AUGUST 2017
UPDATED DECEMBER 2017

Your Power, Our People, the Worlds Defense

In More Ways Than One

PREPARED FOR:
FACEBOOK, INC

PROJECT COMPLETED BY:

KATHLEEN K. WATERS, MS PSYCHOLOGY

COLONEL BRYAN DENNY (RET), MA STRATEGIC STUDIES, AND MA MILITARY ART AND SCIENCE

ABSTRACT

This study aimed to show the inconsistency in Facebook's recognition of fraudulent accounts and the need for changes. According to the website, FBI.gov "In 2016, almost 15,000 complaints categorized as romance scams or confidence fraud were reported to IC3 (nearly 2,500 more than the previous year), and the losses associated with those complaints exceeded $230 million." Research was conducted on multiple fraudulent military accounts, the findings show what was expected to be true. Research shows better technology and more education are critical to the safety of not only social media uses, but the military who's identities are being used for profit. Social media is a power, and with power comes abundant accountability.

UPDATE: December, 2017: Please see the latest data under Account Research Findings
UPDATE: December, 2017: Please see additional Account Names Found and Duplications.

INTRODUCTION

We live in the age of social media. Professional connections, friendships, family, and even true love can speak to the value of social media. Unfortunately, social media can also be used as a breeding ground for scammers. Cunning criminals prey on innocent victims enticing them to send gifts, money and goods. It is understood that this responsibility is a two way street. The victims should know better than to send items to strangers, but by stealing the identities of military men, these criminals take advantage of the generosity and pride of American women. Many victims on social media sites such as Facebook are unaware of the astronomical number of scammers present, what to look for in bogus accounts, and how to properly report or respond when approached by a scammer.

There are many kinds of scams in this technology age, however this proposal is based solely on military romance scammers, and how social media can do a better job recognizing and removing the fraudulent accounts, along with providing education to protect potential victims.

BACK STORY

I only used social media as a friend and family connection; until my mother's friend (who would like to remain anonymous), was deceived by a scammer. Our friend was conned out of $15,000 in four months by a man who presented himself as an "active duty" U.S. military soldier stationed in Syria. When I heard her story, and the un-established account provided by this "soldier," I immediately became suspicious investigated the situation. I found the soldiers last name on the military uniform picture, and found him after completing a Google search. After contacting the real Bryan Denny, I learned that not only was he a retired Army Colonel, but his pictures had been used to lure victims on social media sites for approximately seven months prior to my contact with him.

Not fully understanding the scamming process, Col. Denny and I teamed up to investigate this scam of identity theft and coercion. After further investigation, and over a thousand accounts reported to Facebook as fraudulent with Col. Denny's photographs and personal information, we came to realize this was the work of professionals.

We chose to set up our own fake account and see exactly how their scheme worked. We created an account with details that seem to attract the scammers: a 57 year old, Caucasian, retired, widow named "Nancy Waden". We learned three things: scammers had poor use of the English language, they were not willing to communicate through phone or Facetime, and had a lack of military knowledge.

During our 8 months of research, and submitting false accounts when time permitted, Col. Denny received numerous messages from victims that were scammed by someone using his pictures, on various social media sites. These victims gave money, gifts, and even left their marriages of many years to have a life with the man in the photos. Col. Denny and I realized Facebook technology could not, with accuracy, recognize fraudulent accounts, or determine when a duplicated picture came up during the building of a new account. Because the vast majority of these scammers portraying themselves as United States military men actually reside in places such as Ghana and Nigeria, Africa, the ability for the United States to take action is questionable. We realized something significant needed to be done, and it would need to be done by those who have the power to make changes.

TRIGGERED CONCERNS

What was recognized during the research process.

We have two areas of concern that intertwine. 1. Fraudulent, duplicated accounts and photos, and 2. Facebook's Community Standard's are easily violated.

Scammers create accounts at an alarming rate. They have the time and desire to replicate accounts Facebook software previously deemed violated the "Community Standard." Their sole job is to steal military identities, get women to believe their sob story, and con them out of money. This is an attack against our military, and our friends, that must be fought against.

TRIGGERED CONCERNS

ACCOUNT DUPLICATIONS

Fraudulent, duplicated accounts and photos are widely seen through out Facebook. Facebook has a system in place to report fake accounts. Unfortunately, the facial algorithm program is not powerful enough. As you can see in the graph below labeled EXHIBITS A-C, many profiles were reported as duplicate or fake, but the software did not “agree”, thus allowing scammers to have multiple accounts; often using the same military profile, the same residence, occupation and schooling.

TRIGGERED CONCERNS

"COMMUNITY STANDARDS"

Facebook's Community Standards are easily violated. Facebook wants its users to feel safe. The site states: "By joining Facebook you agree to use your authentic name and identity. You may not publish the personal information of others without their consent." (Facebook.com) The problem, however, is that the software has not kept up with the times. Facebook users are not safe. Fortunately, there is better software available such as "eVestigator Cyber risk Prediction Suite".

One example of how Facebook's "Community Standard" has been shattered is Col. Denny's account. We reported multiple unauthentic accounts that used his face, name, and information to Facebook, yet Facebook replied that they were within their "Community Standards". Not only did the software not pick up on these duplications immediately, but when reported as a fake account, it was still determined authentic (see EXHIBIT D-E). However, when Col. Denny reported accounts under the subheading: "They are pretending to be me or someone else I know," he got relatively successful, results with a few accounts remaining (see EXHIBIT F-G).

The concern is that the person whose identity has been stolen for profit does not usually know about the fraud accounts. It is evident that the current software and manpower are not adequate in policing Facebook's "Community Standards" effectively.

Col. Denny and I contacted more than 1,580 victims found on more than 1,000 fake accounts with his stolen identity. Their responses were surprise, coupled with gratefulness or sometimes anger and denial. We need your help to fight this war!

Account Research

Research: Background

BACKGROUND: From October 2016 to July 2017, we have located and reported over 1,500 fraudulent accounts containing Col. Denny's information and pictures (some including pictures of his spouse and minor son). We took 617 of the fraudulent accounts and noted that 235 had his picture with different names, and 382 had his picture and name. When these fraudulent accounts were reported, the outcomes were inconsistent causing a need for further research into this matter.

