PREPARED REMARKS OF JAMES H. FREIS, JR.
DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. DEPARTMENT OF THE TREASURY

DELIVERED AT THE FINANCIAL SERVICE CENTERS OF AMERICA, INC.
THE 22ND ANNUAL FiSCA CONFERENCE AND EXPOSITION

LAS VEGAS, NV
OCTOBER 2, 2010

The theme of your conference this year – Moving Forward: Issues and Answers for a Changing Industry – is particularly fitting given the issue I would like to discuss with you today. Change is something that your industry has always needed to adapt to. Even more than a decade ago, FiSCA recognized that financial services were evolving. Originally established in 1987 as the National Check Cashers Association (NaCCA), the name was changed in 1999 to the Financial Service Centers of America (FiSCA) to reflect the industry's evolution.

As business people working in a difficult financial environment, you already know how vital it is to be flexible and stay competitive within the business world. It poses an additional challenge when criminal actors try to take advantage of your business or of your customers. But it is in exactly this area where the interests of all of us present here are most closely aligned. It is FinCEN's reason for being to help keep criminal actors from abusing the financial industry and to work with financial services providers to help law enforcement track down criminals, hold them accountable, and seize the proceeds of crime.

Despite law enforcement's very necessary focus on combating serious and organized financial crime, including terrorist–related activities that remain an ongoing threat – one of the simplest and most prevalent ways to commit a financial crime, to steal money, is to commit some form of ***check fraud***. It can be easy to lose sight of the volume of this basic and longstanding type of criminal activity – be it a form of counterfeiting paper instruments, falsifying legitimately created checks, or misrepresenting the authorized drawer or payee; especially, when we compare it to emerging threats to our financial system or new and evolving types of financial transactions and instruments for which criminals devise new methods to commit criminal activity.

The check-cashing industry, including many of you here today, know all too intimately the impact that check fraud can have on your business and the customers that you serve. For although overall check use throughout our country is declining (albeit at a slower rate than many have predicted from time to time), there remains a large number of persons, including unbanked and underbanked consumers, who rely on the services you provide and appreciate the convenience, service and instant access to funds. Once again, we at FinCEN share your concern and interest in doing something about the criminals who seek to abuse your legitimate business model and take advantage of the financial services you provide as well as take advantage of some of your customers.

Thus, today I would like to engage in a dialogue with you about some of the criminal trends and risks related to check fraud across the financial services industry, and then also how we, working in partnership between the government and the financial services industry, might be able to better work together to mitigate these risks of criminal activity.

Check Fraud Remains Common

Every few days the Federal Deposit Insurance Corporation (FDIC) or Office of the Comptroller of the Currency (OCC) sends out a public alert of some type of counterfeit checks or other instruments being circulated around the country.[1] The OCC's most recent listing of counterfeit instruments and stolen documents[2] identified for the five-year period of 2005 to 2009 about two hundred different examples of counterfeit or fictitious cashier's checks, official checks, expense checks, money orders, and other instruments.

While we may never know the full costs of check fraud across the financial industry, some of the available information shows impacts that are staggering. In terms of direct losses to banks – as the financial institutions on which the checks are purportedly drawn or which provide value or credit on the basis of checks – the American Bankers Association (ABA) conducts a regular survey of selected commercial banks. The 2009 ABA Deposit Account Fraud Survey, which collects baseline information on check and electronic payment fraud losses, estimated that industry check-related losses amounted to $1.024 billion in 2008, up slightly from the $969 million in 2006 and marking the first time within the ABA's survey that check-related losses surpassed one billion dollars.[3] By comparison, commercial bank losses from debit card fraud—POS signature, POS PIN, and ATM transactions combined—reached an estimated $788 million in 2008. Eight in 10 banks (80

[1] See, e.g., FDIC special alert that counterfeit cashier's checks bearing the name First Federal Bank, Kansas City, Missouri, are reportedly in circulation (September 15, 2010), http://www.fdic.gov/news/news/SpecialAlert/2010/sa10132.html.

[2] OCC Alert 2010-13 (September 13, 2010), http://www.occ.ÇÏÖŽÓÔÅÔÉÃŽÎÅ×ÓŽÉÓÓÕÅÎÅÓ/alertÓŽçπρπ/ÁÌÅÒÔŽ2010-13.html.

