



**Prepared Remarks of  
James H. Freis, Jr., Director  
Financial Crimes Enforcement Network**

**Nebraska Bankers Association  
Summit on Regulatory Issues  
October 28, 2011  
Lincoln, NE**

Good afternoon. I appreciate the opportunity to speak with you all today about the work we are doing at the Financial Crimes Enforcement Network – known as FinCEN. I know it was six years ago that my predecessor, Bill Fox, spoke before this conference, so I am happy to be in Nebraska representing FinCEN again.

Let me say at the outset that the work being done by the Nebraska Department of Banking and Finance underscores the strong partnership between our two agencies, particularly under John Munn’s leadership as Director. And his work to promote a strong banking system extends beyond Nebraska, as John serves an important role as one of five representatives to the Federal Financial Institutions Examination Council (FFIEC) State Liaison Committee, which works to encourage the application of uniform examination principles and standards by state and federal agencies.

This is all the more an honor and pleasure for me to be here at the culmination of a visit over the past couple of days with bankers, their regulators, and Federal and State law enforcement, discussing how we, working together, can further our shared goals of protecting the financial system and its customers from criminal abuse.

I truly appreciate opportunities like this to meet with bankers, including a few times each year with members of state banking associations, to discuss why and how at FinCEN we do what we do, and why it matters to you as bankers, as well as your customers.

***FinCEN overview***

FinCEN was established 21 years ago to combat money laundering, track illicit finance, and serve as a nexus for information gathering and sharing among Federal, State, and local law enforcement agencies. Providing support to law enforcement is one of the main reasons FinCEN exists. Almost all crime is rooted in financial profit, and it is our job to help law enforcement follow the money and piece the financial trail together.

FinCEN's mission must continue to evolve, and our focus now includes new responsibilities to help combat terrorist financing, fraud, and other increasingly sophisticated financial crimes.

And in any regulatory framework, establishing rules, providing education, guidance and feedback, and enforcing compliance are all critical components and mutually reinforcing. In the anti-money laundering and counter-terrorism financing (AML/CFT) context, the basic types of rules can be simplified down to a few common categories: (i) knowing your customer and being vigilant against criminal abuse; (ii) keeping records so that they are available to "follow the money" if needed as part of an investigation of suspicion or criminal activity; and (iii) reporting of information, most critically Suspicious Activity Reports (SARs).

As many of you know, FinCEN administers the Bank Secrecy Act (BSA), the nation's first and most comprehensive Federal AML/CFT statute. In brief, the BSA authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to take a number of precautions against financial crime, including the establishment of AML programs, and ~~to~~ require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations and proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." The Secretary of the Treasury has delegated administration of the BSA to FinCEN.

The key to everything we do is *sharing* the extremely valuable information that financial institutions provide to us. As part of our responsibility, FinCEN oversees the maintenance of a database with approximately 180 million records of financial transactions and other reports filed by financial institutions like yours. This data represents the most broadly relied upon and largest source of financial intelligence available to law enforcement.

In addition to collecting, analyzing, securing, and disseminating the FinCEN data to our law enforcement and regulatory partners, FinCEN itself is also a financial institution regulator. We have the challenging but important task of writing and coordinating the enforcement of AML rules for over 100,000 banks, credit unions, money services businesses (MSBs), insurance companies, securities brokers, casinos, mutual funds, precious metal dealers, and other financial institutions that face the risk of being used by criminals to support enterprises ranging from drug cartels, mortgage fraud rings, terrorist finance networks, immigrant smuggling, and much more.

And FinCEN works hard with our regulatory partners, including with other banking supervisors through the FFIEC, to ensure consistency and clarity with respect to the compliance expectations we have for banks. When Bill Fox spoke here six years ago, he discussed the roll-out of the FFIEC examination manual, designed to focus the examiner's attention squarely on the quality and effectiveness of a bank's AML program.

It was an important decision for us at the time to make that manual publicly available.<sup>1</sup> The results have exceeded all expectations in terms of helping banks and their regulators work together to achieve the goals of protecting the financial system from criminal abuse. Since that time, the manual has gone through a number of iterations to keep up to date with new regulatory

---

<sup>1</sup> See [http://www.fincen.gov/financial\\_institutions/di/](http://www.fincen.gov/financial_institutions/di/)

and industry developments and ways to mitigate AML/CFT risks. Once again, John Munn, as a state representative to the FFIEC, plays an important role in that effort to ensure consistency of approach among banking supervisors.