Research: Four case studies overview

We reviewed 256 military profiles that contained more than one account, but had the same person in the profile pictures. (We found these accounts by typing in a last name that was mentioned on a previously reported account, and added either Syria, or Kabul - both countries are used with fraud accounts in regard to military scams.)

The first study is titled Porter. Porter is the last name of the actual man in the picture. This example will show you how many accounts were reported to Facebook as fraudulent, the number of times we reported the accounts, and Facebook's response.

The second study is titled Anderson. Anderson is the name of the man in the picture. Anderson's graph will also show you how many accounts were reported as fraudulent, the number of times they were reported, Facebook's response, and how many victims currently remain on the open accounts. (Please see EXHIBIT H below.)

The third study is titled Maupin. We only studied these accounts for the accuracy of fake account recognition and nothing else.

The fourth and final study consisted of seven different military men with multiple accounts. This graph shows the number of successfully deleted accounts, the percentage Facebook accurately recognized the fraudulent accounts, how many of the remaining "open" accounts showed a friends/victims list, and the total number of victims still being conned. (Please see graph in Exhibit I")

PORTER STUDY

In four (4) minutes we reported 11 fraudulent accounts containing Mr. Porters pictures and information. (July 8, 2017 between the times of 1:40pm and 1:44pm) On July 10, and again on July 11, 2017, a total of 4 more fake accounts were reported to Facebook, for a total of 15. The account names were: (1) Frank Porter Williams, (2) Porter Speedy, (3) Jamie Porter, (4) Porter Bradley, (5) Porter James, (6) James Porter, (7) Porter Buton Hans, (8) Chole Porter, (9) Ryan Porter, (10) Steve Thomas Porter, (11) Ronald Porter, (12) Samuel Porter, (13) James Porter (different account same person in picture), (14) Eric Porter, and (15) Raymond Porter. None were removed as Facebook deemed them "within Community Standards," resulting in a terrifying 0% accuracy in identifying fraudulent accounts. By July 17, 2017, four were re-reviewed, and according to Facebook they were found to be in violation of the Community Standards, changing the final accuracy rate to 36%.

ANDERSON STUDY

On June 6, 2017, seven fraudulent accounts with Mr. Andersons face -and some with his minor children's faces - were reported in the matter of 50 seconds (it's really easy to do!). We noticed in this study that not all seven accounts showed a "friends" (victim) list. However, five (5) of the seven (7) accounts listed a total of 1, 012 friends/victims, a majority being female. The account names were: (1) Anderson Wilson, (2) Mark Anderson, (3) Anderson Smart, (4) Steve Anderson, (5) Anderson John, (6) Jackson Anderson, and (7) Michael Anderson (please refer to the following pictures). One hour later, Facebook deemed them all as genuine, making Facebook's accuracy rate of recognizing fake accounts 0%.

MAUPIN STUDY

The name Maupin, a military veteran, was also found in an antiscam group site. We took the name and added Syria as well as Kabul, for example we searched “Maupin Syria” and “Maupin Kabul”. Our findings were astounding. In 90 minutes, we reported 59 fraudulent accounts that contained a picture of the same man, with a variation of names that went with Maupin, similar to the previous studies. Two days later, all accounts had been determined, by Facebook, as such: 15 accounts were recognized as fake, and 44 were found within “Community Standards”. Making Facebook’s accuracy rate of recognized fake accounts for Maupin at 25.4%.

MULTIPLE ACCOUNTS STUDY

The final study included seven (7) different military men with more than 1 active account on Facebook. Our search was for "Syria Army" and "Kabul Army." Out of seven subjects, 179 accounts were found. All 179 accounts were reported to Facebook as fraudulent. Of the 179 accounts, only 37 were considered in violation of Community Standards and deleted, 142 accounts remained open (See graph below). Of the 142 accounts that remained, 52 of the accounts had a friend/victims list totaling 3,792 people, the other 90 accounts had hidden their victims/friends list (the scammers are getting smarter!). Making Facebook's accuracy rate of recognizing fake accounts for Multiple Accounts 20.6

ACCOUNT RESEARCH FINDINGS

The final summary of the research shows that Facebook's recognition software and account detection is averaging a mere 20.5% accuracy rate based on an average of the studies conducted in for this report. This number shows that unfortunately, Facebooks technology has not kept up with the cyber times. Numbers were not found for Facebooks successfully deleted accounts opposed to the fake they considered within "Community Standards."

Update: December 15, 2017: Since the Facebook Meeting on October 18, 2017 there have been 79 fraudulent accounts found on Facebook with Col Denny's photos. Of the 79 accounts, Kathy was able to have 17.7% of those removed. Col. Denny reported the remaining 65 accounts and was able to get another 57% removed. A significantly low percentage considering the "real" Col. Bryan Denny (Ret.) was turning in accounts with his own pictures. Over a third (at 35.44%) of the 79 fraudulent accounts were considered within their "Community Standards" i.e. authentic accounts. Clearly showing Facebook is in need of a better safety/security program for their customers; with hopes these numbers will assist in this process.

PROPOSAL

Helping your company and "faces"

Ideas for Better Success Rates

As noted in our studies, current Facebook technology has a low rate of success in recognizing authentic vs. fraudulent accounts. When we step back and think about the data, and the scammer mindset, we know technology is not the only answer. It is, however, the most powerful one, outside of manpower and education.

PROPOSAL

Ideas for better success rate

Technology

The first option to consider would be advancing cyber security technology. There are several companies and programs that could enhance Facebook's "safe" internet community. Staying one step in front of the scammers will be challenging, but technology that focuses on face identification and IP address would significantly benefit the safety of your users. A low, or no cost, option would be to have all new accounts set up with the most restrictive settings from the start, so users must learn how to unsecure portions of what they would like to expose or share with the social media community.

Manpower

Employees that can focus on fraudulent accounts, and or suspicious activity, are key to safety, and Facebook's "Community Standard". Technology, obviously, cannot do it alone. Additional manpower trained in identifying and deleting fraudulent, duplicated, accounts is necessary.

Education

We believe in personal responsibility. However, criminals deceive many good intentioned people who choose Facebook as their connection to the world. A free, or low cost, idea for a safer community would be continuous PSA posts, and or advertisements, that warn users of fraudulent accounts, how to spot them, how to report them, and how to block the scammer. The most important piece of education would be "never send money or gifts to someone you have not met in person."

