ACAMS® | Advancing Financial Crime Professionals Worldwide

THE LEVERAGING OF SOCIAL MEDIA BY CORPORATE CREDIT UNIONS TO ENHANCE THE DETECTION AND REPORTING OF SUSPICIOUS ACTIVITY

Naomi B. Glass, CAMS

Table of Contents

Executive Summary

Corporate credit unions are presented with unique challenges with respect to the identification and reporting of suspicious activity to law enforcement. That is because they are in the business of processing transactions on behalf of individuals and businesses whose accounts they do not hold. Due to the lack transparency associated with the financial transactions that they process on behalf of third parties, corporate credit unions must identify alternate sources of intelligence to aid in their investigation of suspicious activity. That is where social media comes into play.

Social media sites such as Facebook, LinkedIn and Twitter can be utilized as an investigative tool to identify and vet individuals and businesses, determine connections between counterparties and discover criminal involvement. By leveraging social media as a resource tool in conducting anti-money laundering and terrorist financing investigations, the identification and reporting of suspicious activity by corporate credit unions is greatly enhanced. Ultimately, better reporting to law enforcement increases the likelihood of catching criminals and putting them behind bars.

Background

Corporate credit unions are wholesale financial institutions commonly referred to as the "credit unions for credit unions." Corporate credit unions do not provide financial services directly to individuals or businesses. Rather, they provide payment services to their members, natural person credit unions that serve various segments of the U.S. consumer population. Corporate credit unions are not-for-profit organizations that are federally regulated by the National Credit Union Administration (NCUA). Approximately a dozen corporate credit unions exist in the U.S. today.

Corporate credit unions serve an important industry function in that they provide natural person credit unions with financial services and liquidity. Products and services offered include short-term and long-term investments as well as financial settlement services through the clearing of check payments, ACH and wire transfers. Cash vault services are also available.

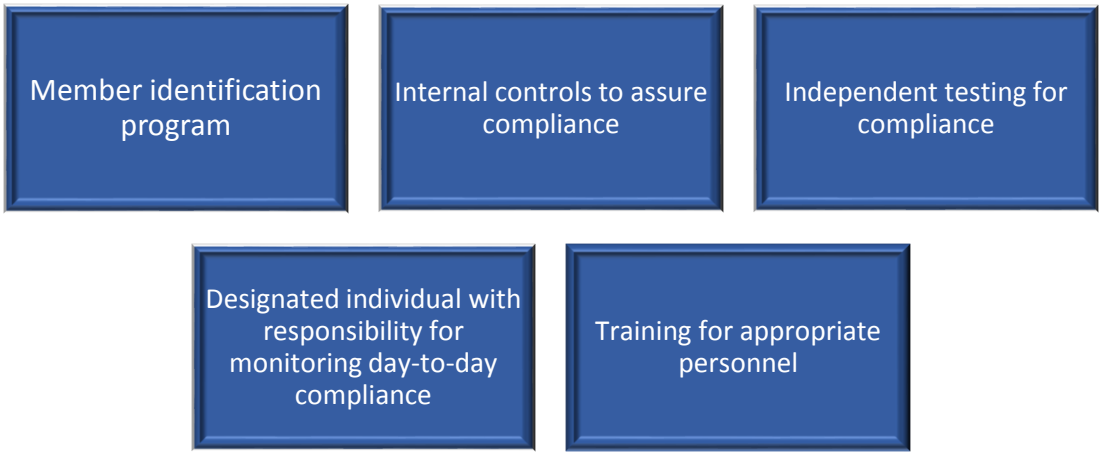
Corporate credit unions are at an increased risk of being exploited for money laundering and terrorist financing (ML/TF) purposes due to their business model. Corporate credit unions operate as correspondent financial institutions. Correspondent banking is defined by the Financial Action Task Force (2016) as, "The provision of banking services by one bank ("the correspondent bank") to another bank ('the respondent bank')." In the case of corporate credit unions, their respondents are the natural person credit unions that they serve.

Since corporate credit unions are utilized to process transactions on behalf of their member credit unions' members, information on these third parties is very limited. Consequently, corporate credit unions face unique challenges with respect to identifying and reporting suspicious activity to law enforcement. Doing so effectively is crucial to the mitigation of these ML/TF risks.