Given the scope of FinCEN's mission, people are often surprised to learn that our workforce is only comprised of slightly over 300 employees. Our dedicated team includes analysts that study and research the reported information to support law enforcement – both domestically and internationally; regulatory experts developing guidance for the financial industry; and IT specialists building systems to ensure the FinCEN information your institutions report is readily accessible to our law enforcement and regulatory partners.

### **Feedback on the Use and Usefulness of the Data Reported to FinCEN**

Last year, FinCEN undertook an outreach initiative to smaller depository institutions all over the country to hear about how these institutions implement their anti-money laundering programs, including unique challenges faced by institutions across this asset class and where additional guidance from FinCEN could be helpful. These meetings built upon FinCEN's previous outreach with large depository institutions in 2008, followed in 2009 by meetings with some of the nation's largest money services businesses.

In addition to on-site meetings with 18 depository institutions in 13 states, FinCEN staff also held town hall style meetings in both Chicago, Illinois and Eden Prairie, Minnesota, where we engaged with more than 40 different institutions.

Based on the number of institutions that expressed an interest in meeting at FinCEN's offices, FinCEN invited a number of them to participate in two town hall meetings – one for banks and one for credit unions – that hosted at FinCEN's offices in suburban Washington, D.C. The one common theme that arose during these meetings was about the use and usefulness of the currency transaction report (CTR) and the suspicious activity report (SAR) information reported to FinCEN. With that in mind, I would like to spend a moment talking about how FinCEN – and others – are using and protecting this data that is provided to us by your institutions.

**Tip Off:** Primarily with respect to a SAR, but also sometimes with a CTR, the FinCEN information provided can be the first tip that starts an investigation. A financial institution employee's good instincts can, and do, result in the contribution of critical information that serves to set investigatory wheels in motion to track down suspected criminal activity. Most people understand and expect this usage, yet fail to appreciate the following broader uses of FinCEN data.

**Identifying Information:** When an investigation is already underway, the information reported to FinCEN can add significant value by pointing to the identities of previously unknown subjects, exposing accounts and other hidden financial relationships, or unveiling items of identifying information like common addresses or phone numbers that connect seemingly unrelated individuals and, in some cases, even confirming locations of suspects at certain times.

Law enforcement, again and again, confirms the reliability and usefulness of the information you report to FinCEN, which is a direct reflection of the diligence and training within institutions such as yours.

**Trends:** Law enforcement investigators, as well as FinCEN analysts, can use technology to examine the entire information base more broadly. When expertly queried, the trends and patterns emerge with tell-tale signs of criminal or terrorist activity revealing their networks and emerging threats. Hidden in the wealth of information, but easily revealed by skilled analysts with the right tools, are very reliable and credible reports of mortgage fraud, check fraud, identity theft, bribery, counterfeiting, insider abuse, and other financial crimes.

This information can also be overlaid on a map to make apparent the geographic range of suspicious activity and allow law enforcement agencies to better allocate their limited resources for maximum effectiveness. We can only gain such insights with the aid of a large database in which we see vulnerabilities otherwise invisible to individual institutions or the limited scope of a single report.

**Deterrence:** The very existence of FinCEN's regulations has a deterrent effect on those who would abuse the financial system. The certainty of a CTR filing and the mere possibility of a SAR filing force criminals to behave in risky ways that expose them to exposure, scrutiny and capture.

Criminals fear detection if they use the U.S. financial system and are willing to take great risk to avoid its well-designed capability to detect illicit activity. The definitive CTR threshold forces criminals to structure their transaction which, in turn, exposes them to a SAR filing. CTRs and SARs are complementary forms that together create an intimidating criminality trap. In addition to the increased likelihood of discovery, it's a success of its own that our collective efforts make it more difficult and time consuming for illicit actors to realize the proceeds of crime or raise and move funds for terrorist training and operations.

In summary, information reported to FinCEN can – and does – play an important role in different ways that contribute to the success of many law enforcement investigations. With that in mind, I'd like to take a minute to share with you more specifics about how FinCEN engages with its law enforcement and regulatory partners in Nebraska.

### ***Who is Using the FinCEN Data?***

FinCEN has 88 MOUs in place with U.S. Attorney's Offices all around the country to enable them to access FinCEN data to investigate and prosecute criminal activity involving the U.S. financial system. There are currently more than 12,000 nationwide users of the information at all levels of the law enforcement and regulatory communities—many of whom can access the BSA data remotely.

Additionally, FinCEN also opens its doors to law enforcement agencies who wish to come to our office to access the FinCEN data. Our Platform Program provides onsite access to FinCEN systems for designated personnel in the Washington, D.C. area who are conducting research for their agency's investigations. Currently, 41 Federal law enforcement agencies participate in this

program, including Federal Inspector General's offices, who work to uncover waste, fraud, and abuse in government programs.

