Disrupting Terrorist Financing on Social Networks and Video Game Platforms

A Guide for Non-Traditional Financial Institutions and the Banks That Hold Their Accounts

Scott F. Butler, CAMS, CFE

Table of Contents

Executive Summary

Transaction monitoring-based and geography-based counter-terrorist finance regimes are not adequate to protect 21st century financial companies from extremist exploitation. A new methodology is required by which non-traditional financial institutions can monitor for "small scale" terrorist finance transactions and guard against radicalization via their platforms. Specifically, this analysis applies to social networks with a money transmission component (like Facebook or Snap) and video game companies that allow their users to interact and transact within virtual environments (Riot Games, Blizzard). Those entities are referred to as "social-financial companies."

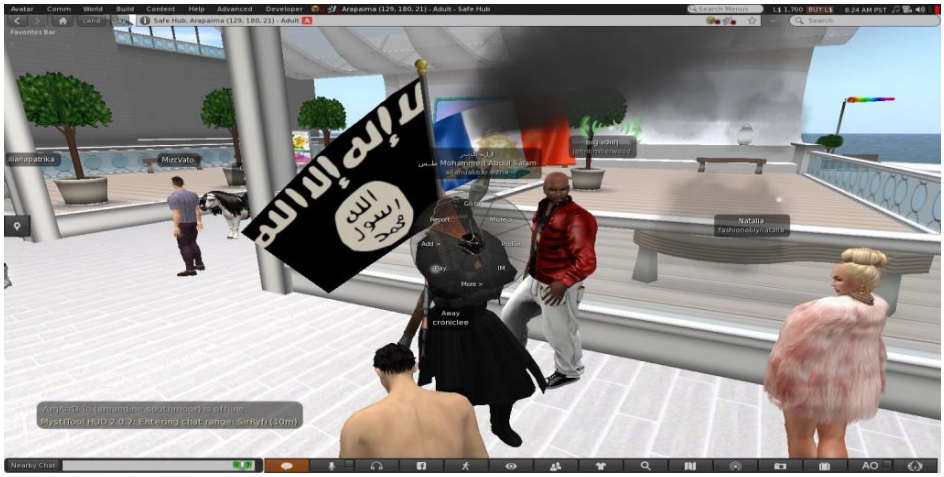
There are myriad ways to prevent known extremists from holding accounts at banks, money transmitters and other legacy financial institutions. That class of companies has also received adequate guidance about how to monitor for terrorist financing transactions. However, those efforts will need to be reconsidered for the new social-financial landscape.

A Tale of Two Alerts

On November 13, 2015, a small group of terrorists killed 89 people inside of the Batalcan night club in Paris, France. The high profile attack was the latest in a series of murders committed by individuals who were either affiliated with or inspired by the global terrorist organization, ISIS.

Less than a month after the Bataclan murders, two incidents of extremist behavior were escalated to the compliance team at Linden Lab, the company that operates the virtual world "Second Life."[1] One escalation was a report that a "resident" (the term used for Second Life players/customers) was selling ISIS flags in Second Life's online marketplace. The second was a report about a resident who had made statements supportive of the Bataclan attack in a public chat forum.

[1] A 'virtual world' is a 3-D simulated social environment that allows individuals to engage with one another via semi-anonymous avatars. "Second Life" is one of the oldest (in operation since 2003) and most successful of these ecosystems. See "Carstens, Cameron and Lawson, Ken. "Virtual Worlds: The New Frontier." *ACAMS Today*, 4 Dec. 2012, www.acamstoday.org/virtual-worlds-the-new-frontier/.



An avatar wielding an ISIS flag, observed within "Second Life" in December of 2015.

Linden Lab is a registered money services business, both with the federal government and (via its payments subsidiary Tilia, Inc.) as a licensed money transmitter in all states where a license for its activity is required. As such, Linden Lab employs an anti-money laundering (AML) program that includes risk-based counter-terrorist financing (CTF) measures. The CTF protocols are informed by the Federal Financial Institutions Examination Council's (FFIEC) Examination Manual, the Bank Secrecy Act (BSA) and data analysis. However, since there was no financial activity involved in the two escalations in question, a CTF regime that relied exclusively on transaction models and geographic risk factors would not have alerted for either of the December 2015 incidents. Though the FFIEC suggests certain transaction types and customer behavior that should alert for suspicious activity,[2] neither of the scenarios would have been captured with protocols based exclusively on that guidance.

