The Bill Blackwood
Law Enforcement Management Institute of Texas

The Call For A Collaborative Approach To Identity Fraud Through The Use Of New Offense-Specific Fusion Centers

---

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Adam Jones

University of Texas Southwestern Medical Center Police Department
Dallas, Texas
February 2015

ABSTRACT

Identity fraud is going to become a pandemic if not addressed with innovative methods designed to mitigate the threats early on as well as to allow for the collaborative effort from the many organizations involved in cleanup process. The Bureau of Justice Statistics published an alarming study that stated that as many as 17 million Americans have been victims of identity fraud in 2012 at a national cost of $25 billion while the cost of all other property-related crimes totaled just $14 billion (Harrell & Langton, 2013). Offense specific fusion centers, which transcend the traditional law enforcement shroud and encompass the private industry, should be created and implemented to fully address the issues surrounding identity fraud and the risks associated with such offenses. In doing so, the costs associated with the victimization can be mitigated or eliminated thus passing on those savings to the general public through reduced private industry costs.

Current estimates show that $0.05 of every dollar spent by U.S. consumers is directly related to fraud (Newman, 2002). Another benefit are the reduced costs for those assigned to investigate these offenses which may include law enforcement; local and federal government; and the private industry. Often, the efforts at the various levels of government are not harmonious and thus the sharing of vital information may not be passed along to those agencies that may be in a position to stop the threat. There is rising sentiment to the overuse of government oversight, which then lends itself to the possibility of overspending, both of which can be overcome through proper monitoring protocols. Thus, real-time crime-specific sharing apparatuses must be used to counter this growing threat before it endangers the global economy.

TABLE OF CONTENTS

INTRODUCTION

As crime evolves in the twenty-first century, law enforcement and the private sector must ensure that they are, at the very least, matching that evolution in order to avoid being passed by those who intend to upset the balance as it currently sits. As law enforcement continually seeks ways to spur innovation, one common theme is to call for the building of a robust system for the sharing of real-time intelligence information as a way to combat the ever-growing problem presented by identity fraud offenses. The Bureau of Justice Statistics published an alarming study that stated that as many as 17 million Americans, 7% of the working age citizens, have been victims of identity fraud in 2012 at a national cost of $25 billion while the cost of all other property-related crimes totaled just $14 billion (Harrell & Langton, 2013). As these offenses present newer large-scale attacks, it becomes increasingly critical to have a system that can immediately share relevant and time-sensitive information between varying levels of law enforcement and their partners in the private sector, namely the banking industry.

Identity fraud offenses are relegated to a specific set of offenses in which one or more culprits use the personal information of another, without that person's consent, in a manner which brings harm to the victim (Texas Penal Code Title 7, 2014). While each state has varying terms and penalties related to these offenses, at their core, they all relate to the unauthorized taking of someone else's private information for personal gain. McNally and Newman (2005) defined identity theft through Congress' Identity Theft Assumption and Deterrence Act of 1998 as anyone who "knowingly transfers or uses, without lawful authority, any name or number to identify a specific individual with the intent to commit any unlawful activity that constitutes a felony under any applicable

State or local law" (p. 1). Identity fraud can often be wrongly misconstrued to be only the unauthorized taking of someone's personal information, such as social security number for the sole reason of taking over someone else's identity. While this is certainly a type of identity fraud, one must not forget the greater occurrence of offenses such as credit or debit card and check fraud. For the purposes of this paper, identity fraud offenses are taken to mean those offenses which fall under Texas' Penal Code Title 7, Chapter 32 Fraud.

Fusion centers are an interesting concept that only recently have taken shape and begun to hit their stride in obtaining their objectives as laid out by the Departments of Justice and Homeland Security in mitigating a broad spectrum of threats. The U.S. Department of Justice defines a fusion center as “a collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity" (U.S. Department of Justice, 2008, p. 47). Fusion centers are, in essence, a centrally-located collaborative center for various officials to provide analytical data and research on a variety of topics to those in the field and those at a senior command level for strategic-level planning. Currently, there are 53 primary fusion centers spread across the country and 25 recognized fusion centers. Each of these fusion centers carry different responsibilities to those whom they serve but all are centrally dictated to carry about similar functions and all are regulated by local, state, and federal laws and regulations. Primary fusion centers receive the greatest funding and allocation of federal resources to include personnel while recognized fusion centers

are those centers not sponsored by federal funding, who are instead designated by their representative state decrees (U.S. Department of Homeland Security, 2014).

