://www.netacea.com/account-takeover-fraud?gclid=CjwKCAiAlb_fBRBHEiwAzMeEdt9Q7PE_YELS19GW6zk1w21zyuhartQdJgM_wEuodgh6OWlOJnXPCBoCCT0QAvD_BwE

Netacea. (2018b). *Bot Management.* https://www.netacea.com/bot-management

Netacea. (2018c). *FAQ.* https://www.netacea.com/faq

Shape Security. (2018). *Shape Protects the Finance Industry from Bot Attacks.* https://www.shapesecurity.com/customers/finance/

Sift Science. (2018). *Complete Guide to Preventing Account Takeover*. http://pages.siftscience.com/rs/526-PCC-974/images/eBook-Complete-Guide-to-Preventing-Account-Takeover.pdf?mkt_tok=eyJpIjoiWkRJd01URTFObVl4WkRJMSIsInQiOiJtNW5DWGhMSFhHczhTVHpETGxNOG1EVXhsMjhhRVFLRDZvWmplRms4ZExwMWRZd1MydWRQR0lWeFNiYjh1Y0lrQU41R1JmNU9pY0R2bnU1ZksyTWh5SGVYc3A3U2RXUG9RcEZUNldaV1I5Tjh6aUlWUzlDYUoyM1JCaElQXC9QSzcifQ%3D%3D

Statista. (2018a). *Loss through cyber crime in the United States in 2017, by state.* https://www.statista.com/statistics/234993/us-states-with-the-largest-losses-through-cybercrime/

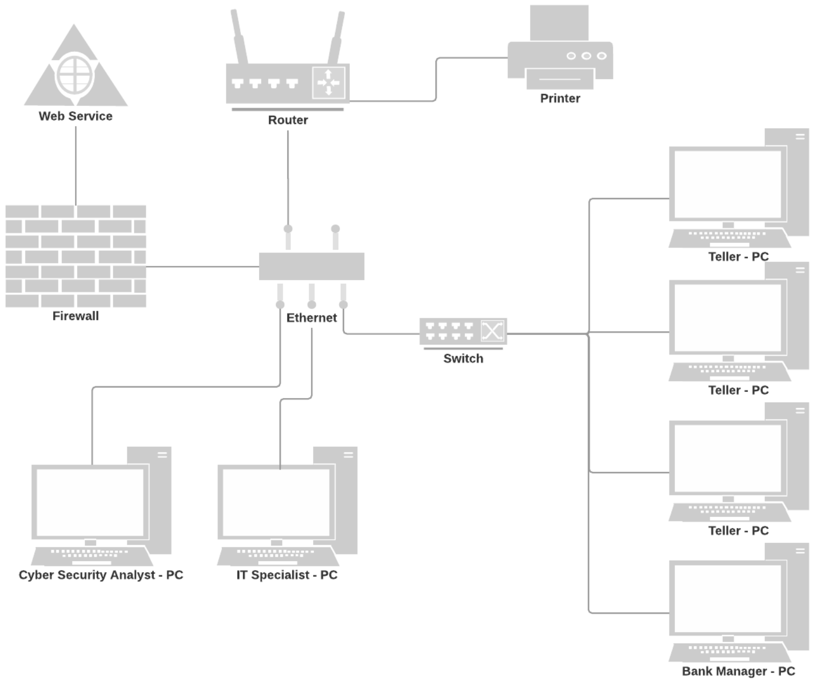
Statista. (2018b). *Number of data breaches in the United States from 2014-2018, by industry*. https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/

# VII. Appendix

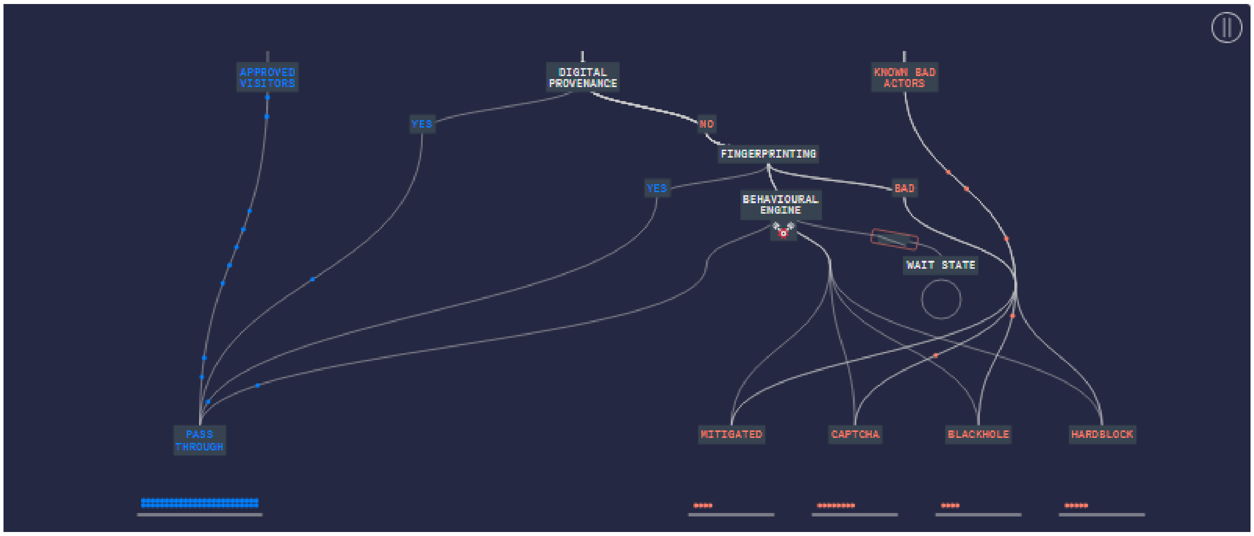
## A. Network Diagram

NETWORK DIAGRAM

Erin Tsai | November 18, 2018



## B. Netacea Bot Management – (Netacea, 2018b.)



APPROVED VISITORS
DIGITAL PROVENANCE
KNOWN BAD ACTORS
YES
NO
FINGERPRINTING
YES
BEHAVIOURAL ENGINE
BAD
WAIT STATE
PASS THROUGH
MITIGATED
CAPTCHA
BLACKHOLE
HARDBLOCK