BSA Compliance Responsibilities

Compliance with the Bank Secrecy Act (BSA) and other anti-money laundering (AML) laws and regulations is fundamental to the effectiveness of a corporate credit union's AML program. Like retail financial institutions, corporate credit unions are "required to establish and maintain procedures reasonably designed to assure compliance with the Bank Secrecy Act and the Department of Treasury's implementing regulations."[1] In addition, corporate credit unions must have AML programs that meet the following basic requirements:[2]

[1] Title 31, Part 103 of the Code of Federal Regulations
[2] Section 748.2(b) of NCUA's Rules and Regulations



Moreover, it is a requirement that corporate credit unions have knowledge of the typical account activity that occurs in the accounts they maintain for their member credit unions and ensure appropriate monitoring and reporting of suspicious transactions within the accounts (NCUA 2004).

To verify that corporate credit unions are adequately meeting their BSA/AML regulatory obligations, annual examinations are conducted by the NCUA. Failure to implement and maintain sound AML programs can result in the levying of enforcement actions such as civil money penalties and cease-and-desist orders. Significant AML program deficiencies can also result criminal liability.

BSA Compliance Limitations

Corporate credit unions face a unique set of challenges with respect to BSA/AML compliance. Because corporate credit unions are correspondent financial institutions processing transactions on behalf of their member credit unions' members, there is a lack of visibility into the transactional activity taking place. Essentially, corporate credit unions are in the business of moving funds on behalf of third parties whom they know almost nothing about. Corporate credit unions are more vulnerable to exploitation by criminals because of this business model. It also makes the detection and reporting of suspicious activity by the corporate credit unions' BSA/AML staff significantly more challenging.

Corporate credit unions are at a distinct disadvantage when it comes to monitoring transactions for unusual or suspicious activity. This is due to several reasons. First, corporate credit unions process almost all transactions in settlement batches. This means that transactions are bundled together in such a way that the individual transactions are not identifiable to the corporate credit union. It is almost impossible for BSA/AML staff to detect and report suspicious activity without visibility into the specific transactions taking place.

Fortunately, domestic and international wire transfers are processed individually and are therefore not batched. While this provides corporate credit unions with increased visibility into the transactional activity being facilitated, corporate credit unions can be at the mercy of their member credit unions to provide specific details related to the wire transfer and its related parties (i.e. originator/beneficiary names and addresses, account numbers and purpose of payment information).

BSA/AML staff struggle to conduct thorough investigations of wire transfer activity when pertinent details of this nature are unavailable. This can be problematic. Money launderers are primarily interested in facilitating the swift and anonymous movement of funds across international lines (S. Rep. No. 107-1, 2000). Correspondent banking is an important means of facilitating cross-border movements of funds (S. Rep. No. 107-1, 2000).

Secondly, corporate credit unions are at a distinct disadvantage when it comes to identifying and reporting suspicious activity because they process wire transactions on behalf of third parties whose accounts they do not hold. Consequently, corporate credit unions lack access to the following key pieces of information that can be of significant value to law enforcement:

Due to the lack transparency associated with the transactions corporate credit unions process on behalf of its member credit unions' members, BSA/AML staff must identify alternate sources of information to aid in its investigation of suspicious activity. One method of acquiring intelligence is through the leveraging of social media as an investigative resource.

Definition of Social Media

There is not one universally agreed upon definition of social media because it is constantly changing and evolving with advancements in technology. One definition that merits consideration from a compliance perspective is that of the Federal Financial Institutions Examination Council (FFIEC). The FFIEC is a U.S. government interagency body that was established in 1979 to promote uniformity in the way financial institutions are supervised by the various regulatory agencies. Its members include the NCUA, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Consumer Financial Protection Bureau and the State Liaison Committee. The FFIEC defines social media as follows:

Social media is a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. Social media can take many forms, including, but not limited to, micro-blogging sites (e.g., Facebook, Google Plus, MySpace, and Twitter); forums, blogs, customer review web sites and bulletin boards (e.g., Yelp); photo and video sites (e.g., Flickr and YouTube); sites that enable professional networking (e.g., LinkedIn); virtual worlds (e.g., Second Life); and social games (e.g., FarmVille and CityVille). Social media can be distinguished from other online media in that the communication tends to be more interactive…Messages sent via email or text message, standing alone, do not constitute social media.