CONCLUDING REMARKS

Last year $230, 000,000.00 was reportedly sent to scammers (FBI data), imagine how our markets would thrive if that money stayed in our community. Imagine how much bandwidth could be saved without all the scamming sites! Professional scammers need to be challenged by professional security. If the two of us, in our spare time, could find multiple fake accounts, imagine what better technology and skilled manpower can do! With great power comes responsibility...Imagine giving he people the power to build a community and bring the world closer together - safely!

ON A MORE PERSONAL NOTE

Victim Bryan Denny is a retired Colonel for the Untied States Army and holds two Masters Degrees in Strategic Studies, and Military Art and Science, whereas Kathy Waters is a full time employee for Kaiser Permanente and also holds a Masters Degree in Psychology and BS in Human Services. After writing to over 1,580 victims found on the fake accounts containing Colonel Denny's pictures, and reporting over 1,000 fake accounts, something greater and more profound had to be done. These numbers are based on the pictures of one person and one person alone. Please take the recommended changes and improvements into consideration for the health of your company, the respect of your military and the justice of your customers.

References

Colvin, Geoff. “Why You Should Care That Facebook’s Getting Really Good at Facial Recognition.” Time Inc. 6 February, 2017

Facebook, "Community Standards", 18 July, 2017. Retrieved from Facebook.com

FBI.gov, "Romance Scams, Online Imposters Break Hears and Bank Accounts." 13, February, 2017

EXHIBIT A of A-C

ACCOUNT NAMES FOUND & DUPLICATIONS

Tracking Start Date:	October 26, 2016-July 11, 2017
ACCOUNT NAMES	TIMES USED
Wilson Moore	
Thomas Denny	10
David Bryan Denny	
Kelvin Denny	7
Scott Denny	4
Denny Scott	
Philip Smith Denny	
Philip Fred Denny	
Philip Taylor Denny	
Philip Denny	
Denny Bradley	1
Foy Denny	1
Ray Denny	3
Dickson Denny	
Jefferey Denny	3
Billy Denny	87
Andrew Denny	1
Bryan Denny	49
Larry Arnold Denny	
David Denny Bryan	2
Aiden Denny	
Denny Anthony	
Benjamin Denny	
Clark Denny Alexander	2
Denny Townsend J Cooper	1
Denny Anderson	
Denny Wallace	
Roland Denny	2
Paul Denny	11
Robert Denny	5
Clement Denny	
Denny Johnson	3
Adams Denny Shipley	
Denzel Fortner (Denny)	
Ronald Denny	3
Melissa Denny Holmes	
Ronald M. Denny	
Wilson Denny	9
Prince Denny	
Steve Denny	
Brown Denny	2
Denny Brown	
Jack Denny	
Jack Denny Alphonso	
Chris Denny	4
Ryan Denny	
Greg Reynold (Denny)	
Denny Walter	
Gary Denny	
Charles Denny	
Dennis Alvin Jorgensen	
Denny Kelvin	1
Wayne Denny	
David Denny	2
Avin Denny	
Denny James	
Denny Richard	2
Kelvin Denny Smith	
Jeffery Johnson	
Jack P. Denny	
Denny White Johnson	
Eric Denny	
Denny Bruce	
Ben Denny Shipley	
Denny Brown	
Denny Pete	
Larry Barons Denny	
Denny Reilly	3
Denny Francisco Dollin	
Bill Matt	
Sanders James	
Mike Sanders	
Sanders Rogers	
Sanders Cox	
Sanders Brown	
Sanders Jackson	
Sanders Holloway	
Rodney Sanders	
Sanders James	
Sanders Vaughn	
Paton Sanders	
Harris Denny	
Alex Denny	1
Johnson Denny	1
Greg Howes	3
Kelvin Robert Denny	
Denny Kelly Robert	
Denny Scott Michael	
Walter Denny	2
Donald Denny	
Alberto Denny	1
Luke Denny	
Noah Denny	4
Jackson B. Denny	
Denny Anthony Bryan	
Earl Denny	
Dwayne Johnson	
Dick Denny	
Kennedy C. Denny	
Hillwood Denny	
Scott Mike Denny	5
Kelvin Anthony	

EXHIBIT B of A-C

ACCOUNT NAMES FOUND & DUPLICATIONS CONTINUED

ACCOUNT NAMES	TIMES USED
Roger Denny	6
Joel Denny	1
Chandler Denny	
Drake Denny	
Denny Roberts Sanchez	1
Kevin Denny	
Richard Denny	4
Denny Jason	
Mike Denny	1
Thomas Aldason Denny	
Denny Robert	1
Denny Brian	1
Denny Michael	
Denny Walter	9
Parker Denny	
Bryan E. Denny	
Edward Denny	
Denny Scott	
Harry Denny	
Joy Denny	
Deny Ma Edmun	
Denny Edmund	
John Denny	6
Terry Denny Eric	
Tim Denny	
Patrick Denny	
Braww Denny	
Denny Lucas Davidson	
Jack Anderson	2
Denny Craig	
Denny Bensen	
Larry Roswell Denny	
Jackson Denny	1
Anthony Denny	
Michael Gabriel	
Denny Ryan	
Michael Denny	2
Michael Scott Denny	
Boyce Bryant	
Christopher Denny	
Kelly Denny Roland	
Albert Denny	2
Denny Davison Max	
Louis Bradley	
Bryan Denny Jimenez Erazo	
Denny Bryan	11
Denny Walter Bryan	
Bryan Denny Inoc	
Bryan O Denny	
Denny O'brien	3
Jackson Mikel	3