[3] See http://www.aba.com/Surveys+and+Statistics/2009_Deposit_Fraud.htm.

percent) continued to report having check fraud losses in 2008, the same percentage as in 2006.[4]

While new technology can increase the speed and efficiency of the check clearing process, it also may create new opportunities for fraud. For example, remote deposit capture (RDC) through digital scanners and increasingly mobile devices such as iPhone cameras is tremendously convenient to businesses and consumers. The digital images, however, fail to capture many of the protections developed over the past two generations to mitigate check fraud and counterfeiting: magnetic ink character recognition (MICR) encoding, indelible inks, microprinting, watermarks, etc. How can we prevent an unscrupulous criminal from scanning a check for deposit at a bank and then trying to negotiate the same instrument with a check casher? Financial institutions need to anticipate such risks as they develop new products. FinCEN and the Federal Banking Agencies have published some information on supervisory expectations with respect to RDC.[5] We welcome further suggestions from industry participants as to how we can continue to promote the benefits of evolving technology while responsibly managing the risks across all parties involved in related financial transactions.

In some circumstances, banks will be in a position to mitigate a direct loss to the bank by offsetting the value of the fraudulent instrument against the account of the individual or business who deposited the instrument (in an analogous way to how banks seek to reverse a string of transactions to return checks where the drawer has insufficient funds in the underlying demand deposit account). This provides little comfort to the merchant or individual who accepted a check in good faith. For the check-cashing industry, such losses cut directly into your bottom line, which in turn affects your ability to provide your services to the consumers who need them. By one estimate, the check cashing industry provides $80 billion in services a year. I understand from FiSCA that approximately 1.2% of cashed items are not paid to the financial service centers due to fraud.

---

[4] See http://www.aba.com/Surveys+and+Statistics/SS_Depositfraud.htm.

[5] See Federal Financial Institutions Examination Council (FFIEC), Bank Secrecy Act / Anti-Money Laundering Examination Manual (2010), pp. 209-211, http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf ; FFIEC, Risk Management of Remote Deposit Capture, p. 5, http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf ("Risks associated with fraud are not unique to RDC; however, certain aspects of fraud risk are elevated in an RDC environment. Check alteration, including making unwarranted changes to the Magnetic Ink Character Recognition (MICR) line on the image of scanned items, may be more difficult to detect when deposited items are received through RDC and are not inspected by a qualified person. Similarly, forged or missing endorsements, which may be detected in person, may be less easily detected in an RDC environment. Certain check security features may be lost or the physical alteration of a deposited check – such as by "washing" or other alteration techniques – may be obscured in imaging or electronic conversion processes. Counterfeit items may be similarly difficult to detect. Duplicate presentment of checks and images at the institution or another depository institution represents both a business process and a fraud risk.").

The Declining Use of Checks

While it is clear that check fraud continues to plague the industry, it is interesting to step back for a moment and consider this in the context of how the use of checks has evolved in recent years.

Checks or related types of demand drafts have been around for hundreds of years. Although checks are still commonly used in the United States, it is fair to say that their heyday is past. This evolution has been hastened first by the rise in credit cards, and more recently by shifts to debit cards, the Automated Clearing House (ACH) for check conversion or one-time ACH debit transactions, and other emerging payment technologies such as on-line payment systems. According to statistics from the Committee on Payment and Settlement Systems (CPSS), the five years through 2008 witnessed a steady decline in check usage in all thirteen CPSS member countries, while direct debits in particular were generally rising.[6] Last December, the United Kingdom's Payments Council – the organization that sets strategy for payments within the UK – announced that their banks intend to phase out checks in 8 years time – in October 2018.[7]

Here in the United States we estimate that check use peaked in the mid–1990s. A Federal Reserve Bulletin published in 2002 – after its Retail Payments Research Project was complete – notes that data shows that an estimated 32.8 billion checks were paid in the United States in 1979, 49.5 billion in 1995, and 42.5 billion in 2000.[8] Survey data collected for the Federal Reserve in 2007 indicates an ongoing shift in the ways consumers and businesses make payments. By 2006, the number of electronic payments was more than double the number of check payments, or about two-thirds of all noncash payments.[9]

Even within the Federal Government, the use of checks began to diminish within this same time period of the mid-1990s. Signed into law in 1996, the Debt Collection Improvement Act (DCIA) required the use of electronic funds transfer (EFT) for most federal payments, with the exception of tax refunds.[10] The Department of the Treasury issued a final rule implementing the DCIA on September 25, 1998, which also established the circumstances under which waivers to the DCIA are available.[11]

---

[6] See Committee on Payment and Settlement Systems of the Group of Ten Countries, Statistics on payment and settlement systems in selected countries, (December 2009), http://www.bis.org/publ/cpss88.pdf, at 241, Table 7.