A second definition of social media worthy of consideration is derived from the scholarly works of Boyd and Ellison (2007) who stated that social networking sites are web-based services that allow individuals to:

1. Construct a public or semi-public profile within a bounded system;

2. Articulate a list of other users with whom they share a connection; and

3. View and traverse their list of connections and those made by others within the system.

Brunty and Helenek (2015) further expanded upon that definition by stating that a social medium:

4. Encourages its users to communicate with other users who are a part of that network and/or the site creators themselves; and

5. Creates an environment for users to share content and/or connect through their similar interests.

Popular Social Media Platforms

Hundreds of social media and social networking sites exist on the internet and new sites are being launched every day. A corporate credit union's BSA/AML staff cannot spend countless hours researching counterparties across all social media platforms. Targeting the most popular social media sites is a more effective and efficient method of gathering information as part of the investigative review process. The three most popular social networking sites today are Facebook, LinkedIn and Twitter. Below is a brief description of each:

Facebook

Facebook is a social networking site that allows users to share personal information and stay connected to friends and family. On average, Facebook has 1.32 billion daily active users. Facebook users create profiles which contain profile pictures, contact information, photographs and details related to education, interests and hobbies. Facebook users can also chat with other users, create and join groups, post messages and upload videos, among numerous other features (Facebook.com, 2017).

LinkedIn

LinkedIn is a social networking site that is geared towards professionals. Per its corporate website, LinkedIn is the largest professional network on the internet with more than 500 million members in over 200 countries and territories. The site is used by individuals to display job

histories and qualifications, post articles, join online professional groups and find and apply for jobs (LinkedIn.com, 2017).

Twitter

Twitter is a social networking site that allows users to post information in real time. Members can post "tweets" which are limited to 140 characters in length. Users can connect to the latest news, stories, ideas and opinions. Twitter has 328 million monthly active users (Twitter.com, 2017).

Leveraging Social Media to Identify and Report Suspicious Activity

Social media can be leveraged as an investigative tool in the identification and reporting of potentially suspicious activity to law enforcement. This is not a new concept. In fact, the practice of conducting social media checks by AML departments across the financial services industry has been around for years. Utilizing social media as an investigative resource is crucial for corporate credit unions, however. Why? Because they are in the business of processing payments on behalf of third parties whose records they do not house and whose accounts they do not maintain.

Corporate credit unions are reliant on obtaining intelligence about counterparties through social media as it helps put the pieces of the puzzle together in determining whether transactional activity is suspicious or not. This ultimately results in better case decisioning as well as the filing of more informed suspicious activity reports (SARs) which is of greater benefit to law enforcement.

Corporate credit unions can leverage social media as an investigative tool by utilizing Facebook, LinkedIn and Twitter to identify and vet individuals and businesses, determine connections between counterparties and discover criminal involvement.

Facebook can be used to identify relevant personal information about a counterparty such as age, date of birth, location and occupation. This enables BSA/AML staff to form a basic framework regarding the individual they are researching. Adding personal details of this nature can also

INVESTIGATIVE TIP

BSA/AML staff need to "know their source" when obtaining information from social media. Information retrieved from social media may not be accurate or reliable. User-created content should always be taken with a grain of salt since it is easy for suspects to create social media pages and profiles for fictitious individuals and businesses.

Red flags to be on the lookout for:

* User content is not consistent across the various social media platforms.

* Information retrieved from social media conflicts with public records (i.e. Secretary of State business registration).

be useful for filing out SAR forms which would otherwise contain multiple blank subject fields due to lack of personal information.

LinkedIn can be used to identify an individual's job and employment history. This information can be extremely useful as BSA/AML staff attempt to ascertain whether the transactional activity under review could be related to the individual's line of work, or business in the case of business ownership. It is also helpful because BSA/AML staff can attempt to determine whether the transactions being conducted are within the financial means of the individual under review or whether the transactions appear atypical given the counterparty's employment background. For instance, BSA/AML staff would certainly question whether it makes reasonable sense for a counterparty with a low-income job to be wiring thousands of dollars to an unverifiable entity overseas. Knowing a counterparty's occupation can help resolve cases if the transactional activity appears plausible for that individual. BSA/AML staff are reliant on determining a counterparty's occupation considering they do not have access to view that individual's source or use of funds within their credit union account.