Nevertheless, one of the escalations resulted in attention from federal law enforcement and prompted an enhanced criminal investigation. If not for a commitment to CTFF: Count-Terrorist Financing *and Facilitation* as opposed to the minimally required CTF program, the behavior may not have been detected.

Which case turned out to be more serious? Which alerted individual would eventually mirror the profile another notorious, violent extremist? How were both cases disposed and/or escalated? How should future extremist alerts be handled?

[2] "Appendix F: Money Laundering and Terrorist Financing Red Flags." Bank Secrecy Act Anti-Money Laundering and Terrorist Financing "Red Flags" , Federal Financial Institutions Examinations Council, Dec. 2014, www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_106.htm.

The New Reality of "Small Scale" Terrorist Financing and Recruitment

"The single best predictor of whether someone gets involved in a terror organization is if their friends or peers are also involved,"[3] posits Oxford University professor Scott Atran. Atran is an expert in extremist recruitment who has presented his findings to the United Nations and is a frequent contributor to the discourse surrounding trends in modern terrorism. Atran was referencing an incident in which seemingly well-adjusted Somali medical students shocked their families by traveling to Syria to join ISIS. However, he could just have easily been referencing the phenomenon of the nebulous peer groups that form on social media platforms like Facebook and Snap or in collaborative online gaming experiences hosted by platforms such as Microsoft's Xbox Live or Sony's Playstation Network.

National security analyst Peter Bergen echoed Atran's sentiment in testimony before the U.S. Senate Committee on Homeland Security, calling for a reconceptualization of the lone wolf terrorist in the "age of social media." "A militant radicalizing in front of his or her computer by himself at home is now not really alone," Bergen declares. "He/she is swimming in a virtual sea of jihadist recruiters, cheerleaders and fellow travelers who are available for interaction with him or her 24/7."[4]

Likewise, Middle East scholar Nate Rosenblatt's comprehensive study "All Jihad is Local", notes that hyper-local and hyper-specific conditions are the main predictors of an individual's radicalization. In other words, discrete personal and political grievances can foment into violent political extremism. While Rosenblatt's analysis specifically concerns the phenomenon of the ISIS terrorist organization, his conclusion that intervention is key to impeding politically motivated violence can be applied to social media and gaming platforms.

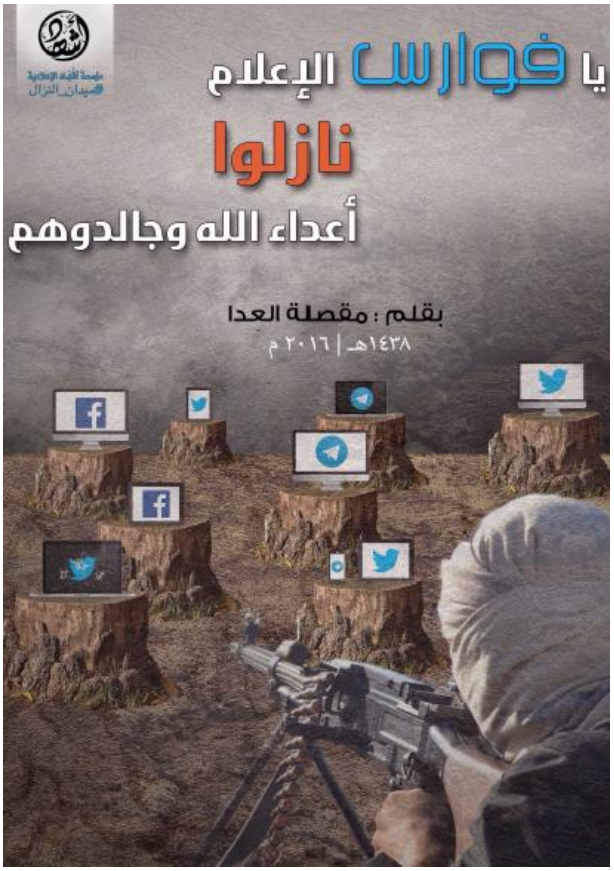
From the Austrian teenager who downloaded bomb-making plans via Sony's Playstation Network,[5] to the jihadi who groomed a developmentally disabled teenager via Facebook's

[3] Vedantam, Shankar, and Maggie Penman. "The Psychology of Radicalization: How Terrorist Groups Attract Young Followers." Hidden Brain, National Public Radio, 15 Dec. 2015, www.npr.org/2015/12/15/459697926/the-psychology-of-radicalization-how-terrorist-groups-attract-young-followers. The quote is Vedantam's summary of Scott Atran's radicalization thesis.