Identity fraud cannot be allowed to continually seep through the cracks of society to erode and shake the foundation of trust built in the very system it espouses to destroy. Thus, the problem must be addressed head-on, in a manner that gives it the credence and attention it deserves. Multi-jurisdictional, representing various levels of law enforcement and a broad spectrum of private industry, identity fraud-related fusion centers should be created and implemented to combat the rising trend in identity theft. Effectively tackling identity theft calls for the coordinated effort amongst law enforcement and the private sector using a shared intelligence model such as fusion centers as a way to jointly attack the problem and eliminate on-going threats. The elimination of identity fraud greatly benefits the public, law enforcement, and the private sector to such a decree as the elimination of prohibition represented to the same parties in the 1920s through the reduction of crime costing the U.S. taxpayers millions of dollars annually.

POSITION

With the tragic consequences of the attacks of September 11th, the federal government mandated the reassessment of the intelligence process as a way to potentially mitigate future attacks on United States. One of the major failures discovered came through the failure to adequately share information across broad spectrums of industry to include the various levels of law enforcement and the private sector, specifically the banking industry. In creating local and state fusion centers across the

country, the benefits across the broad spectrum of people and entities will shake the very foundation of the identity theft crisis.

The overwhelming victimization of those affected by identity theft related offenses occurs to the public. There is not a single state in the United States that does not feel the effects of identity theft in some form which results in countless hours lost as people attempt to pick up the pieces of their shattered lives. Not only are people victimized through the initial offense but are again victimized while going through the very system put in place to help either catch the offenders or those put in place to offer the assistance needed afterwards. In typical identity theft offenses, victims experience an initial loss, either of their personal information or perhaps a credit card, which is compromised once, used once, and then is never used again. This would be considered a classic identity theft and one that presents the victim with the least amount of emotional scaring. On average, the typical identity fraud victim incurs a financial burden, associated to the misuse of their information and any mitigation efforts, of approximately $500 per incident (Finklea, 2014). This figure does not calculate the effects of work time missed nor the potential ongoing cost if they are repeatedly victimized.

The most common example of identity fraud is credit and debit card fraud as reported between the years 2000 and 2008 (Federal Trade Commission, 2012). With a staggering cost of approximately $25 billion in lost revenues to corporate entities, those costs are passed on to consumers as increased costs of doing business. Much the same as costs of shoplifting are passed on to consumers as wastage, this push-back cost can be lowered as incidents of identity fraud are reduced or outright eliminated.

Along these same lines, the costs that are absorbed by law enforcement agencies, is staggering due to the labor intensive investigations that are often required to solve these offenses. As is typically seen, credit card frauds involve several separate criminal episodes that must each, in their own unique way, must be solved in order to lead back to the culprit. There is usually an initial theft or compromise of the credit card number that must be first identified and investigated because the initial thief may not be the later culprit who uses that stolen credit card information.

A current issue affecting all the states lining the Gulf of Mexico and the East Coast are the thieves known as the "Felony Lane Gang" who are known for smashing the windows of unsuspecting mothers as they drop off their children at their daycare centers (Cops, 2014). These "gang" members then either pass off those stolen credit cards or simply take them to local establishments to make illegal purchases using those stolen credit cards. They are also using stolen checking information and attempting, often successfully, to make fraudulent withdrawals from the victim's banking institutions using the outer-most lane, often referred to as the felony lane, making it hard for the Bank's teller to compare identities between the individual driving and the stolen identity from a stolen driver's license. Successful prosecutions are being seen across the country as investigators, from both the private sector and law enforcement, are learning to share information in near real-time through intelligence centers such as fusion centers and other federally sponsored intelligence-sharing platforms (Bureau of Justice Assistance, 2012).