FinCEN's systems also provide us with alerts when more than one agency is researching the same subject within the FinCEN data. Last year alone, FinCEN networked agencies together more than 1,000 times by contacting investigative personnel in the respective agencies and providing them contact information for other agency personnel.

Networking can help law enforcement by facilitating information sharing, avoiding potential negative impacts on other cases, and maximizing resources. Our networking capabilities are also enhanced by the fact that FinCEN has representatives working on-site as liaisons from 12 different Federal law enforcement and regulatory agencies.

FinCEN also provides direct analytical support to law enforcement efforts across the state of Nebraska, and conducts strategic analysis based on studying the information reported to FinCEN. The focus of much of our work in this area has been on mortgage loan fraud.

Recently, FinCEN issued its Mortgage Loan Fraud (MLF) analysis for the first quarter of 2011, which found that the number of MLF suspicious activity reports (SARs) rose to 25,485, up 31 percent year over year from 19,420 in the first quarter of 2010. Our analysis attributes the increase to large mortgage lenders conducting additional reviews after receiving demands to repurchase poorly performing mortgage loans. In the 2011 first quarter, 80 percent of MLF SARs reported activities which occurred more than three years prior to the filing of the SARs.

### ***How the FinCEN data is used in Nebraska***

Law enforcement and regulatory officials, including the Nebraska Department of Banking and Finance, the Attorney General's Office, the US Attorney's Office, and the Nebraska State Patrol, are very active users of the information reported to FinCEN. In fact, in October 2008, John Munn authored an article in the SAR Activity Review, Trends, Tips and Issues, that discussed the importance of the use and protection of FinCEN data.

As Director Munn states in the article, "The Department monitors SAR activity among our state-chartered banks on an ongoing basis and each month, SARs are downloaded, printed, and reviewed by legal staff for suggestions of criminal wrong-doing. After gaining approval from FinCEN and the Nebraska State Patrol, a SAR may be referred to the Nebraska Attorney General for follow-up with the county attorney." Director Munn's office also finds the FinCEN data valuable during the evaluation process for executive officers and in their supervision of mortgage and payday lending.

The FinCEN data is also made available to state and local law enforcement agencies. Each state also has a coordinator, so law enforcement agencies without direct access to the FinCEN data are able to make requests through them to query the information. In Nebraska, numerous state and local agencies are utilizing the information reported to FinCEN through the Nebraska State Patrol, your state's coordinator. FinCEN conducts audits of how the data is being used and also conducts on-site inspections to ensure appropriate protocols designed to protect this sensitive data are being followed.

There are also over 100 SAR Review Teams located throughout the country, typically coordinated through the U.S. Attorney's Office. SAR Review Teams are comprised of State, local, and Federal law enforcement and regulatory authorities in the area, meet on a regular basis to review SARs filed within their judicial district, and coordinate law enforcement investigative follow-up as appropriate.

Nebraska has an active SAR Working Group, coordinated by the U.S. Attorney's Office, reviewing SARs filed within their jurisdiction. Nebraska's SAR Working Group includes representatives from Federal, State and local agencies throughout the state who participate in the monthly meetings.

The agencies include: the Internal Revenue Service, the United States Secret Service, the Department of Homeland Security, the Social Security Administration, the Drug Enforcement Administration, the Department of Labor, the United States Postal Inspection Service, the Federal Bureau of Investigation, the Federal Deposit Insurance Corporation, the Omaha Police Department, and the Nebraska Department of Revenue.

There have been several success stories resulting from investigative efforts in Nebraska. While I am unable to discuss some of these cases as they are still in the indictment phase, in one case a proactive review of SARs triggered an investigation that uncovered a scheme to defraud individuals and businesses out of millions of dollars. Not only did the SARs provide crucial details of an ongoing fraud, the 314(b) provision of the USA PATRIOT Act enabled financial institutions to work together and share information, resulting in the closing of suspect accounts and slowing the spread of the fraud. The subject ultimately pled guilty and was sentenced to 4 years in prison and was ordered to pay \$3.7 million in restitution.

### ***Nebraska Filings: A Snapshot***

Now that we've spent some time discussing the use of the data, I wanted to quickly touch on what FinCEN is seeing statistically when we look at the information reported to FinCEN, Nebraska institutions are filing.

SAR filings in Nebraska totaled 1,879 in 2010, down 5% from the previous year's total of 1,987 filings (just slightly more than the 3% decline in SAR-DIs filed nationally). Looking more closely at the Nebraska filings, decreases were seen in filings reporting suspected credit card fraud (down 41% from the previous year), and identity theft (down 20% from the previous year). However, there was an increase in mortgage loan fraud SARs between 2009 and 2010 of 55%.