BSA/AML staff can also utilize social media to assist in validating the existence and legitimacy of business entities. Many businesses maintain an active presence on social media. BSA/AML staff can check to see if a business entity under review has a Facebook profile and/or Twitter account, and if so, whether the profiles contain contact information, pictures, customer reviews, etc.

A review of a counterparty's Facebook "friends" or LinkedIn "connections" can reveal personal, familial or business ties between counterparties. Understanding the relationship between counterparties can help shed light on the nature and purpose for the wires and whether the activity makes sense given the connection between the parties. For instance, if BSA/AML staff can determine that wires are originating from a parent in another state to a college student with a different surname, they can ultimately move forward with closing the case assuming the dollar amounts and frequency of the wires also make sense for providing financial support.

BSA/AML staff's review of pictures, videos and postings on Twitter or Facebook can reveal potential criminal behavior or nefarious activity perpetrated by, or associated with, a counterparty. Criminals can publicize their involvement in illegal activity on social media unintentionally or by design. The term "performance crime" has been coined to describe the latter. This is a relatively new phenomenon that occurs when individuals boast about their criminal behavior to their friends and followers through social media (Surette 2015). Ultimately, identifying illegal activity through social media and reporting it in a

INVESTIGATIVE TIP

Not all criminal activity is created equal. When conducting investigations, BSA/AML staff should be on the lookout for criminal information that is material. In other words, activity that may be indicative of money laundering, terrorist financing, fraud or other financial crimes. Lessor offenses such as parking infractions, DUIs or disorderly conduct charges may not be relevant as it pertains to the investigation.

SAR can aid law enforcement in its efforts to investigate and combat drug trafficking, human smuggling, money laundering and fraud.

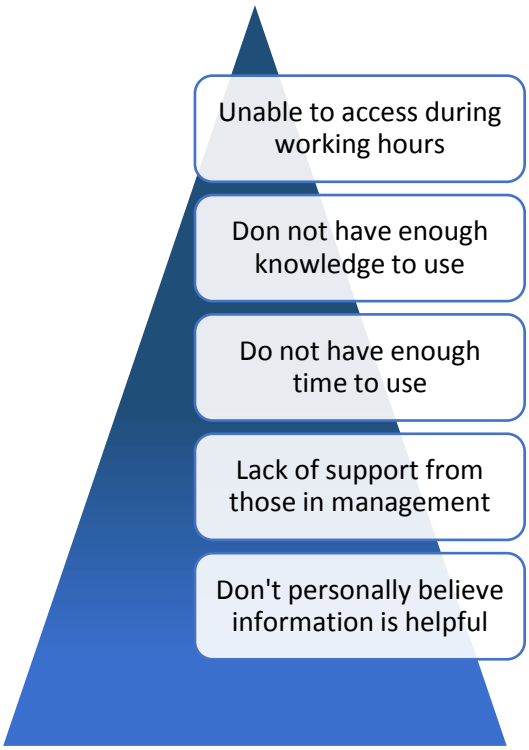
There are several additional forms of social media that BSA/AML staff can leverage in conducting counterparty research aside from popular social networking sites like Facebook, LinkedIn and Twitter. They consist of forums, blogs and bulletin boards, particularly those contained on public or government websites warning of fraud schemes and scams (i.e. consumer.ftc.gov, ripoffreport.com, 419eater.com)

Websites that alert the public to fraud schemes and scams typically include a comments section or bulletin board where victims can post messages to communicate with each other and share their experiences. Posts will include specific details related to the scam or scheme, including the names, addresses, even bank account numbers, of the parties allegedly involved in carrying out the crime. If BSA/AML staff perform a Google search of a counterparty's name or address, it could appear within one of the victims' posts thereby strengthening the argument that the counterparty is somehow involved in fraudulent or illegal activity. Reporting this finding within a SAR can be of great benefit to law enforcement as it could be the missing piece of the puzzle that inevitably leads to the dismantling of a much larger fraud ring or criminal enterprise.