Dennis Alvin Jorgensen	
Denny Kelvin	1
Wayne Denny	
David Denny	2
Avin Denny	
Denny James	
Denny Richard	2
Kelvin Denny Smith	
Jeffery Johnson	
Jack P. Denny	
Denny White Johnson	
Eric Denny	
Denny Bruce	
Ben Denny Shipley	
Denny Brown	
Denny Pete	
Larry Barons Denny	
Denny Reilly	3
Denny Francisco Dollin	
Bill Matt	
Sanders James	
Mike Sanders	
Sanders Rogers	
Sanders Cox	
Sanders Brown	
Sanders Jackson	
Sanders Holloway	
Rodney Sanders	
Sanders James	
Sanders Vaughn	
Paton Sanders	
Harris Denny	
Alex Denny	1
Johnson Denny	1
Greg Howes	3
Kelvin Robert Denny	
Denny Kelly Robert	
Denny Scott Michael	
Walter Denny	2
Donald Denny	
Alberto Denny	1
Luke Denny	
Noah Denny	4
Jackson B. Denny	
Denny Anthony Bryan	
Earl Denny	
Dwayne Johnson	
Dick Denny	
Kennedy C. Denny	
Hillwood Denny	
Scott Mike Denny	5
Kelvin Anthony	

EXHIBIT C of A-C

ACCOUNT NAMES FOUND & DUPLICATIONS

Duke Bruse Salinas	
Thompson Freeman	
Rolf M. Reynolds	
John Owens	
James Wilson	
Jeff Rogers	
Paul Wilson	
Johnson James	
Kelvin Smith	
Denny Francisco	
Burrows Kelvin	
Denny Jordan	
William Denny	3
Lovely William Denny	
Scotch Denny	
Denny Bryan Harrington	
Grant Brian	
Scott Denny Lugard	
Henry Denny	
Denny Hurley	
Patrick Dennis	
Denny Frank	
Frank Richard Denny	
Henry Mark Denny	
Denny Reilly	
Scotty Denny Lugard	
Scotty Bryan Lugard	
Jackson Denny	

614

Key
Unable to Delete

UPDATED: DECEMBER 2017

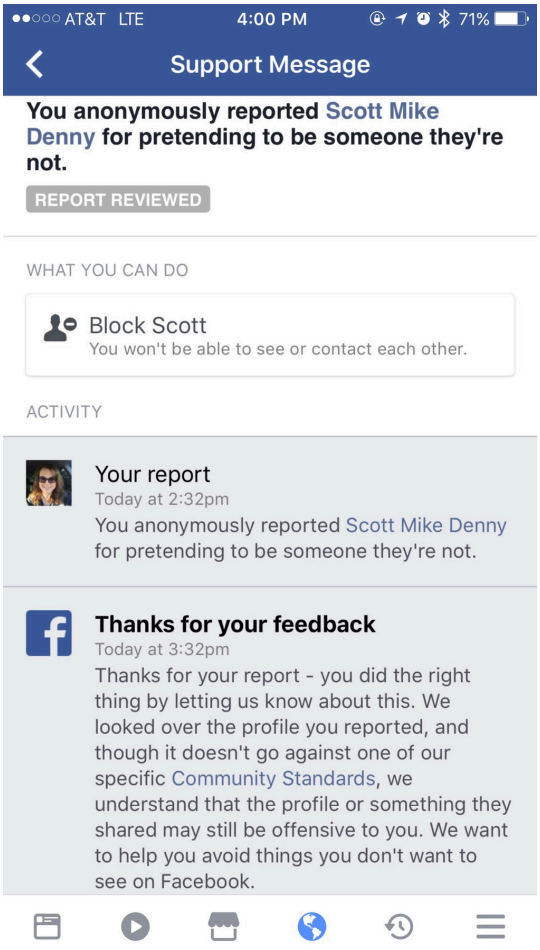
UPDATED ACCOUNT NAMES FOUND & DUPLICATIONS

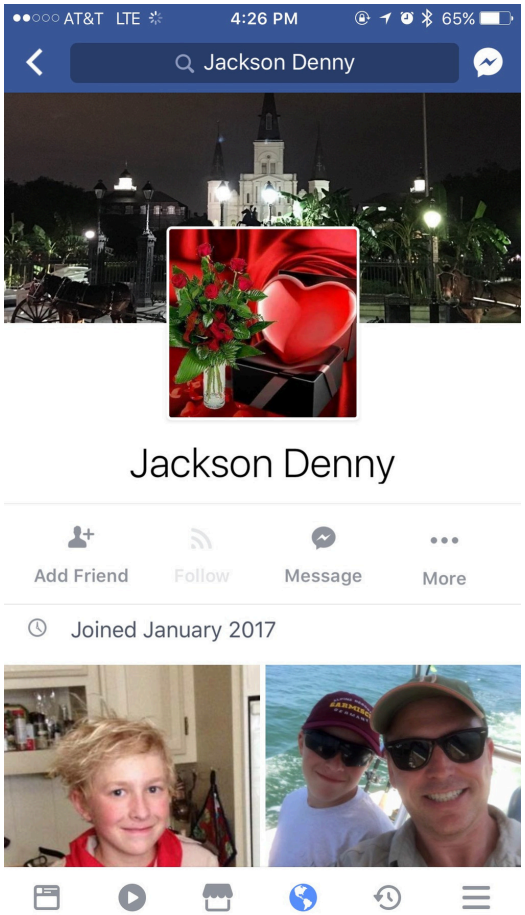
ACCOUNT NAMES	TIMES USED
Garry Denny	
Frank Denny	
Duncan James Philips	
Dennis Bryan	
Christopher Denny	
Marcos Alonso	
Sean Denny	2
Mcanthony Danny	
Maxwell Denny	
Henry Mark	6
Eric D. Lawrence	1
Jeff Smith Denny	
Denny Kenneth	
Bryan Kenneth	
Roger Denny	
Avalon Samuel Denny	
Denny Jerry	
Jefferry Egua Denny	
Blanchard Denny	1
Denny Stephen	
Denny Plantt	
Duke Bruse	14
Duke Bruse Alinas	
Duke Salinas Bruse	1
Duke Bruse Manilas	
Duke Bruse Toure	
Salinas Bruse Duke	1
Richard Cole Peter	
Peter Cole	
Jeff Denny	
Ron Perkins	
Nicholas Henry	
Maxwell Herrick (Bone)	
Denny Benson	3
Austin William Denny	
Duke Bruse Henry	
Henry G. Stevens	
William Frank	
Salinas Duke Bruse	
Henry Mark Duke	
Marc Denny	
Eric Danny Klein	
Steve Minnick	
Rob R. Perkins	
Jackson Morris	
Ryan George Danny	