[7] See http://www.paymentscouncil.org.uk/media_centre/press_releases_new/-/page/855/ . With the increasing popularity of debit cards and online money transfers, banks in the UK estimate that the number of checks written each day has declined from 11 million in 1990 to 4 million in 2009.

[8] See http://www.federalreserve.gov/pubs/bulletin/2002/0802_2nd.pdf.

[9] See http://www.federalreserve.gov/pubs/bulletin/2008/articles/payments/default.htm#t1.

[10] See https://www.fms.treas.gov/debt/dmdcia.pdf.

[11] See https://www.fms.treas.gov/eft/regulations/31cfr208.txt.

The Government can both increase efficiency and provide better services to citizens by evolving the ways it makes payments. One of the federal agencies most impacted by the DCIA is the Social Security Administration (SSA). While the direct deposit program was first introduced by Treasury and the SSA in 1975, participation for SSA benefit payments had only reached 50% by 1990.[12] As the SSA notes, direct deposit payments provide advantages to all parties and offer cost savings to Federal agencies, a significant portion of which can be attributed to the fact that, based on SSA estimates, the cost of issuing an electronic payment is only $0.02, compared with $0.43 for a check.[13] Additional savings come from a reduction in the workload for handling payment-related problems, including fewer claims of non-receipt, as well as a reduction in overpayments caused by double check negotiations. In fact, the U.S. Treasury reported that an individual paid by direct deposit is 20 times less likely to have a payment-related problem compared to individuals paid by check.

The decline in check usage – even an accelerated decline – by no means implies that checks are going to disappear in the United States anytime soon. The Federal Reserve Bank of Boston noted in a working paper issued in 2009 that the decline in check use "had been predicted at least since the 1960s… although the check decline was not surprising, its (late) timing, magnitude, and swiftness were, and the forecast for check use remains quite uncertain."[14] In a more recent Economic Commentary published by the Federal Reserve Bank of Cleveland in June 2009, the declining use of checks in the post-Check 21 era was also studied, to include an analysis on how check clearing is evolving to adapt to changing payment methods.[15] While the study notes that the increasing popularity of electronic payments will continue to decrease the check's overall share in total payments, it also predicts that check volume will "likely stabilize, with billions of checks being written into the future."

I was working at the Federal Reserve Bank of New York on payment systems issues when a committee under the leadership of Board of Governors of the Federal Reserve System Vice Chair Alice Rivlin undertook a fundamental review of the role of the Federal Reserve in the payments system and considered how alternative roles for the Federal Reserve might enhance or undermine the integrity, efficiency and accessibility of the payments system.[16] While acknowledging that even at the time "the persistence of paper checks seem[ed] an anachronism" in the context of alternative and emerging electronic technologies and projections of future decline in check volumes, the committee recommended among other things that the Federal Reserve continue its role in check clearing and work to increase the efficiency of that process. Although the Federal Reserve Banks are now processing less than half the volume of checks they did around the time the Rivlin Report was issued in 1998, in the second quarter of this year, the Federal Reserve's *daily* volume and *daily* value

[12] See http://www.ssa.gov/history/ssa/ssa2000chapter5.html.
[13] See http://www.ssa.gov/history/ssa/ssa2000chapter5.html.
[14] See http://www.bos.frb.org/economic/wp/wp2009/wp0901.pdf.
[15] See http://www.clevelandfed.org/research/commentary/2009/0609.pdf.
[16] See The Federal Reserve in the Payments System (January 1998) ("Rivlin Report"), http://www.federalreserve.gov/boarddocs/press/general/1998/19980105/19980105.pdf.

of commercial checks collected were still over 31 million items valued at over 44 billion dollars.[17] A survey of FiSCA membership showed your financial service centers cashed over 138 million items in 2008.