Reasons for Non-Use of Social Media

Despite the obvious benefits associated with leveraging social media as an investigative resource tool, there are a multitude of reasons for its non-use.

One of the primary reasons is due to BSA/AML staff's inability to view social media at work. This restriction is not uncommon in today's workplace. In fact, 36% of employers actively block access to social media sites (Proskauer Rose LLP 2014). Employers cite concerns over misuse by employees, lack of available network bandwidth and cybersecurity risks as being the predominant factors in choosing to restrict employees' access. In the case of the latter, employers are fearful that granting employee access to social media could inevitably result in bringing viruses and Trojan horses inside the network. It could also increase the risk of hackers being able to infiltrate the company's IT infrastructure if vulnerabilities are detected and then exploited by cyber criminals.



Even when social media access is granted to BSA/AML staff, many choose not to use it as an investigative resource due to lack of knowledge of

how to effectively do so. Corporate credit unions do not spend the time or money training BSA/AML staff on how to incorporate social media checks into their investigative process. This causes BSA/AML staff to have to "wing it" which can be a deterrent to those with little personal experience utilizing social media. This ultimately results in inconsistent application by AML/BSA staff throughout the institution.

A third reason for non-use of social media in investigations is due to lack of time. As previously indicated, BSA/AML staff cannot spend countless hours researching counterparties on social media (as much as they would love to!). Their burgeoning caseloads simply won't allow it. Along these same lines, management might not support its use if it causes a slowdown in production. This could ultimately put the organization at risk of not meeting its SAR filing obligations in accordance with regulatory prescribed time frames.

Finally, some BSA/AML staff fail to leverage social media because they do not find the information useful. This could be due to concerns that the information gathered is not accurate or reliable.

Technology-Based Solutions for Social Media Searches

Searching various social media platforms to gather intelligence related to counterparties can be quite tedious and cumbersome. As previously mentioned, BSA/AML staff may be refraining from incorporating it into their investigative process due to lack of knowledge of how to use it effectively and lack of time to be able to use it efficiently. Recent advancements in technology, however, may be able to change that… for a hefty price.

What is this miracle technology? Vendor software now exists that offers a social media search function that BSA/AML staff can leverage when conducting counterparty research. While this type of technology was previously only available to law enforcement, one vendor, LexisNexis, has rolled out a similar version that can be used in conjunction with its other subscription-based intelligence gathering platforms.

LexisNexis claims that with one search, its Social Media Locator scans hundreds of social networking sites and millions of websites, including the deep web[3], to uncover information on individuals and any businesses or organizations with which they may be associated. A small sample of the hundreds of websites that are queried are reflected below:

[3] The Deep Web contains websites that are not indexed and therefore cannot be accessed through conventional web browsers (Google, Yahoo, Bing). They are only accessible with the exact URL and permission to visit the site.

Amazon	Doof	LivingSocial	Posterous	Tumblr
Ancestry	eBay	Los Angeles Times Blogs	Pownce	Twimg
Android Forums	eHarmony	Manta	Profilactic	TwitPic
Ars Technica	eHow	MapleStory	Qik	Twitter
Auto Trader	Engadget	Mashable	QQ Tencent	TypePad
AutoBlog	Epinions	Match	Real Fairies	Urban Dictionary
Backpage	Etsy	Media Bistro	Realtor	USA Today
Battle.Net	Examiner	MeetUp	Reddit	UStream
Bit.ly	Ezine Articles	MegaVideo	Refnery29	Verdict Search
Black Planet	Facebook	Merchant Circle	Reuters	Vimeo

Search results are reflected within the Results Summary (see screenshot below). The summary shows the count of results by category and the boxes next to each category can be checked so that only those results are displayed in the list. The results list links directly to the social media posting or website.

The major drawback associated with utilizing LexisNexis's Social Media Locator is the excessive cost. At $4 per search, corporate credit unions do not have the funds in the budget to be able to support widespread utilization of this feature by their BSA/AML staff. Management might even scoff at the price since searching social media the "good old-fashioned" way is completely free.