ACCOUNT NAMES	TIMES USED
Denny Scott Lugard	1
Denny Scotty Lugard	
Eric Richard (Denny)	
Binney Scott (Binney A. Scot)	
Louis Aaron	
Rolly Denny	
Charles Kennedy Denny	
Gervas Wilson	5
Denny Wilson	
Denny Williams	2
Benson Denny	
James Morris	
James Bryan	
Bryan James	
Roger David Denny	
Eric Lawrence	
Carlos Olievera	
David Bryan	
Roger Amos Denny	
Roger Denny Frank	
James Collins	1
Bryan Danny	
TOTAL ACCOUNTS FOUND	735

UPDATE: December 2017- Facebook has deleted those mentioned
Additional 121 accounts found since July 2017 and added to list

EXHIBIT D of D-E





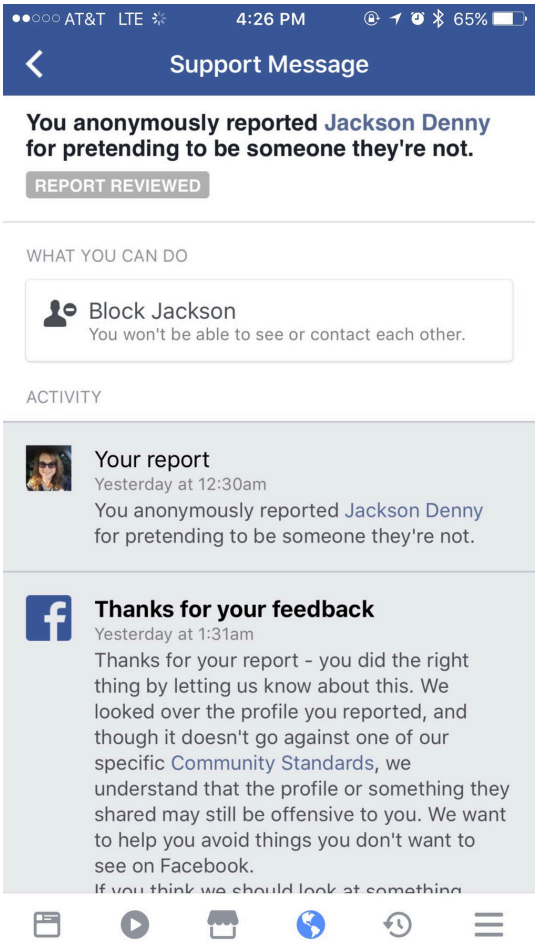
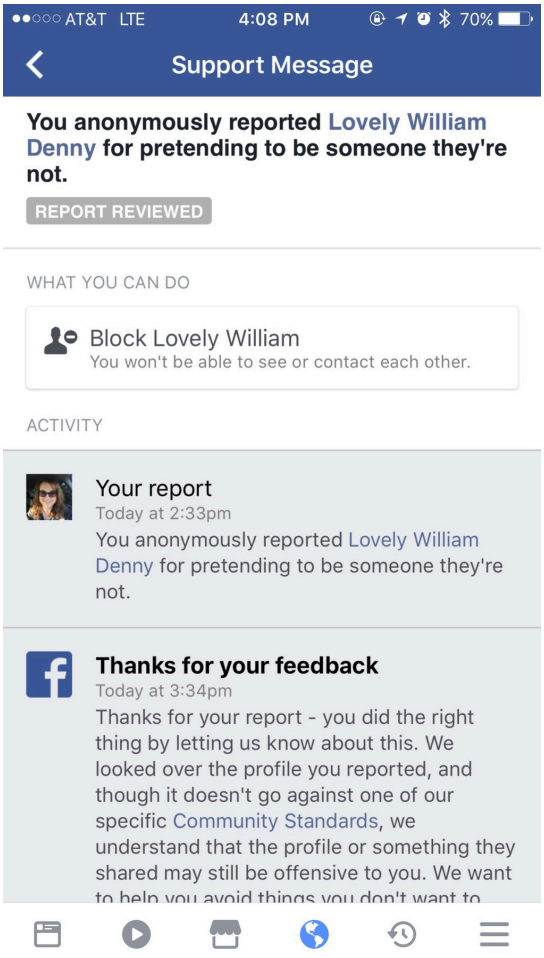
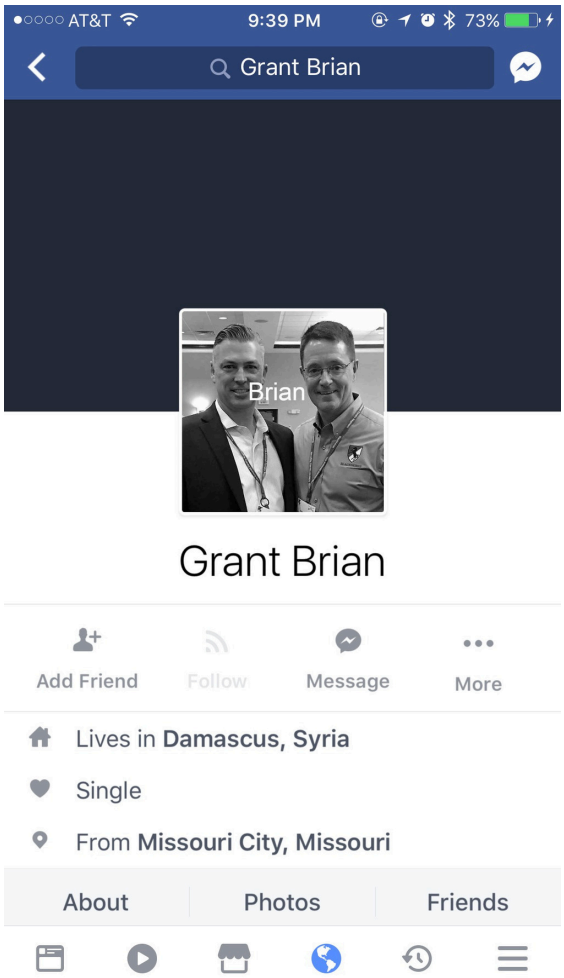