Nebraska's SAR filings account for less than 1% of national SAR filings, and Nebraska ranks 48<sup>th</sup> in terms of number of SAR subjects per capita in calendar year 2010. Geographically – and understandably – the highest concentration of SARs filed in Nebraska came from the state's most populated areas, including Omaha and Lincoln.

In terms of characterizations of suspicious activity, BSA/Structuring/Money Laundering was the most frequently cited violation, occurring in 1/2 of the SARs filed (which is what we see on average nationally as well.) The 2<sup>nd</sup> ranked characterization is cited as "other." In taking a

closer look, SARs reflecting a violation of “other” showed the following type of transactions (in one form or another) as occurring with the most frequency: Cash Kiting; Tax Evasion/Tax Fraud; Large Cash Deposits/Withdrawals; and Unregistered MSB.

Elder Financial Abuse was also noted in about 7% of those SARs reflecting “other” in 2010. In February 2011, FinCEN issued an advisory to help financial institutions spot and report on activities involving elder financial exploitation, and the SARs filed so far in 2011 by Nebraska depository institutions indicate that banks are continuing to identify and make us aware of this activity. When reviewing the narratives of the SARs filed in 2011 marked as “other,” 11% reflect suspected elder financial abuse.

I know the Nebraska Bankers Association is also doing its part to help banks identify and report this activity. Today’s NBA E-Update highlights its comprehensive Elder Abuse Handbook, which provides “red flags” to help banks spot the abuse, as well as information on reporting this activity.<sup>2</sup> As the guide states, while Nebraska law does not require banks to report suspected elder abuse, “banks may consider not processing a transaction requested by the elder or the elder’s representative and may voluntarily elect to make a report to Adult Protective Services.” The training guide further notes, “Banks should be aware that in certain circumstances, it may be appropriate to make a report to Adult Protective Services *and* file a Suspicious Activity Report (SAR) under federal law.”

For those of you interested in learning more about SAR statistics either in your state or across the country, FinCEN publishes statistics twice a year on our website where you can not only review various numerical breakdowns, but can also see the information plotted using mapping techniques.

### ***Information Sharing***

#### **314(a)**

Another area I wanted to touch on, which was also discussed during our outreach meetings last year, is the use of the 314(a) and 314(b) programs.

As most of you are probably aware, FinCEN’s regulations under Section 314(a) of the USA PATRIOT Act enable Federal, State, local, and foreign law enforcement agencies, through FinCEN, to reach out to more than 45,000 points of contact at more than 22,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or significant money laundering.

FinCEN receives requests from law enforcement agencies and upon review sends requests to designated contacts within financial institutions across the country generally once every two weeks via a secure Internet Web site. The requests contain subject and business names, addresses, and as much identifying data as possible to assist the financial institutions in searching their records.

---

<sup>2</sup> See <http://www.nebankers.org/index.php/Bank-Security/elder-abuse-prevention-handbook.html>

The financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last six months, unless a different time period is specified in the request. Financial institutions typically have two weeks from the transmission date of the request to respond to 314(a) requests. If the search does not uncover any matching of accounts or transactions, the financial institution is instructed not to reply to the 314(a) request.

To date, financial institutions have responded with over 100,000 positive subject matches – and over 300 of these responses have come from 31 depository institutions in Nebraska. And based on the total feedback we have received, 78% of 314(a) requests have contributed to arrests or indictments, demonstrating the high value of information these institutions are providing to law enforcement.

FinCEN's review of our data also shows that in the past 5 years, approximately 64 percent of positive 314(a) matches have come from institutions with assets under \$5 billion. In addition, of the total number of institutions that have responded to 314(a) requests over this 5-year period, FinCEN estimates that 92 percent of these institutions have assets under \$5 billion.

The general proposition remains true that in absolute terms a very small depository institution is statistically less likely to be touched by organized criminal activity than the largest depository institutions with millions of customers and tens or hundreds of billions in assets. But the 314(a) statistics alone have shown that in comparative terms a disproportionately high number of actual cases of terrorist financing and significant money laundering have involved accounts and transactions at smaller depository institutions. The 314(a) statistics underscore the importance that all financial institutions, big and small, have an understanding of the risks affecting them and should implement appropriate policies and procedures to mitigate those risks.

### **314(b)**

Section 314(b) of the USA PATRIOT Act allows regulated financial institutions to share information with each other for the purpose of identifying and, where appropriate, reporting possible money laundering or terrorist activity.