According to a review conducted by McNally and Newman, "The FBI estimated the average cost of an investigation... to be $20,000 between 1998 and 2000. Further,

many cases handled by these agencies do not involve elements of identity theft, which may require considerably more resources to investigate" (McNally & Newman, 2005, p. 33). The very concept of a fusion center is to reduce redundancy and bring about more efficient use of investigators time by having all the involved knowledge bases brought into a joint environment ensuring better collaboration. Considerable time is wasted in investigations, duplicating work that has either been done by another law enforcement agency or by an investigator in the private sector who is tasked with identifying breaches to their corporate information. If these costs are reduced through better collaboration, that cost savings can either be reinvested into the agency, such as more officers who can be directed at other crime sectors, or it can be passed back to the public as reduced operating costs.

Identity fraud offenses tend to spread themselves out across multiple jurisdictions, especially in larger metropolitan areas such as Houston, Dallas, or San Antonio where multiple jurisdictions often overlap or have flowing boundaries that do not follow clearly identified lines of demarcation. In reviewing the Felony Lane Gang, it is seen that the criminals will often roam city to city in search of easy victims and thus their offenses should be looked at as a criminal spree versus a one-time offense. With this change in thought, the use of a real-time intelligence sharing apparatus could easily link these offenses and divvy out investigative responsibilities to better maximize the resources involved. This also has the benefit of allowing investigators to link their offenses to other on-going offenses which in turn increases the odds of a successful prosecution. Oftentimes, investigators are unaware of other on-going investigations that have or could have a major impact on their cases to include other agencies that have

prosecuted the same individuals sought by other agencies. If information could be freely shared, there would be no need to spend countless hours wasting investigative resources in the attempt to identify criminals who have already been identified and prosecuted by other agencies.

Fusion centers have become synonymous with counter-terrorism and drug interdiction efforts. This train of thought has effectively limited the abilities of these fusion centers to these responsibilities but in its narrow-minded focus, other uses have been cast aside. In changing the mindset about how to effectively utilize fusion centers, important and costly crimes can be greatly reduced or eliminated completely when brought to the forefront of these mighty crime fighting entities. As patrol officers are called to the scene of a possible crime involving any fraud-related offense, those officers can, in real-time, relay information back to a fusion center to be quickly analyzed and that information relayed back to the officer to assist them in their investigation. When utilized in this way, officers are better able to link a criminal predicate which in turn raises the solvability rate of those offenses. According to Johnson, with the Rio Vista Police Department, it is important that patrol officers and other initial responders have a clear understanding of solvability factors as this information is crucial to successful follow-up investigations or there runs a risk of cases not being assigned due to the lack of solvability factors (Johnson, 1998). Therefore, if the initial investigating officer can utilize real-time information to correctly annotate on their offense report, there is a higher likelihood of a successful follow-up investigation when the case is turned over to the Investigations Division. This is a more efficient use

of the investigator's time as they do not have to duplicate work that could or should have been done by the initial investigating officer, had that information been readily available.

The use of fusion centers as they relate to identity fraud-related offenses can utilize near real-time information to reduce costs incurred by the citizens, the private sector, and the government in the form of investigative resources. Victims no longer have to endure being re-victimized by the very system set in place to protect them due to the lack of intelligence sharing protocols and as such, large crime sprees can be quickly investigated and possibly solved when information is freely shared.

COUNTER POSITION

Law enforcement agencies typically do not 'play nice' with other agencies especially in terms of sharing information or intelligence. The thought of sharing information is a relatively new concept as the failures of the pre-9/11 environment showed in that if information is freely shared at near real-time, threats can be quickly identified and possibly mitigated. There is a concern for privacy rights and dissemination rights, which is a legitimate concern (Bain, 2008). In their book, *Police and Government Relations: Who's Calling the Shots?,* Beare and Murray expounded upon this further by adding that an agency's ego is usually to blame for poor information sharing in that an agency may hold onto information as a source of power (Beare & Murray, 2007). Fusion centers are the antithesis of the old adage of hording information for the holding agency to gain power and influence as a means of doing business. As has been seen post 9/11, information sharing has a greater good associated with it than the need to withhold that information for the agencies own uses.