EXHIBIT E of D-E





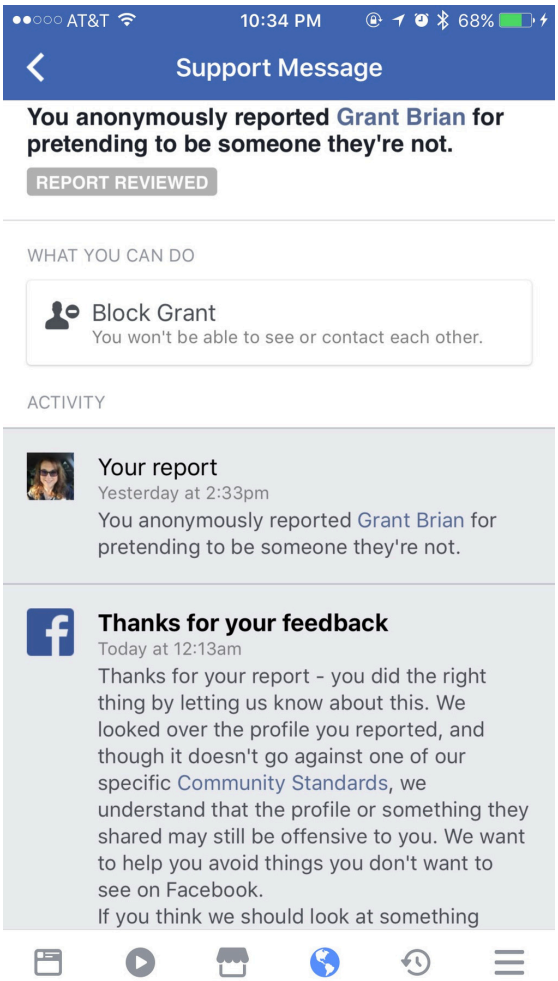
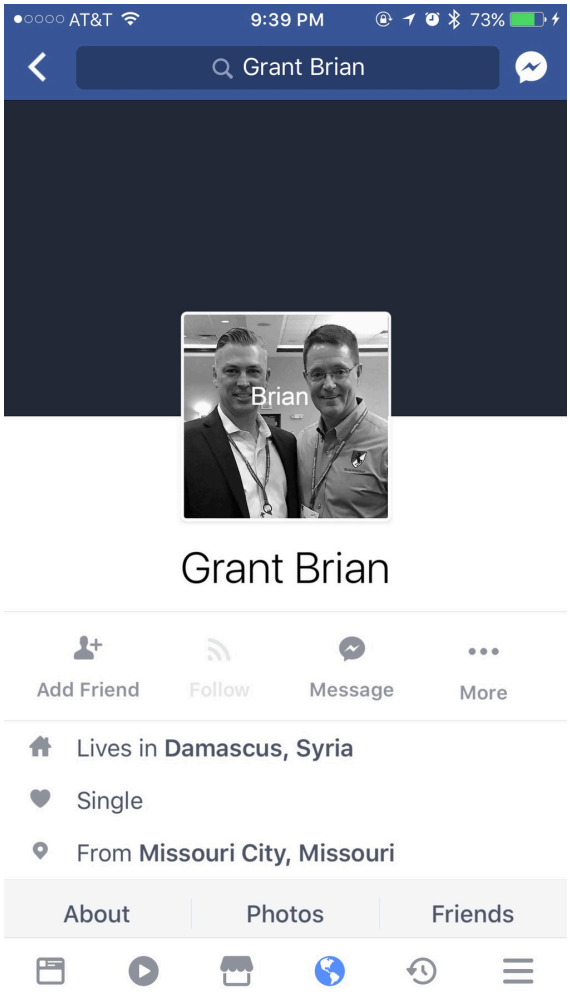
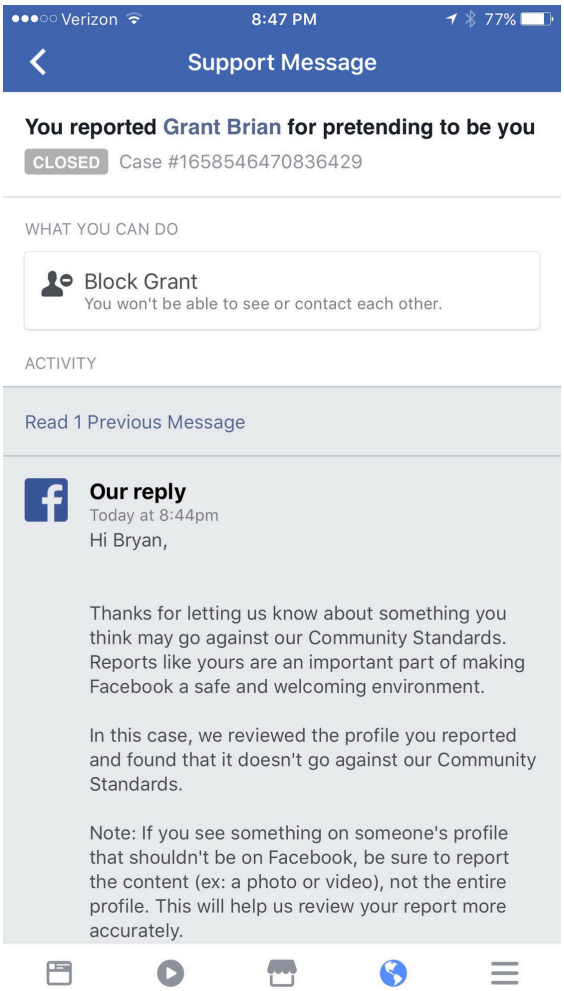