In speaking with many of the largest banks in 2008, FinCEN found use of the 314(b) process to be quite extensive, with several banks noting that they often use the 314(b) process throughout the course of a SAR investigation, before filing a SAR or making a decision to close an account. In our discussions with institutions with assets under \$5 billion, however, FinCEN found there was rather limited use of the 314(b) program.

For an institution to share, they simply need to visit FinCEN's Web site and fill out a short form providing notice of their intent to share information, and designating a point of contact. The form is very simple to complete and FinCEN will provide you with a 314(b) certification for your records.

In FinCEN's town hall meetings last year, institutions shared their experiences with 314(b) including how simple the procedure is to register with FinCEN. One institution shared how



difficult it was to discuss a case with a counterpart (for example, seeking more information about a potentially suspicious wire transfer from the institution originating the transfer) in the absence of the institutions being registered under 314(b).

This is exactly the kind of situation where the institutions should be relying on the safe harbor available under 314(b). Absent the safe harbor provided by 314(b), an institution could find itself in violation of laws and customer confidentiality obligations.

While participation in 314(b) is ultimately voluntary, FinCEN is continuing to pursue avenues in which the importance of information sharing in order to protect the financial system can be conveyed.

FinCEN specifically put out guidance in June 2009 on the scope of the safe harbor includes the sharing of information on possible money laundering relating to an array of underlying fraudulent and criminal activity.<sup>3</sup>

For those of you not among the 73 institutions in Nebraska currently signed up to share via the 314(b) program, I hope you will visit FinCEN's Web site at [www.fincen.gov](http://www.fincen.gov) or contact the FinCEN 314 Program Office with any questions you may have. The number is (866) 326-8314.

As I mentioned earlier in one of the Nebraska investigations started by a SAR, two Nebraska institutions shared information through the 314(b) program, enabling the fraud to be slowed down considerably. I think we would all agree that everyone benefits – your customers, your business, and law enforcement – when fraudulent activity can be detected, shared, and mitigated as early as possible.

### ***E-Filing***

One last area I would like to touch on, and in which we've had recent developments, is E-Filing. E-Filing is a free, web-based electronic filing system that allows filers to submit through a secure network their reports required under FinCEN's regulations implementing the BSA.

On September 14, FinCEN formally requested comment on its proposal that reports required under the BSA be electronically filed beginning June 30, 2012. The benefits of E-Filing, both to the government and to the filer, are obvious and compelling. As more and more financial institutions migrate to E-filing, they will be impressed with the ease and convenience of using their basic Internet connections, while gaining immediate feedback to continually improve the quality and usefulness of the reported information in the effort to combat financial crimes.

In the past six months, approximately 90% of CTRs filed by Nebraska financial institutions were E-filed; while only two-thirds of SARs were filed electronically. For those institutions in Nebraska that are still filing on paper, we encourage you to begin looking into transitioning to E-filing.

---

<sup>3</sup> See [http://www.fincen.gov/statutes\\_regs/guidance/pdf/fin-2009-g002.pdf](http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-g002.pdf)

E-Filing is a faster and more convenient, secure, and cost-effective method of submitting their reports as well as for receiving confirmation of their acceptance and notices of any errors. Support is available through FinCEN's website or through our helpline at 866-346-9478 to get you started or answer any questions you may have.

One final point: the greater use of E-Filing also assists FinCEN in providing important information relevant to money laundering and terrorist financing investigations to law enforcement in the quickest manner possible. Through E-Filing, reports are available to and searchable by law enforcement in two days, rather than two weeks, for example if filed on paper.

### ***Conclusion***

I hope through my remarks today you have a better understanding about the work FinCEN does – particularly in the area of how we use the information you report to us, and the usefulness to law enforcement of this information. Providing feedback in this area is something we take very seriously. However, we must also be diligent to find the appropriate balance between sharing information and maintaining appropriate confidentiality.

Particularly with respect to SARs, FinCEN and law enforcement take very seriously the obligation of public trust in which sensitive personal and financial information about customers is reported under an expectation and obligation of confidentiality. The obligation to protect the confidentiality of reported information prevents us from disclosing that a SAR was filed or from providing too many investigative details even in the case of an ultimate criminal conviction.

And even in more general trend reports, sometimes we seek to avoid providing a level of detail that would serve as a roadmap for criminals to see how others have successfully laundered money or the investigative techniques that law enforcement has used to apprehend them.

With that being said, FinCEN is committed to continuing to share as much as we can in this area. Thank you again for your time today and I am happy to answer any questions you may have.

###