Not everyone welcomes the use of these intelligence sharing capabilities as seen by a 2005 statement from the American Civil Liberties Union (ACLU) where they laid out reasons for their concern to civil rights: “The establishment of a single source intelligence center raises important issues concerning the scope of its operations and need for safeguards to ensure that its operation do not violate civil liberties or intrude on personal privacy” (American Civil Liberties Union, 2005, para. 2). Civil rights violations are an unfortunate aspect that is continually dealt with in law enforcement but there are relatively easy ways to counteract these concerns through the use of transparency, adequate policies and procedures, and government oversight such as that which is used to govern intelligence sharing databases, 28 Code of Federal Regulations Part 23 (28 CFR Part 23).

The greatest concern in regards to implementing the use of fusion centers as they relate to identity fraud-related offenses is the initial cost and high operating costs. In a biting 141 page report, the Senate's permanent subcommittee on Homeland Security and Governmental Affairs identified significant areas of wasteful spending with inadequate oversight in their spending practices (Committee on Homeland Security and Governmental Affairs, 2012, p. 61). They further went on to state that in order to assess the success of any program, one must know how much has been invested to show the return on investment but the Department of Homeland Security (DHS) has been unable to identify what returns, if any, they have received from the outpouring of public funds. To counteract this outpouring of public funds into a controversial area, it can be argued that the use of private-sector funds and fees related to court costs and fees should take a higher initiative. The Bill Blackwood Law Enforcement Management Institute of

Texas (LEMIT) is an example of a successful program that uses court fees assessed on criminal offenses to fully support the program which is a nationally recognized law enforcement leadership programs that prepares officers for roles in command-level leadership positions by affording them an academic background in leadership theory and applicability (Oakley, 1997). As the private-sector sees a cost-benefit to the investment in such centers, the monetary support should follow. Another source of revenue that could alleviate the burden on public funds could come from funds seized from criminals after their successful prosecutions which helps eliminate any wrongful seizures that occur prior to prosecution thereby adding in an additional checks and balances factor through the use of a third party, the court in this instance, that ensures any seizure funds used are those that have been deemed illicitly gained proceeds.

RECOMMENDATION

Real-time intelligence and investigative-lead sharing apparatuses should be implemented to address the issue of identity fraud using the resources of both law enforcement and the private sector. The current law enforcement culture already supports the use of fusion centers as a reactionary and, hopefully, a proactive approach to crime solving. A shift in mindset should happen between law enforcement and the private-sector, namely the banking industry, to allow for a collaborative approach to this fastest rising criminal sector.

In using the cross-industry fusion center approach to solving criminal activity, a collaborative approach will be used to a degree that has not been done before. Typically, financial industries utilize their own investigative resources to mitigate losses to their bottom-line but those same resources can be a valuable resource to law

enforcement whose objective is not too different than their private-sector counterparts. This then results in a benefit to all involved, from the victim to the law enforcement investigators and finally to the State. Additionally, the banking industry could reap the rewards in terms of millions of dollars saved to either be passed back to the consumer or into the very program for which they can thank for that savings. There are estimates that $0.05 of every dollar spent was in some way related to fraud and that amount roughly translates to over a billion dollars in the U.S (Newman, 2002). The benefits are mainly in monetary terms due to the high amount of monetary investment from each of those end users but those effects can also be felt through the increased efficiency seen across all industries as these offenses are cleaned up or eliminated.

This approach will not be taken so lightly by the public who already heavily distrusts the banking industry and, at best, has contempt for law enforcement. In this day in age where the various intelligence apparatuses have been caught with their pants down while snooping on the very citizens they proclaim to protect, the addition of another intelligence gathering, sharing, and analyzing think-tank may push those sentiments to the breaking point. This line of thought can be overcome through the fusion center having both governmental and private oversight through use of strict policy and procedures set in place so that the information gained, used, analyzed, and distributed meets the strictest possible guidelines to protect the general public. The banking industry already has set in place some of the strictest consumer protections already in place and so does the current fusion center through use of the Code of Federal Regulations. Another way to circumvent this issue is to have the public understand that law enforcement will not have access to sensitive banking databases