[4] "ISIS Online: Countering Terrorist Radicalization & Recruitment on the Internet and Social Media." Peter Bergen's testimony before the U.S. Senate Committee on Homeland Security, Permanent Subcommittee on Investigations. 6 July 2016. Accessed 1 September 2017.

[5] Nasralla, Shadia, and editing by John Stonestreet. "Teenager in Austrian 'Playstation' terrorism case gets two years." Reuters, Thomson Reuters, 26 May 2015, www.reuters.com/article/us-mideast-crisis-austria/teenager-in-austrian-playstation-terrorism-case-gets-two-years-idUSKBN0OB0LK20150526.

WhatsApp messaging service,[6] to the Al-Qaeda fighters who post Snapchat "selfies" with AK-47s the same way that mainstream social media celebrities would "hashtag their bling,"[7] extremist leveraging of online platforms is a reality. Furthermore, to paraphrase Rosenblatt's study, when a potential member of a violent group is only an instant message away no matter where he or she is located in the physical world, all extremism is local.



The cover of a manual distributed by an ISIS propaganda arm in which jihadists are encouraged to engage in hacking, agitprop and other forms of mayhem via social platforms.[8]

[6] Gardham, Duncan. "Teenage Islamic terrorist who groomed man with learning difficulties to carry out Lee Rigby-Style attack on British soldier is jailed for eight years." Daily Mail Online, Associated Newspapers, 29 May 2015, www.dailymail.co.uk/news/article-3102624/Teenage-Islamic-terrorist-groomed-man-learning-difficulties-carry-Lee-Rigby-style-attack-British-soldier-jailed-eight-years.html.

[7] Bodetti, Austin. "The selfie jihadi: Inside al-Qaeda's Snapchat network." Alaraby, The New Arab, 19 Sept. 2017, www.alaraby.co.uk/english/indepth/2017/9/19/selfie-jihadi-inside-al-qaedas-snapchat-network.

[8] The "Ashhad Media Foundation" is a propaganda arm of the ISIS terrorist organization. This publication was issued by the foundation in October of 2017 and accessed via the "dark web" with a complete copy available via Bayt Al-Masadir, the Jihidi Primiary Source Omnibus.

To their credit, Snap Inc., Google, Microsoft, Twitter, Facebook and others companies in that shared space seem to recognize the problem. The tech organizations formed the Global Internet Forum to Counter Terrorism (GIFCT), a forum that will focus on technological solutions, research and knowledge sharing.[9] The formation of the commission is an acknowledgement of the issue that has concerned some national defense and industry experts since 2008. Namely that online games, virtual worlds and social networks provide both enemy nations and terrorist organizations "completely unfettered access to communications, recruiting, financing, planning and operations."[10] When you include the relatively recent phenomena of online radicalization, "lone wolf-mass casualty" attackers inspired by "global" rhetoric and the evident low cost of recent violent attacks (the price of a truck rental, guns and ammunition, a hotel room, etc.), the problem is clear.

What is less clear are the next concrete steps that can be taken from an anti-money laundering/counter-terrorist financing compliance perspective. For company officers who implement BSA programs within social financial companies or for compliance officers at banking institutions that hold accounts for those companies, what are realistic, pragmatic steps that can be taken to ensure that our CTF (or CTFF, as I would advocate) programs are effective? What constitutes a meaningful CTF regime in light of this new landscape?

The Online Extremist Threat Matrix

"Make no mistake: the fight is moving from the battlefield to the internet," stated Prime Minster Theresa May during the first G7 meeting following the May 2017 ISIS-inspired attack on a concert in Manchester.[11] At that meeting, the member nations were in unanimity that social media and internet companies must to do more to crack down on extremist content. Were they aware of the extent that money can be exchanged via most social media profiles or the ease in which money transfers can be arranged via collaborative online games, it stands to reason that the G7 leaders would argue that it is even more critical for social media and internet companies that facilitate money movement to curb the extremist activity on their platforms.

---

[9] "Global Internet Forum to Counter Terrorism." Twitter, Twitter Public Policy, 26 June 2017, blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html.

[10] Ricks, Thomas E. "Terrorists, video games and us." Foreign Policy, 16 Nov. 2015, foreignpolicy.com/2015/11/16/terrorists-video-games-and-us/.

[11] LeFebvre, Rob. "Theresa May wants to force tech giants to curb extremist content (Updated)." Engadget, 30 May 2017, www.engadget.com/2017/05/26/theresa-may-g7-extremist-content/.