EXHIBIT F of F-G





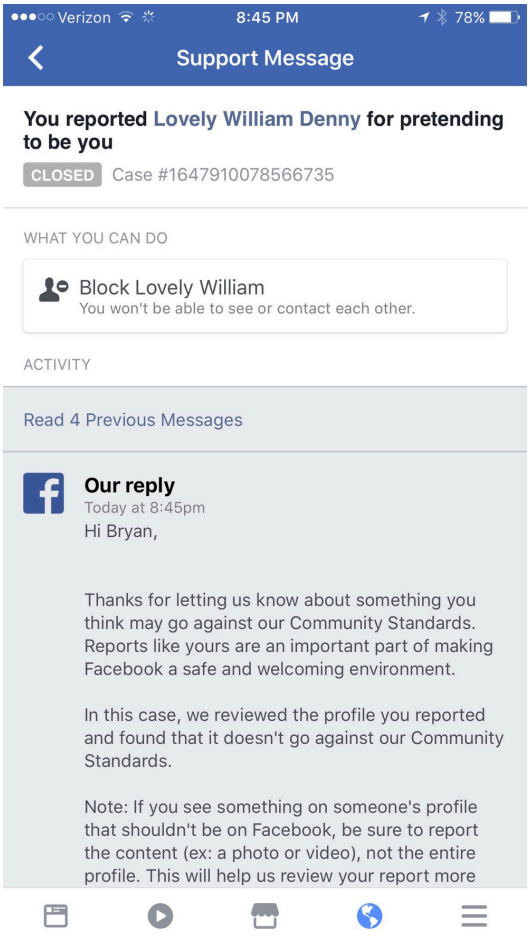
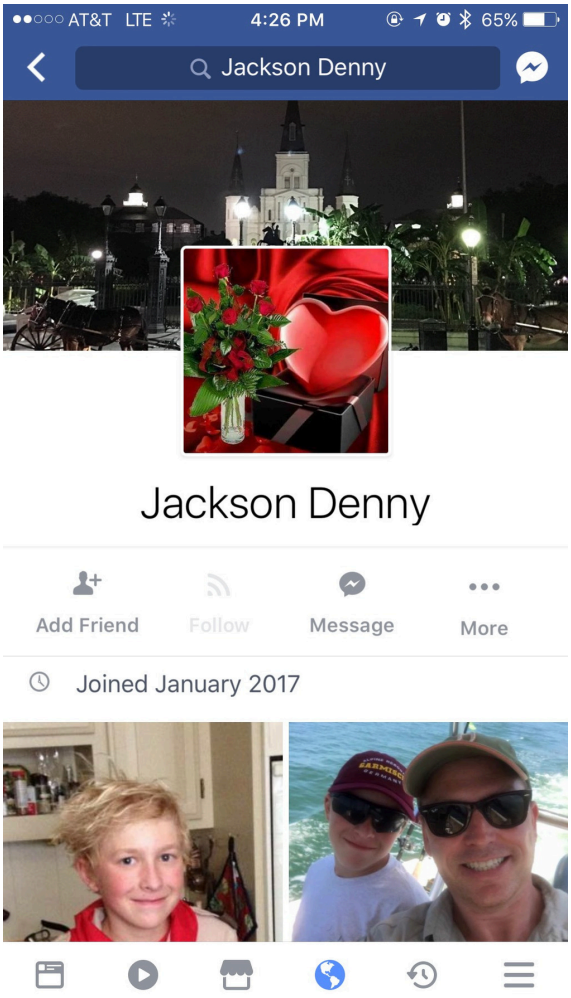


EXHIBIT G of F-G



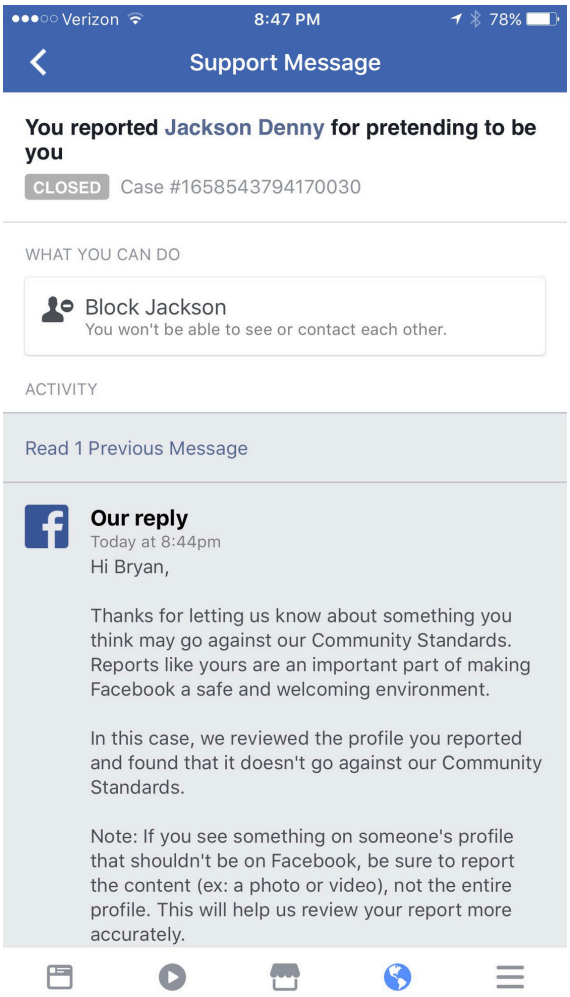
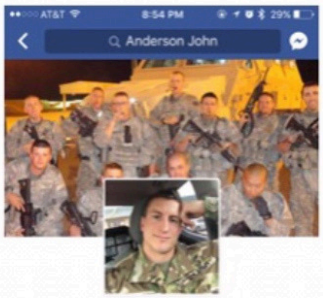


EXHIBIT H



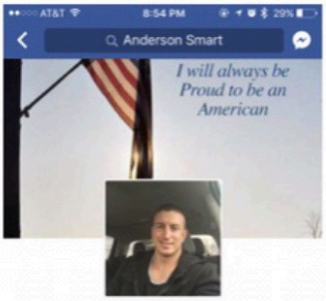
Anderson John

Add Friend · Message · More

i easily socialise with people..i love meeting people and understanding peoples predicaments.