and vice versa so as to keep each system's integrity in place. Instead, those investigators from both industries will simply be housed in the same location to allow for quicker, real-time information to be passed back and forth in order to capture streams of seemly unrelated data and process them together to have a better understanding of the whole picture instead of just having the 'slice of the pie' dealt to them by their proximity to either the offense or the victim. In the State of Texas, victims of fraud, especially those involving credit card offenses, have the ability to report offenses to either the agency where they live, where the initial theft or breach of the credit card's information occurred, or where the card was fraudulently used (Texas Code of Criminal Procedure, 2014). Using this approach, while convenient for the victim, ensures that those agencies involved may never be able to link the various offenses and victims that may be connected due to great distances and unfamiliarity between agencies.

The Federal Bureau of Investigation (FBI) has already established an intelligence sharing program, InfraGard, similar in nature but dealing strictly with the protection of infrastructure. This program has been around since 1996 but even though this program has enjoyed great success, it too is not immune from the perception of malfeasance. A 2004 report from the ACLU stated "there is evidence that InfraGard may be closer to a corporate TIPS program, turning private-sector corporations - some of which may be in the position to observe the activities of millions of individual customers - into surrogate eyes and ears for the FBI" (Stanley, 2004, p.12). Some 18 years later, there have been no reports to substantiate this line of thought or any reports of malfeasance. InfraGard also deals with the protection of infrastructure from terrorist attacks but does not concern itself with issues that can be directly understood through the burden placed

upon the public in terms of losses to businesses which are then put on the backs of their customers.

Lastly, the issue that stands the greatest chance of dooming this concept is the issue of cost or funding. Understandably, there will be a large upfront cost to establish these centers across the U.S. in terms of infrastructure, network capabilities, data storage, and personnel but these costs can be offset in a myriad of ways to include the use of monetary seizures, dedicated funding through the court system, and federal and state grants or some combination of the three. In a two year span, 2001-2002, Texas received over $22 million in seized property and in 2006, $33 million of actual currency was seized (Williams, Holcomb, & Kovandzic, 2010). Fusion centers would be expected to cost millions each year to operate and these costs can easily be offset through the proper restructuring of current procedures nation-wide so as to capture minor amounts from each seizure across the country which would result in millions of dollars available for expenditures. Another example would be to use the court systems to help offset some of the costs by imposing minor fees, such as the LEMIT program has already in place, on each criminal court proceeding. This would require that legislation be passed in each state's legislature but again, with a little education to the public in terms of cost-savings, this issue should have relatively easy success passing into law. Finally, there is the need to gather financial support from the private-sector which may be a little more difficult. Businesses must rely on the bottom dollar for any decisions they make and the benefits may not be immediately apparent to those corporations until success is seen through the reduction of fraud. This type of success is not easily quantifiable and may have to have a period of 'watch and see' imposed

upon the centers as a measure of success. Corporations can shift their operations for these types of endeavors over to the fusion centers but those shifts will incur costs but again, those costs can be offset through the funding ideas previously proposed. Simply put, if the corporations will shift their operations over to the fusion center, the centers can be self-funding until success is measured and then that success can then be sold back to the corporations for future funding. Funding will ultimately be the most difficult hurdle to leap over but one that has a myriad of solutions for those of creative aspirations.

This type of program is not new and has already seen great successes in England through the Metropolitan and London Police's Dedicated Cheque and Plastic Crime Unit established in 2011 with primary monetary support from banks that are members of the Association of Payment Clearing Services (APACS). News reports have praised them in that in addition to investigating identity fraud offenses, they will investigate check, cash machine, and other offenses where organized crime is involved. The APACS members have funded approximately three-quarters of the start-up costs, thus freeing up government monies for other tasks (Fight against credit card fraud, 2011). In October 2012, the unit successfully apprehended a criminal organization who exceeded £10 million and who was estimated to be making approximately £50,000 a week by passing counterfeit checks (City of London Police, 2012).