A more conservative reading of the FFIEC Examination Manual seems to indicate that social financial companies already have the responsibility to gauge how radicalization on their platforms could give rise to terrorist financing. At the risk assessment level, compliance officers are compelled to assess how "products and services" offered by their institution affect their institution's risk profile.[12] Similarly, in the OCC's counter-terrorist financing guidelines, the agency mandates that banks need to have a "thorough understanding" of the risks within its lines of business.[13] An OCC examiner should, by that measure, assess the strength of a customer's CTF regime based on the underlying risks of the company. A money transmitter that supports a platform where people worldwide can create semi-anonymous personal profiles, privately interact with individuals in other parts of the world and potentially consume dangerous propaganda, such as Facebook Payments Inc. for Facebook, would need to take into account the underlying risk of Facebook as a tool for radicalization and hotbed of extremist activity, independent of the risks associated with actual money transfers.[14]

Given the absence of guidance in the online social-financial company space, what should regulators and invested parties be seeking in the risk assessment for such companies? What are the measures of a successful CTF regime for those institutions?

The Online Extremist Threat Matrix: Escalations

The foremost requirement for a CTF regime within a social-financial company is a strong system of escalations. Since chat room activity- some of it ephemeral by design, some of it verbal- cannot be easily mined or sorted, the data used to detect and intercept extremist behavior is most effectively derived via escalations/alerts generated by other customers/game players ("the community").

[12] "BSA/AML Risk Assessment - OVerview." Online Manual - BSA InfoBase - FFIEC, Federal Financial Institutions Examinations Council, 2014, www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_005.htm.

[13] "Counter Terrorist Financing." OCC: Counter Terrorist Financing, 29 Dec. 2010, www.occ.treas.gov/topics/compliance-bsa/bsa/counter-terrorist-financing/index-counter-terrorist-financing.html.

[14] Dreyfuss, Emily. "This Is How Facebook Fights Extremists." Wired, Conde Nast, 16 June 2017, www.wired.com/story/facebook-counterterrorism/. Accessed 2 Oct. 2017. Facebook has acknowledged that it must continue to find ways to combat extremism on its platform and has engaged in deradicalization efforts.

A regulator or financial institution that wished to gauge the health of an online social-financial company within its purview should test for the following:

- Does the company have an "escalations manual" that details the way extremist and other behaviors are brought to the attention of the company?
- Does the company have an escalation form that is easily accessible to its users/players?
- Does the form specifically identify extremist/violent rhetoric and activity or reference extremist recruitment?
- Is there a flexible system in place for banning extremists and extremist language in user names, avatar names, etc.?
- From the escalation path, are analysts able to determine the origin of the threat via IP detection and device ID detection?

The ideal escalations path would be both reactive and proactive.

The reactive portion should include a "one touch" or "low touch" escalations path for users/customers. Twitter, for instance, offers a pull-down menu in the upper right-hand corner of each communication that allows you to "report" a Tweet, which then sends the communication on an escalation path that preserves the original Tweet and provides the reviewing analyst with context to the escalation. In a social network, the escalation could include a post, a portion of a chat or a profile. In a gaming environment the escalation could include a communication or a screenshot of the offending behavior. The technical capabilities of the escalation path should be suited to the product.

Foremost, the escalation must be actionable. The profile name (in the case of a social media company) or avatar name (in the case of a virtual world or gaming company) must trace to a customer profile. If the individual behind the alerted profile/avatar has transacted with the company, the reviewing analyst should be able to inspect the corresponding transaction record. If the person has not yet transacted (e.g. a social media profile that has not engaged in money transfer activity; a gamer who has yet to make "in-game" purchases), the analyst should still be able to cull metrics to create a "back-end" profile of that individual. At minimum, these markers should meet

the FFIEC guidelines for mobile security[15] but will ideally include IP address identification with a proxy/fake IP detection component and a device identification/device reputation tool.

In the context of escalations for extremist behavior, any transactions associated with the alerted customer must receive heightened scrutiny. Analysts should review the alerted individual's money transfers or purchases regardless of the amount. Traditional transaction monitoring models or pattern recognition systems may not be configured to detect relatively low dollar amounts. Nevertheless, low dollar activity when attributed to a higher risk individual should be considered high risk because those small sums have (in recent history) been used to fund low-cost terrorist operations and cross-border travel to extremist-controlled territories.[16] The very nature of an escalation for extremist behavior, when deemed credible via first level/tier one analysis, should compel the analyst to treat the individual as "high risk", with ensuing escalations to more advanced tiers of reviewers for further action or reporting.