FinCEN's Focus on Trends in Check Fraud

I have just set out some high-level statistics about how check fraud is significant and has been rising, while overall check usage remains high but in a trend of decline. Now I would like to turn more specifically to look at some of FinCEN's own statistics as they shed insight on this type of financial crime.

First, let us set the context by recalling FinCEN's approach to regulating financial institutions. Although FinCEN regulates a broad range of financial services providers – banks, check cashers, sellers of money orders, money transmitters, casinos, securities broker-dealers, insurance companies, futures commission merchants, and precious metals and jewelry dealers among others – the purpose is a focused one of preventing money laundering, terrorist financing, fraud, and other financial crimes. In practice, FinCEN's regulations can be simplified to three basic categories: vigilance to prevent the financial institution from being abused by criminals (in the form of anti-money laundering programs), recordkeeping requirements to keep a trail of transactions that law enforcement can follow in investigating suspected criminals, and reporting requirements (such as for cash transactions in excess of $10,000).

On that last point, in the mid-1990s – 1996 to be exact – FinCEN finalized a new rule and began collecting reports of suspicious activity from depository institutions on the Suspicious Activity Report form. Of the many possible types of suspicious activity that can be reported by depository institutions on this form, check fraud – as well as related activities such as check kiting, and counterfeit checks – are among them. Almost half of the total number of depository institutions' SARs we have received since that time are for the general category of suspected money laundering, including attempts to evade the reporting requirements of the Bank Secrecy Act (BSA).

But after suspected money laundering, the second most commonly cited suspected suspicious activity indicated on the depository institution SAR form are suspected incidents of ***check fraud***, which accounts for more than 600,000 SAR filings since 1996. And when you include the related activities of check kiting and counterfeit checks – the number of depository institution SAR filings surpasses 1 million.

FinCEN's statistics are likely just a small window into the total volume of possible check fraud. Often FinCEN cautions that a report of suspicion does not necessarily indicate underlying criminal activity, since reporting is required when a financial

[17] See Commercial Checks Collected through the Federal Reserve--Quarterly Data, 2010:Q2, http://www.federalreserve.gov/paymentsystems/check_commcheckcolqtr.htm.

institution knows, suspects, or has reason to suspect that a crime is involved, or even where there is no apparent explanation for a transaction or pattern of transactions.

In many cases of check fraud, however, the bank is certain that there is a fraudulent instrument, even when the bank does not know who initiated the crime. For this reason, the check fraud statistics may be fairly close indicators of criminal activity. On the other hand, the reported check fraud may only be a portion of the check fraud of which a bank may become aware, because FinCEN only requires reporting for amounts in excess of $5,000. Keep in mind that according to survey data collected for the Federal Reserve in 2007, the average value of checks written in 2006 was $1,363.[18] In the second quarter of this year, the average value of commercial checks cleared through the Federal Reserve was $1,406.[19] I understand from FiSCA that based upon a November 2008 survey of your membership the average check cashing transaction amount was $398.

Regarding recent trends, FinCEN's *SAR Activity Review, By the Numbers*, published in January 2010, concluded that reported instances of check fraud increased 19% in the first six months of 2009, compared to the corresponding six-month reporting period in 2008. SARs listing counterfeit check increased 36%, compared to the corresponding six-month period in 2008. (Among related reporting categories, only with respect to check kiting was a multi-year trend broken with a reported decrease, 13% in the first six months of 2009, compared to the corresponding six-month reporting period in 2008.)[20]

And in FinCEN's most recent *SAR Activity Review, By the Numbers,* published in June 2010 and covering all of calendar year 2009, it was noted that 27% of the suspicious activity reported by depository institutions in 2009 can be attributed to fraud-related activities, and that check fraud was one of only two categories that has seen an ***increase*** in SAR reports between 1996 and 2009.[21]

These recent trends have deep roots. FinCEN's very first issue of the *SAR Activity Review* published ten years ago in October 2000 included the American Bankers Association's Check Fraud Loss Report for the first quarter of 2000.[22] This information was provided again in the *Review* that was issued in February 2003, covering check fraud losses from the second quarter of 2002.[23] And even back then, check fraud was second only to money laundering and structuring as the most commonly reported suspicious activity.