Social Media Use Policies & Procedures

Because corporate credit unions generally lack formal policies and procedures related to the utilization of social media for investigating suspicious ML/TF activity, they are at risk of falling behind the times. It would therefore behoove corporate credit unions to develop and adopt social media use policies and procedures that provide BSA/AML staff with a clear framework and understanding as to its permissibility and proper usage.

There are many factors that management will need take into consideration when developing formal social media use policies and procedures, some of which are as follows:

- Should BSA/AML staff be permitted to utilize their own personal devices to conduct social media research if their access at work is restricted?

- Should BSA/AML staff be utilizing their own personal social media accounts to conduct research? If so, are there certain privacy settings that must be put into effect first to

ensure searches are conducted anonymously? Failing to conduct searches anonymously could result in "tipping off" criminals to the fact that they are under investigation.

- Should BSA/AML staff be creating fictitious social media profiles to utilize for investigative purposes? What type of content is permitted, or not permitted, to be included on a fictitious profile?

Ultimately, it is up to the corporate credit union to determine which policies and procedures best align with the needs and risk tolerance of the organization.

Conclusion

Like retail financial institutions, corporate credit unions are tasked with ensuring compliance with respect to all BSA/AML laws and regulations. The importance of protecting the U.S. financial system from being utilized by money launderers, terrorist financers and other criminals cannot be overstated. Corporate credit unions, however, are at a disadvantage in that they are required to investigate and report any and all suspicious transactions that are flowing through their institutions. These are transactions conducted on behalf of their member credit unions' members, third parties whose accounts the corporate credit unions do not hold. This business model is known as correspondent banking.

Because corporate credit unions have extremely limited information on these third parties, they are reliant on obtaining intelligence about them through other investigative channels. One of the most useful sources of information is social media. Popular social media platforms, such as Facebook, LinkedIn and Twitter, contain an abundance of publicly available information about counterparties. This can include important details related to their identities, employment histories, even personal and business ties. It could also reveal possible criminal or nefarious activities. When BSA/AML staff can gather this type of intelligence, it strengthens their ability to ascertain whether the transactions under review are suspicious or not.

By leveraging social media as a resource tool in conducting ML/TF investigations, the identification and reporting of suspicious activity by corporate credit unions is greatly enhanced. Ultimately, better reporting enables law enforcement to become more effective in its pursuit of criminals.

References

"About Twitter". Twitter, Inc., 2017. Retrieved October 2, 2017 from https://about.twitter.com/en_us/company.html

Boyd, D. and Ellison, N (2007). Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication,* 13 (1), 210-230. http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full

Brunty, J. and Helenek, K. Social Media Investigation for Law Enforcement. New York; Routledge, 2015.

"*Facebook.com Company Info".* Facebook. 2017. Retrieved October 2, 2017 from https://newsroom.fb.com/company-info/

FATF (2016), *Guidance on correspondent banking services*, FATF, Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/correspondent-banking-services.html

"LinkedIn - About". LinkedIn Corporation. 2017. Retrieved October 2, 2017 from https://press.linkedin.com/about-linkedin?#

Lynn-Nelson, G (2016). *Social Media Locator*. LexisNexis® InfoPro Community. https://www.lexisnexis.com/infopro/literature-reference/librarian-relations-consultant-research/b/researchtip/archive/2016/03/10/social-media-locator.aspx

NCUA (2004), *Corporate Credit Union Guidance Letter on Bank Secrecy Act (BSA) Compliance*, (No. 2004-02). https://www.ncua.gov/Resources/Documents/LCCU/LCCU2004-02.pdf

Social Media: Consumer Compliance Risk Management Guidance, Federal Financial Institutions Examination Council (December 11, 2013). https://www.ffiec.gov/press/PDF/2013_Dec%20Final%20SMG%20attached%20to%2011Dec13%20press%20release.pdf

Social Media in the Workplace Around the World 3.0. 2014. Proskauer Rose LLP.

Surette, R. "Performance Crime and Justice" [2015] CICrimJust 21; (2015) 27(2) Current Issues in Criminal Justice 195.

U.S. Senate. Committee on Governmental Affairs. *Minority Staff of the Permanent Subcommittee on Investigations Report on Correspondent Banking: A Gateway for Money Laundering.* (107 S. Rpt. 107-1). Washington: GPO, 2000. Print.