The proactive aspect of an effective escalation process involves the collection and analysis of data that is related to the escalations. The information should be used to inform a process to review problem areas within a social network or game and to exile any bad actors. The International Centre for the Study of Radicalization and Violence's (ICSR) "Countering Online Radicalization" study[17] and a more recent Council on Foreign Relations white paper[18] suggest measures that include deterring producers of extremist material via periodic content reviews and takedowns and empowering online communities to self-regulate (encouraging escalations).

Again, the foundation of an effective CTF policy for social-financial companies is an understanding of each individual company's customers' behavior. A reliable escalation process is the first step; a reliable process for discerning genuine threats from mere nuisances is the second.

---

[15] Lynch, Michael. "How device intelligence tech can help FIs comply with key FFIEC mobile security guidelines." Mobile Payments Today, 10 June 2016. www.mobilepaymentstoday.com/articles/how-device-intelligence-tech-can-help-fis-comply-with-key-ffiec-mobile-security-guidelines/.

[16] Martin, Will. "One chart shows how little its costs terrorist groups like ISIS to carry out attacks in Europe." Business Insider, 2 Dec. 2016, www.businessinsider.com/how-much-do-terrorist-attacks-cost-deutsche-bank-2016-12.

[17] "Countering Online Radicalisation: A Strategy for Action." The International Centre for the Study of Online Radicalisation and Violence, 2009, doi:10.18411/d-2016-154.

[18] "Countering Islamic State Exploitation of the Internet." Council on Foreign Relations, Council on Foreign Relations, 18 July 2015, www.cfr.org/report/countering-islamic-state-exploitation-internet. Accessed 1 Sept. 2017.

The Online Extremist Threat Matrix: Extremist Profiles

The Global Head of Financial Intelligence and Security for Western Union, Bryant Gofstein, advocates a "target to typology" approach to combatting terrorist financing[19]. He recommends recording the characteristics of terrorist financiers, searching all transactions based on those typologies and identifying any individuals or entities that meet that criteria.

Mr. Gofstein's recommendation with regard to CTF regimes in banks and money services businesses will also be effective for social-financial companies. While helping to construct Facebook's initial anti-money laundering program[20] and conceiving the compliance program for Linden Lab's payments subsidiary, I personally reviewed escalations, alerts and data related to "bad actors" within those respective ecosystems. Based on that experiential data, along with anecdotal data gleaned via information sharing sessions with Coinbase, AirBnB, LinkedIn and Google,[21] I developed the following CTF(F) "risk matrix" for social-financial companies.

The matrix parses three types of alerts for users/customers who have been escalated for having potential terrorist sympathies or who are at risk for financially assisting a terrorist operation: griefers, supportive actors and threats.

---

[19] Gofstein, Bryan. "The New CTF: Reviewing Practical Tools to Counter Terrorism's Evolving Financing Methods." ACAMS 16th Annual Global and Financial Crime Conference, ACAMS, Las Vegas, Nevada, 26 Sept. 2017.

[20] First as an AML consultant, then a Compliance Manager, then as a Chief Compliance Officer, I installed Facebook Payments Inc.'s anti-money laundering and counter-terrorist financing controls, including the first compliance program for Facebook Messenger's peer-to-peer money transfer system.

[21] As per a statement from the organizers, including Paul Rockwell, Head of Trust and Safety at LinkedIn, the "Risk Salon" is an invite-only forum for people who work in the risk space that includes fraud, compliance, and trust & safety. The goal of the group is to share ideas between people at different companies from diverse function areas of risk including ops, data sceince, engineering and product. Infromation regarding this paper was discussed under Chatham House rules at the Risk Salon event on September 13, 2017 and should not be construed as specific advice provided by or for any specific company.

	Degree of threat	Recommended Action
Griefers	One-off abusive communication	> Warning or discipline as per organization Terms of Service ("TOS")
	Serial abusive communications	> Discipline as per organization TOS
	Coordinated abusive communications	> Discipline and/or banning of alerted individuals
Supportive Actors	Customer engaging in hacking or fraud from a high risk jurisdiction	> Banning of alerted individual
	Repeat hacking or fraud activity from a high risk jurisdiction	> Banning of alerted individual and strong consideration for SAR filing even if below $ reporting threshold
	Coordinated hacking or fraudulent behavior from a high risk jurisdiction	> Banning, SAR reporting and coordination with security, site integrity and anti-fraud teams
Threats	Extremist rhetoric followed by attempt to "back channel" extremist communications	> Enhanced monitoring, investigation, possible SAR filing
	Operation of an extremist chat room or serial extremist postings.communications	> Enhanced monitoring, investigation, preservation of chat logs and other evidence, SAR filing even if below $ reporting threshold
	Identified as making actual threats; verified contacts with known extremist groups or individuals	> Immediate coordination with law enforcement, preservation of chat logs and other evidence, enhanced monitoring, SAR filing