---

[18] See http://www.federalreserve.gov/pubs/bulletin/2008/articles/payments/default.htm#f8r.
[19] See Commercial Checks Collected through the Federal Reserve--Quarterly Data, 2010:Q2, http://www.federalreserve.gov/paymentsystems/check_commcheckcolqtr.htm.
[20] See http://www.fincen.gov/news_room/rp/files/sar_by_numb_13.pdf.
[21] See http://www.fincen.gov/news_room/rp/files/sar_by_numb_14.pdf.
[22] See http://www.fincen.gov/news_room/rp/files/sar_tti_01.pdf#page=32.
[23] See http://www.fincen.gov/news_room/rp/files/sar_tti_05.pdf#page=73.

Check fraud shows up in insidious ways. A few years ago, in the October 2007 issue of the *SAR Activity Review*, FinCEN published a lengthy analysis of suspicious activity, specifically identity theft, surrounding the use of convenience checks.[24] As part of this analysis, FinCEN conducted an assessment of Suspicious Activity Reports (SARs) filed during the period April 1, 1996 to March 31, 2007 with narratives containing three key search terms: "credit card checks," "convenience checks," and "courtesy checks." A review of a sample of the SAR narratives indicated the following types of suspected activity involved with convenience check fraud:

- Stolen convenience checks endorsed and deposited for illegal gain.
- Convenience checks counterfeited using computers, scanners, and copiers to create illegal checks.
- Checking accounts established using stolen identities and convenience checks at account opening. Checks subsequently issued from the account were returned for insufficient funds.
- Check kiting used in instances where the subject opened two or more accounts using convenience checks to create fraudulent balances.
- Convenience checks written on closed accounts.

While we know a lot about the individual ways criminals continue to engage in check fraud, perhaps of greater concern is the interrelationship with other types of criminal activity for which we frankly do not know enough. I believe few in this audience would disagree with the proposition that most check fraud activity is unlikely to involve a single instance of criminal behavior. Rather, most suspect that check fraud often occurs as a serial or repeated activity.

But beyond the repetition, criminals who commit check fraud may not stop there. Many may be involved in other illegal activities as well. FinCEN sees examples of this regularly in the reporting it receives from depository institutions. It is not surprising that the most frequently associated suspicious activities commonly listed with check fraud on the SAR form include: 1) counterfeit check, 2) credit card fraud; 3) identity theft; 4) check kiting; and 5) "other." This "other" category really drives home how interconnected check fraud is to other crimes. Some of the related activities reported on a check fraud SAR include: tax evasion; account takeover; ACH fraud, internet and lottery scams; stolen/forged checks; and ATM fraud. Although less directly apparent, experience with individual law enforcement investigations has shown check fraud connected with organized criminal activity from narcotics trafficking to trade-based money laundering to terrorist financing.

And the dollar amounts are staggering. Of the nearly 49,000 SARs filed so far this calendar year by depository institutions reflecting "check fraud," the average suspicious activity amount was for $766,270 and the average loss amount was for $18,836. The amount is reflective not of an individual fraudulent check, but rather

[24] See http://www.fincen.gov/news_room/rp/files/sar_tti_12.pdf#page=11.

the total related activity, including a myriad of other transactions and sometimes repeated financial activity.

Combating Check Fraud

Rest assured that law enforcement does take check fraud seriously and that investigations are pursued and fraudsters have been held accountable. Reports of suspicious activity filed with FinCEN are often a key source of lead information for law enforcement.

I previously mentioned the fact that check fraud was addressed in FinCEN's first *SAR Activity Review* from October 2000, a semi-annual series through which we provide guidance and feedback about how SARs are used by law enforcement. That inaugural edition included a law enforcement success story where a depository institution SAR led to the identification of additional check fraud perpetrated by a subject already under investigation by special agents within the U.S. Secret Service's (USSS) Tampa Field Office.[25] As a result of the SAR filing, investigators were able to make a necessary link and attribute additional fraud losses to the defendant. The defendant was arrested, convicted and sentenced to 48 months in prison on counterfeit check fraud.

In a different case initiated from a proactive review of SARs, an individual pled guilty to fraud when authorities discovered a scheme to defraud individuals and businesses out of millions of dollars. Not only did SARs trigger the investigation, but two filing institutions described in detail transactions related to the check fraud. In addition, the 314(b) provision of the USA PATRIOT Act enabled the institutions to work together and share information, resulting in the closing of suspect accounts and slowing the spread of the fraud.