It is proposed that Texas follow the Dedicated Cheque and Plastic Crime Unit's model, either in one of the larger metropolitan areas such as Dallas, Houston, or San Antonio, with the same modeling as currently established through use of the current fusion centers. An easier solution may be to simply allow for space in the already

established fusion centers for these units to be implemented statewide so as to reduce infrastructure costs and mitigate security concerns.

REFERENCES

American Civil Liberties Union. (2005, May 11). ACLU of Massachusetts questions scope of fusion center activities [Press release]. Retrieved from https://www.aclu.org/technology-and-liberty/aclu-questions-scope-intelligence-fusion-center-massachusetts

Bain, B. (2008, February 14). *A new threat, a new institution: The fusion center*. Retrieved from http://fcw.com/articles/2008/02/14/a-new-threat-a-new-institution-the-fusion-center.aspx

Beare, M. E., & Murray, T. (2007). *Police and government relations: Who's calling the shots?* Toronto, Ontario, Canada: University of Toronto Press.

Bureau of Justice Assistance. (2012, June). *Increasing analytic capacity of State and Local Law Enforcement Agencies: Moving beyond data analysis to create a vision for change.* Retrieved from https://www.bja.gov/Publications/LEFGIncreasingAnalyticCapacity.pdf

City of London Police. (2012, October 26). *Police break-up suspected £10 million counterfeit gang*. Retrieved from http://www.actionfraud.police.uk/police-break-up-suspected-10-million-counterfeit-gang-oct12

Committee on Homeland Security and Governmental Affairs. (2012). *Federal support for and involvement in State and Local Fusion Centers.* Washington, DC: United States Senate.

Cops: Felony lane gang behind spike in Texas smash 'n grabs. (2014, June 30). *CBSNews*. Retrieved from http://www.cbsnews.com/news/cops-felony-lane-gang-behind-spike-in-texas-smash-and-grabs/

Federal Trade Commission. (2012, January). *Consumer sentinel network data book for January - December 2012.* Retrieved from http://www.ftc.gov/sites/default/files/documents/reports/consumer-sentinel-network-data-book-january/sentinel-cy2012.pdf

Fight against credit card fraud. (2011, March 18). Retrieved from http://www.dailymail.co.uk/news/article-111658/Fight-credit-card-fraud.html

Finklea, K. (2014). *Identity theft: Trends and issues.* Washington DC: Congressional Research Service.

Harrell, E., & Langton, L. (2013). *Victims of identity theft, 2012.* Washington, DC: Bureau of Justice Statistics.

Johnson, S. A. (1998). *Solvability factors: Managing the criminal investigation function through early closure.* Huntsville, TX: Bill Blackwood Law Enforcement Management Institute of Texas.

McNally, M. M., & Newman, G. R. (2005). *Identity theft literature review.* Washington DC: U.S. Department of Justice.

Newman, G. R. (2002). *Check and Card Fraud.* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Oakley. (1997). *Bill analysis: C.S.H.B. 2617.* Austin, TX: Texas Board of Higher Education.

Stanley, J. (2004). *The surveillance-industrial complex: How the American government is enlisting private parties in the construction of a surveillance society.* New York, NY: ACLU.

Texas Code of Criminal Procedure. (2014). *Code of Criminal Procedures, Title 1. Code of Criminal Procedure, Chapter 13.02 Forgery.* Retrieved from http://www.statutes.legis.state.tx.us/Docs/CR/htm/CR.13.htm

Texas Penal Code Title 7, A. (2014, July 1). Retrieved from http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.32.htm

U.S. Department of Homeland Security. (2014, July 1). *Fusion center locations and contact information*. Retrieved from http://www.dhs.gov/fusion-center-locations-and-contact-information

U.S. Department of Justice. (2008, September). *Global justice information sharing initiative (Global)*. Retrieved from https://www.fema.gov/pdf/government/grant/2010/fy10_hsgp_fusion.pdf

U.S. General Accounting Office. (2002, March). *Identity theft: Prevalence and cost appear to be growing.* Retrieved from http://www.gao.gov/new.items/d02363.pdf

Williams, M. R., Holcomb, J. E., & Kovandzic, T. V. (2010, March). *Policing for profit*. Retrieved from https://www.ij.org/part-i-policing-for-profit-2