1 - "Griefers" (sometimes referred to as "trolls") are individuals who may pose as extremists or use extremist rhetoric to elicit a strong reaction from another game player or social media user but are otherwise non-affiliated with extremist groups. Griefers or "griefing" in the online gaming world is an "anti-social phenomenon" that involves one game player deliberately disturbing another game player's experience. While the motivations behind griefing are myriad they are not, according to studies of griefing behavior, affiliated with the material support of "real world" extremist activity[22].

[22] Achterbosch, Leigh. "A taxonomy of griefer type by motivation in massively multiplayer online role-playing games." Taylor & Francis. March 29, 2017.

An illustrative exchange took place in 2014/2015 within Rockstar Games' "Grand Theft Auto" (GTA) forum. One game player reported that a group of game players (a "crew") had been posing as a terrorists within the GTA environment.[23] The online community conducted their own ad hoc investigation (looking at the crew's public profile and other activity) and responded to the individual's concern by indicating that the terrorist crew were more than likely "griefers" due to the analysis of their behavior within the wild and lawless "in-world" environment that comprises the GTA universe. All social-financial companies should have the internal intelligence to formally conduct similar investigations based on a knowledge of their own ecosystems so that resources can be devoted to eradicating actual threats.

2 – "Supportive Actors" are customers who have not made explicit pro-extremist/pro-terrorist statements but have exhibited behaviors or characteristics that have been identified as "high risk" for extremism.

These alerts can be generated via escalations (e.g. customers observing a suspect Facebook page that purports to be an Islamic charity) fraud or transaction monitoring alerts.

An example of an alerted "supporting actor" would be a group of "card testers" (individuals who attempt small transactions with a large pool of stolen credit cards to determine if the cards are valid) who are from a jurisdiction that is at high risk for terrorism.[24]

These cases should be treated with elevated concern even if the card testers do not otherwise resemble extremist accounts.[25] A suspicious activity report (SAR) should be filed, even if the dollar amount falls below the reporting threshold; closure and/or ongoing monitoring of the alerted accounts should recur, as warranted.

---

http://www.tandfonline.com/doi/abs/10.1080/0144929X.2017.1306109?journalCode=tbit20. Volume 36, 2017 - Issue 8

[23] "Terrorist crews on GTA Online." Rockstar Support, 27 Apr. 2017, support.rockstargames.com/hc/en-us/community/posts/115006229927--p-Terrorist-crews-on-GTA-Online-p-. (the report of "terrorist" activity was from a Community Forum page for Rockstar Games' Grand Theft Auto game; that particular crew has since been removed from the online GTA game.)

[24] "Militants using gift cards to bankroll terrorism, intelligence agency says." The Guardian, Guardian News and Media, 1 May 2017, www.theguardian.com/australia-news/2017/may/02/militants-using-gift-cards-to-bankroll-terrorism-intelligence-agency-says.

[25] "Country Reports on Terrorism." U.S. Department of State, U.S. Department of State, 30 Apr. 2017, www.state.gov/j/ct/rls/crt/. Accessed 0ADAD.

3 – "Threats" are individuals or groups whose behavior is in sync with some of the methodology used for online radicalist recruitment, such as a period of exhorting extremist rhetoric in an effort to find like-minded or vulnerable individuals that is followed by a period of "going dark" or ceasing communications.

Unlike "griefers" who will relentlessly needle other individuals or pollute a public environment and persist until their presence is neutralized, individuals who operate on the "threat" level will sometimes include a reference to a "back channel" communication such as a private chat room or an open invitation to a non-public chat.

Once that behavior is identified, a thorough review of the individual's online activity should occur, with scrutiny placed on any transactions that the individual may have attempted or executed.

If the investigation yields additional red flags, a law enforcement contact should be consulted (even off the record) to determine potential next steps. Extended logging of the individual's activity/chats should be initiated and the individual's account should be closely monitored.

The Avatar Broke Bad

The "Online Extremist Threat Matrix" was effective in handling and disposing both of the alerts described at the outset of this paper. The seller of the ISIS flag turned out to be a non-threatening marketplace salesman. His virtual shop- a place where Second Life game players could purchase flags for their avatars or avatars' homes- was comprised entirely of international flags. The proprietor of the shop did not realize that it would be upsetting to most people within the Second Life community to see a flag that symbolizes violence and terror within their public marketplace. The virtual shopkeeper voluntarily deleted the ISIS flag from his store.