In another recent investigation, a SAR initiated the investigation of an automobile dealer who used multiple accounts to defraud several banks. The defendant held several accounts at different institutions and continually transferred funds among the accounts, which caused the accounts to be overdrawn, by millions of dollars. In fact, the car dealer was involved in check-kiting schemes that resulted in losses of more than $7 million to banks.

In the narrative of the SAR that started the case, the bank describes the relationship with the defendant and notes that he received a loan for his car dealership. However, the defendant was not using proceeds from the loan to fund his business. As it turns out, he had several bank accounts with various financial institutions and he was moving funds from one account to another. The scheme ran for over a year before he was arrested. He later pleaded guilty and was sentenced to a significant prison term and ordered to pay substantial restitution.

[25] See http://www.fincen.gov/news_room/rp/files/sar_tti_01.pdf#page=20.

The foregoing case examples illustrate two fundamental points. First, FinCEN can gain tremendous insight into organized criminal activity by piecing together suspicious financial transactions reported by multiple financial institutions, including from different sectors. This underscores the reason why FinCEN exists and has been mandated by Congress to regulate a range of financial institutions to combat money laundering and terrorist financing. Second, more specific to check fraud and related crimes such as check kiting, the manner in which checks are negotiated and clear would suggest that combining insights across multiple financial services providers could be particularly valuable.

The point is while several institutions see relatively small amounts lost to fraud, when they share information, a different picture emerges. What may look like a small time scammer could be in actuality a criminal enterprise that has pulled down millions because the activity is spread across a number of financial institutions, each of whom can't see enough to connect the dots. FinCEN, working to analyze SAR information with law enforcement, can paint a more complete picture, using information reported on SARs filed by a number of institutions working in relative isolation.

What More Can We Do Together?

One would hope that with a long history of criminal abuse of checks, individuals and businesses would learn ways to help avoid becoming victims of criminal abuse. The government has been active on many fronts in educating the public and the financial industry about the risks of check fraud as well as ways to mitigate the risks.

Earlier I mentioned how the FDIC and OCC alerted banks about fraudulent instruments, and I explained how FinCEN seeks to raise awareness of particular criminal trends and how reporting by alert financial institutions can help catch criminals. In February 1999, an interagency group of law enforcement and regulators, citing FinCEN SARs as evidence of the growing problem of check fraud, issued an explanatory document for depository institutions entitled *Check Fraud: A Guide to Avoiding Losses*.[26] The United States Secret Service plays a lead investigative role when it comes to financial crimes such as check fraud. I recommend that you review and consider how well your own procedures measure against the tips that the Secret Service provides on their website on ways to protect you and your business from check fraud.[27]

What more can we do? We understand the basic modus operandi of the criminal involved in check fraud. We know that the amount of check fraud is very large and likely growing, notwithstanding the fact that overall check usage is declining. Does this mean that would-be criminals are increasing their focus on checks? Is this due to the legacy of relying on the float time before a fraudulent instrument is

[26] http://www.occ.gov/chckfrd/chckfrd.pdf.
[27] See http://www.secretservice.gov/faq.shtml#faq14.

identified? Or is this due in part to relatively greater difficulty in committing crimes involving other payment mechanisms? For example, it is certainly more difficult and impractical to search all the information available on a paper instrument – such as signature, endorsements, and notations in the "for" line – as compared to the way electronic payments are often monitored through transaction screening software.

Whatever the reasons (which we at FinCEN will continue to probe and ponder), I hope I have provided you a greater understanding of FinCEN's role and some insight into the lenses through which we scrutinize check fraud in working with law enforcement to combat financial crime. Most importantly, FinCEN has the advantage of looking at all available pieces of information to draw together a more complete picture of likely criminal activity than any one financial institution could do on its own.

This leads us to the obvious question as to whether check cashers should be required to file SARs. FinCEN posed this very question for public comment in May 2009.[28] FinCEN did not at the time propose to impose a reporting requirement, but rather posed the question together with a notice of proposed rulemaking clarifying the definition of money services businesses (MSBs), FinCEN's category for financial institutions – including check cashers – subject to regulation. As we continue to work through the MSB regulatory proposal, we appreciate FiSCA's thoughtful comments, including support for FinCEN's proposed revisions to the definition of check casher.