Captain at U.S. Army

Lives in Bradfordsville, Kentucky



Anderson Smart

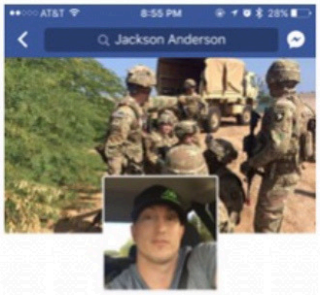
Add Friend · Message · More

Seargent Major at United States Army

Former Captain at United States Army

Studied at University of Kentucky

Went to construction high school



Jackson Anderson

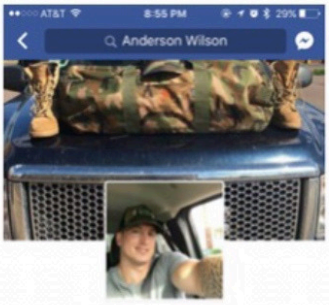
Add Friend · Message · More

Sergeant at U.S. Army

Single

From New York, New York

About · Photos · Friends



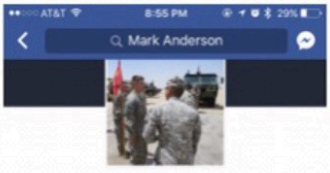
Anderson Wilson

Add Friend · Message · More

Sergeant at Arms at United States Military Academy

Went to West Point - The U.S. Military Academy

Lives in Mission Beach, Washington



Mark Anderson

Add Friend · Message · More

Worked at United States Army

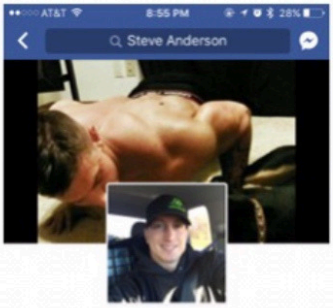
Studied Bachelor of Science in Business Administration/Small Business Management and Entrepreneurship at University of Phoenix

Went to Serrano High School

Lives in Kuwait City

From Wrightwood, California

About · Photos · Friends



Steve Anderson

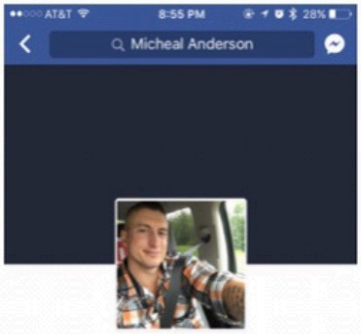
Message · More

Sergeant of Officers at U.S. Army

Lives in Denver, Colorado

From Denver, Colorado

About · Photos · Friends



Micheal Anderson

Add Friend · Message · More

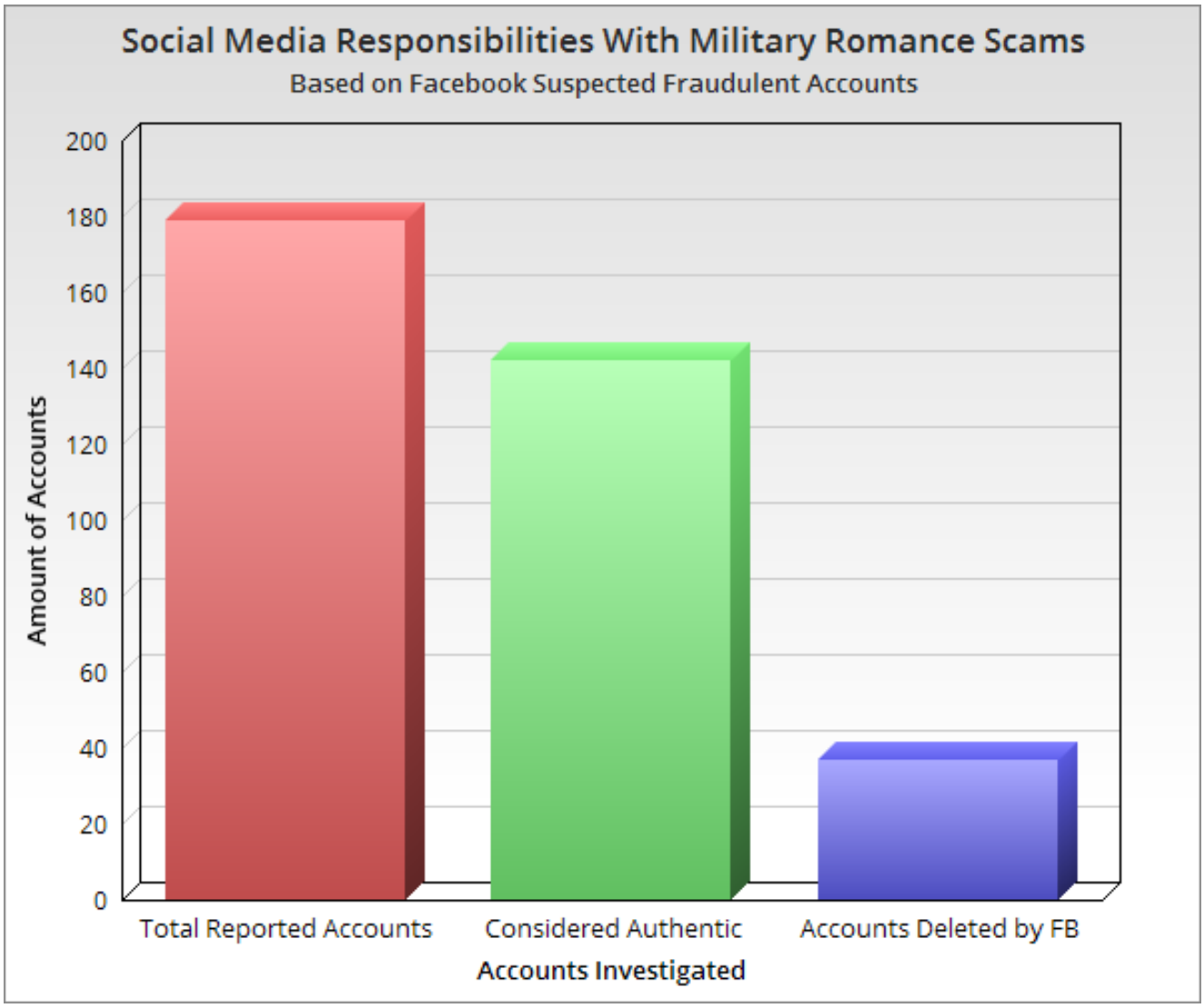
Works at U.S. Army

Lives in Indianapolis, Indiana

Single

From Indianapolis, Indiana

EXHIBIT I


Social Media Responsibilities With Military Romance Scams
Based on Facebook Suspected Fraudulent Accounts
Amount of Accounts
200
180
160
140
120
100
80
60
40
20
0
Total Reported Accounts
Considered Authentic
Accounts Deleted by FB
Accounts Investigated