The second alerted individual (referred to as "the suspect" going forward) exhibited very different behavior. This suspect chatted openly about his extremist views and- when he identified individuals within his chat room who seemed sympathetic to some of his statements- he invited them into a private chat. The move from public to private is a red flag as it suggests that more nefarious activity (such as financial arrangements, incident planning, etc.) could be taking place "out of sight" of administrators and the rest of the community.

The subsequent investigation of the "suspect" revealed him to be an individual who had participated within the Second Life ecosystem for approximately five years. Alerts about the individual increased over time, with the suspect having been previously reported for boasting about

a firearms collection. An analysis of the suspect's "in world" activity found increasingly frequent cycles of the suspect espousing extremist rhetoric in open fora followed by periods of private, "off-the-grid" activity.

On the date that the second alert was escalated to the compliance department, the "suspect" had espoused extremist views in an open forum but quickly expressed an interest in engaging further in a private chat room. Based on an escalation within the suspect's private chat area, the suspect apparently believed that the Bataclan terrorist attack in Paris was justified and suggested that another attack was imminent.

After consulting with a contact at Financial Crimes Enforcement Network (FinCEN), the compliance team alerted the FBI field office within the suspect's jurisdiction. When the investigator in the case attempted to access the individual's account for further monitoring, she discovered that the suspect had closed his account and fled Second Life, seemingly aware that his online behavior had been exposed.

Conclusion

The escalated cases at Linden Lab were only two reports of many (in some cases thousands) that game companies and social networks receive on a daily basis. For regulated entities, the BSA requirement that a company screen its in-scope customers against sanctions lists and that transactions are monitored for terrorist financing are guidelines that may satisfy regulators but are entirely inadequate to protect platforms and platform customers from extremist behavior, radicalization and any related illicit financing.

The new "online threat matrix" should provide regulators- and regulated entities that conduct business with social network/video game companies- measures for evaluating whether terrorist finance risk is being adequately addressed based on the platform's content. Social-financial companies are at enhanced risk for exploitation by bad actors and, as such, enhanced measures must be taken by those institutions to protect their online communities as well as the communities outside their online worlds or corporate offices.

REFERENCES

[1] "Tilia Inc. Description of Business", an internal company document supplied to state regulators during the money transmitter license application process.

[2] "Appendix F: Money Laundering and Terrorist Financing Red Flags." Bank Secrecy Act Anti-Money Laundering and Terrorist Financing "Red Flags", Federal Financial Institutions Examinations Council, Dec. 2014, www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_106.htm. Accessed September 2017.

[3] Vedantam, Shankar, and Maggie Penman. "The Psychology of Radicalization: How Terrorist Groups Attract Young Followers." Hidden Brain, National Public Radio, 15 Dec. 2015, www.npr.org/2015/12/15/459697926/the-psychology-of-radicalization-how-terrorist-groups-attract-young-followers. The quote is Vedantam's summary of summary of Scott Antram's radicalization thesis.

[4] "ISIS Online: Countering Terrorist Radicalization & Recruitment on the Internet and Social Media." Peter Bergen's testimony before the U.S. Senate Committee on Homeland Security, Permanent Subcommittee on Investigations. 6 July 2016. Accessed 1 September 2017.

[5] Nasralla, Shadia, and editing by John Stonestreet. "Teenager in Austrian 'Playstation' terrorism case gets two years." Reuters, Thomson Reuters, 26 May 2015, www.reuters.com/article/us-mideast-crisis-austria/teenager-in-austrian-playstation-terrorism-case-gets-two-years-idUSKBN0OB0LK20150526.

[6] Gardham, Duncan. "Teenage Islamic terrorist who groomed man with learning difficulties to carry out Lee Rigby-Style attack on British soldier is jailed for eight years." Daily Mail Online, Associated Newspapers, 29 May 2015, www.dailymail.co.uk/news/article-3102624/Teenage-Islamic-terrorist-groomed-man-learning-difficulties-carry-Lee-Rigby-style-attack-British-soldier-jailed-eight-years.html.

[7] Bodetti, Austin. "The selfie jihadi: Inside al-Qaeda's Snapchat network." Alaraby, The New Arab, 19 Sept. 2017, www.alaraby.co.uk/english/indepth/2017/9/19/selfie-jihadi-inside-al-qaedas-snapchat-network.