FinCEN received a number of direct responses to the question: "Should check cashers be subject to a SAR requirement?" Several of the comments, including those from representatives from the Congress as well as some industry associations, were supportive of a SAR requirement for check cashers. However, FiSCA stated in its comment letter that although FiSCA does encourage voluntary SAR filings by check cashers, FiSCA did not support a mandatory check casher SAR requirement.[29] As background, SAR filings that are not mandatory can still benefit from the safe harbor protections designed to promote the reporting of suspicious activity to FinCEN.[30] And while FinCEN does receive some SARs from MSBs related to check fraud, including a limited number of voluntary SARs from check cashers, the overall volume is much lower than the check fraud SARs from depository institutions cited earlier, despite the fact that, overall, depository institutions and MSBs file similar numbers of SARs in a given time period.

FiSCA's concerns were that a mandatory check casher SAR requirement might result in a large number of reports to FinCEN with little or no benefit to the BSA goals of curbing money laundering and terrorist financing. An appropriate threshold is one

---

[28] See 74 FR 22129, 22136, http://edocket.access.gpo.gov/2009/pdf/E9-10864.pdf.
[29] Comments received in response to the notice of proposed rulemaking are available at http://www.fincen.gov/statutes_regs/files/CommentListMSBDef.pdf.
[30] See 31 U.S.C. § 5318(g)(3).

way to manage the number of reports that are filed. The question of benefit is one that deserves further exploration.

I have stated many times before, but would like to emphasize for you here today, that fighting fraud has always been and remains a high priority for FinCEN in furthering the purposes of the BSA.[31] The purpose of fraud and almost any type of financial crime is profit, and the proceeds of crime are often laundered through the financial system. Unfortunately, it is true that if a criminal fraudulently obtains dollars from a check casher for some type of false instrument in an amount around the aforementioned FiSCA average of $398, the trail where that criminal spends those funds is likely lost. But if that criminal is a repeat player at check fraud, or if that criminal is involved in other types of illegal activity, then an individual report of check fraud might provide exactly the link or clues (e.g., attributes of the perpetrator, stolen or false identification that was used, nature of the check or monetary instrument, other products purchased) that will allow law enforcement to later identify the criminal actor.

It would appear that SARs filed by check cashers would provide exactly the type of lead information you would wish law enforcement to follow up on – individuals trying to take advantage of your business and customers you serve. Once again to underline the point fundamental to FinCEN's very reason for being – to provide insight into the way criminals move value through any type of financial services provider – I will leave you with some final statistics. In the *SAR Activity Review – By the Numbers*, in addition to the detailed statistics on the number of SARs filed by different types of financial institutions broken out by types of activity and geography, we also highlight changes we see in filing trends. In the most recent edition of this publication from June 2010, FinCEN highlighted among the notable increases not only check fraud with respect to depository institutions, but also that SAR filings by institutions in the securities, futures and insurance industries characterizing the suspicious activity type as check fraud increased 15% in 2009 when compared to those filed in 2008. And to finish on a note most appropriate to our meeting location in Las Vegas today, "Casino SARs identifying check fraud[32] as the Type of Suspicious Activity jumped 47%, from 336 instances reported in 2008 to 493 in 2009."[33]

Conclusion

The criminal activity of check fraud that robs from the bottom line of check cashers may be but one component of a prevalent and likely interconnected form of financial crime. You have my commitment that FinCEN will continue to do its part to help

---

[31] See, e.g., Prepared Remarks of James H. Freis, Jr., Director, Financial Crimes Enforcement Network, Association of Certified Fraud Examiners, 20th Annual Fraud Conference, Las Vegas, NV (July 13, 2009), http://www.fincen.gov/news_room/speech/pdf/20090713.pdf.

[32] The characterization of Check Fraud on the Casino SAR also includes Counterfeit Check.

[33] http://www.fincen.gov/news_room/rp/files/sar_by_numb_14.pdf.

uncover the patterns and work to mitigate risks, as well as to support our law enforcement partners and their investigative efforts. I welcome and look forward to hearing more specific suggestions from check cashers and the broad range of other financial institutions victimized by check fraud as to how, working together, we can do more to combat this illegal activity.

Thank you for your time and for your continued focus on these important issues.

###