[8] "Islamic State – Ashhād Foundation: "O Knights of Media, Descend for Combat with Allāh's Enemies and Fight with Them"." Bayt al-Maṣādir, 13 Oct. 2016, baytalmasadir.com/2016/10/12/text-pdf-islamic-state-ashhad-foundation-o-knights-of-media-descend-for-combat-with-allahs-enemies-and-fight-with-them/. (was made aware of the exitence of the Ashhād media manual via this article; located the actual source manual via the dark web).

P.3 to p.5 Karen Yourish, Derek Watkins And Tom Giratikanon. "Where ISIS Has Directed and Inspired Attacks Around the World." The New York Times, 17 June 2015, www.nytimes.com/interactive/2015/06/17/world/middleeast/map-isis-attacks-around-the-world.html (Information in this referenced were used to confirm assumptions about ISIS attack statistics but was not specifically referenced).

[9] "Global Internet Forum to Counter Terrorism." Twitter, Twitter Public Policy, 26 June 2017, blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html.

[10] Ricks, Thomas E. "Terrorists, video games and us." Foreign Policy, 16 Nov. 2015, foreignpolicy.com/2015/11/16/terrorists-video-games-and-us/.

[11] LeFebvre, Rob. "Theresa May wants to force tech giants to curb extremist content (Updated)." Engadget, 30 May 2017, www.engadget.com/2017/05/26/theresa-may-g7-extremist-content/.

[12] "BSA/AML Risk Assessment - OVerview." Online Manual - BSA InfoBase - FFIEC, Federal Financial Institutions Examinations Council, 2014, www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_005.htm.

[13] "Counter Terrorist Financing." OCC: Counter Terrorist Financing, 29 Dec. 2010, www.occ.treas.gov/topics/compliance-bsa/bsa/counter-terrorist-financing/index-counter-terrorist-financing.html.

[14] Dreyfuss, Emily. "This Is How Facebook Fights Extremists." Wired, Conde Nast, 16 June 2017, www.wired.com/story/facebook-counterterrorism/. Accessed 2 Oct. 2017. Facebook has acknowledged that it must continue to find ways to combat extremism on its platform and has engaged in deradicalization efforts.

[15] Lynch, Michael. "How device intelligence tech can help FIs comply with key FFIEC mobile security guidelines." Mobile Payments Today, 10 June 2016,

www.mobilepaymentstoday.com/articles/how-device-intelligence-tech-can-help-fis-comply-with-key-ffiec-mobile-security-guidelines/.

[16] Martin, Will. "One chart shows how little its costs terrorist groups like ISIS to carry out attacks in Europe." Business Insider, 2 Dec. 2016, www.businessinsider.com/how-much-do-terrorist-attacks-cost-deutsche-bank-2016-12.

[17] "Countering Online Radicalisation: A Strategy for Action." The International Centre for the Study of Online Radicalisation and Violence, 2009, doi:10.18411/d-2016-154.

[18] "Countering Islamic State Exploitation of the Internet." Council on Foreign Relations, Council on Foreign Relations, 18 July 2015, www.cfr.org/report/countering-islamic-state-exploitation-internet. Accessed 1 Sept. 2017.

[19] Gofstein, Bryan. "The New CTF: Reviewing Practical Tools to Counter Terrorism's Evolving Financing Methods." ACAMS 16th Annual Global and Financial Crime Conference, ACAMS, Las Vegas, Nevada, 26 Sept. 2017.

[22]Achterbosch, Leigh. "A taxonomy of griefer type by motivation in massively multiplayer online role-playing games." Taylor & Francis. March 29, 2017. http://www.tandfonline.com/doi/abs/10.1080/0144929X.2017.1306109?journalCode=tbit20. Volume 36, 2017 - Issue 8

[23] "Terrorist crews on GTA Online." Rockstar Support, 27 Apr. 2017, support.rockstargames.com/hc/en-us/community/posts/115006229927--p-Terrorist-crews-on-GTA-Online-p-. (the report of "terrorist" activity was from a Community Forum page for Rockstar Games' Grand Theft Auto game; that particular crew has since been removed from the online GTA game.)

[24] "Militants using gift cards to bankroll terrorism, intelligence agency says." The Guardian, Guardian News and Media, 1 May 2017, www.theguardian.com/australia-news/2017/may/02/militants-using-gift-cards-to-bankroll-terrorism-intelligence-agency-says.

[25] "Country Reports on Terrorism." U.S. Department of State, U.S. Department of State, 30 Apr. 2017, www.state.gov/j/ct/rls/crt/. Accessed 0ADAD.