

	SWIFT MT103	103.33 CitiBank (1)	Bank of America	JPM Chase	Wachovia (1)	Western Union (2)	MoneyGram (3)
Originator Name	x	x	x	x	x	x	x
Originator Address	x	x	x	x	x	x	x
Amount of the transfer	x	x	x	x	x	x	x
Execution date	x	x	x	x	x	x	x
Payment Instructions	x	x	x	x	x	x	x
Beneficiary Name	x	x (6)	x	x	x	x	x
Beneficiary Address	x	x (6)	x	x	x	x	x
Beneficiary Account Number	x	x (6,7)	x	x	x	(4)	(4)
Originator Account Number	x	x (6,7)	x	x	x	(4)	(4)
Specific Identifier		x (6)				x	x
Beneficiary's Financial Institution	x	x	x	x	x	x (5)	x (5)
Originator Financial Institution	x	x	x	x	x	x (5)	x (5)

Notes:

1. Column header information not provided
2. Only transfers over \$3,000
3. Included transfers both over and under \$3,000
4. While an account number was not present, a transaction ID or reference number was always present
5. These are all intra-institution transfers.
6. If available.
7. When originating a transfer, the FI must keep the account number of the beneficiary. When receiving, the FI must record the account number of the recipient.

17



April 16, 2009

(b)(6)
[Redacted]
Staff Director, Majority Staff
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

(b)(6)
[Redacted]
Staff Director, Minority Staff
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

Dear Messrs. [Redacted] (b)(6)

The Securities Industry and Financial Markets Association¹ (SIFMA) commends the Senate Finance Committee's efforts to capture lost revenue through offshore tax compliance initiatives. We appreciate the opportunity to provide preliminary feedback on the Committee's proposals and hope our comments will result in an effective proposal that achieves the goal of improving tax compliance.

The comments below are specific to the proposal that would require information reporting on funds transfers to foreign accounts. It is our understanding the intent of the proposal is to provide the Internal Revenue Service (IRS) with additional data to track funds moving offshore, thereby enabling the IRS to better detect and investigate cases of potential tax evasion. In addition, third-party reporting of information to the IRS may deter tax evasion since US taxpayers will know the information is being furnished to the IRS.

We would like to make a few general observations about the proposal before making specific comments.

- First, we believe many of the terms and concepts in the legislative draft require clear definitions before financial institutions can determine the feasibility of the proposal and identify operational challenges. We would appreciate the opportunity to provide additional comments once we have a better understanding of the proposal's scope and intent.

¹ The Securities Industry and Financial Markets Association brings together the shared interests of more than 650 securities firms, banks and asset managers. SIFMA's mission is to promote policies and practices that work to expand and perfect markets, foster the development of new products and services and create efficiencies for member firms, while preserving and enhancing the public's trust and confidence in the markets and the industry. SIFMA works to represent its members' interests locally and globally. It has offices in New York, Washington D.C., and London and its associated firm, the Asia Securities Industry and Financial Markets Association, is based in Hong Kong.

- Second, the proposal creates new tax reporting requirements to track funds that move offshore, but requires information that may not be systematically obtained by a firm, or if obtained, is more likely gathered through a firm's anti-money laundering (AML) efforts. Firms are actively exploring the sharing of information between the tax reporting and AML functions. However, incorporating AML information into a firm's tax system may not be feasible because tax reporting must be as "mechanical" as possible while AML programs require significant manual work to properly evaluate risk. In other words, an efficient tax reporting system must be highly automated and objective while an efficient AML system must be, at least partially, manual. A blended tax-AML regime would require an account-by-account and transfer-by-transfer analysis, which is very challenging given the overwhelming number of transactions that will have to be reported. If the committee chooses to rely on tax reporting as the mechanism for tracking funds transfers, we recommend using tax concepts and definitions to the greatest extent possible. This will help ensure the proposal can be implemented.
- Finally, it is worth noting that in October 2006, the Financial Crimes Enforcement Network (FinCEN) released a Congressionally-mandated report regarding the feasibility of reporting cross-border electronic funds transfers for purposes of combating money laundering and terrorist financing. The report found that such reporting requirements raise numerous policy considerations and pose extensive technical hurdles. The report notes:

"A significant concern is the cost, both to U.S. financial institutions and to the government, of implementing the reporting requirement and building the technological systems to manage and support the reporting. Related to these concerns are questions about the government's ability to use such data effectively. These concerns must be weighed carefully as we proceed. Another concern is the potential effect that any reporting requirement could have on dollar-based payment systems such as: (1) a shift away from the U.S. dollar toward other currencies (i.e., the Euro) as the basis for international financial transactions; (2) the creation of mechanisms and facilities for clearing dollar-based transactions outside the United States; and (3) interference with the operation of the central payments systems. The U.S. has economic and national security interests in the continued viability and vitality of dollar-based payments and these possible outcomes must inform and guide the rulemaking process."²

Ultimately, the project stalled and was never implemented. The Finance Committee proposal is even more complex than the proposal studied by FinCEN because it is broader in scope and would require financial institutions to make determinations about the nature and purpose of wire transfers.

² U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Feasibility of a Cross-Border Electronic Funds Transfer Reporting System Under the Bank Secrecy Act," October 2006.

Specific Issues and Recommendations

- **Annual Versus Transactional Reports** – Because of the very large volume of wire transfers, we recommend giving financial institutions the option of providing aggregated annual reports rather than transactional reports. If this option is elected, a financial institution would report the total dollar amount of wire transfers sent to a particular financial account outside the United States during the calendar year.
- **Reporting to Transferors** – It is unclear why the proposal requires reporting to the transferor since there is no requirement to match taxpayer and financial institution data on the transferor's tax return. It should be sufficient to notify the transferor that the information is being reported to the IRS. SIFMA believes the proposal will help deter tax avoidance if customers are informed that transfers will be reported to the IRS rather than if customers are provided with statements the year after the transfer has taken place. We believe the requirement to report to the transferor is unnecessary and should be dropped.
- **Definition of a "Financial Institution"** – The term "financial institution" is not defined in the proposal. As a result, it is unclear to whom the reporting responsibility applies. The definition of a financial institution should be broad enough to create a level playing field and to ensure the proposal achieves the intended tax compliance goals. As a result, the definition should not be limited to transferors who are brokers for purposes of Code section 6045. Rather, the definition should capture all entities in the United States that transfer funds outside the United States. Definitions of "financial institution" can be found in the USA PATRIOT Act and in Treasury regulation section 1.165-12(c)(iv). The Committee may want to consider these definitions as a starting point.

It is also unclear whether the reporting requirements are intended to apply to financial institutions located outside the United States (i.e., foreign financial institutions and foreign branches of US financial institutions). Imposing the reporting requirements on foreign financial institutions and branches would capture funds transferred from one foreign account to another (as opposed to capturing funds transferred out of the United States to a foreign account). We question whether this result is intended and note that the proposal's reporting requirements may conflict with the laws of the foreign country (e.g., data protection laws) in which the foreign branch or foreign financial institution operates.

- **Multiple Parties to Wire Transfers** – As written, the proposal would result in multiple financial institutions reporting on the same transfer. As a result, the proposal needs to clarify who is responsible for filing the information return when there are multiple financial institutions involved with a single wire transfer. For example, if a customer of a US broker-dealer requests that money be wired to an account located in a foreign country, the US broker-dealer will likely send the

instruction to a major bank to effect the wire transfer. It is unclear whether the broker-dealer or bank would be responsible for the information reporting. In another example, a wire transfer request made at a local bank might be executed by a money center bank because the local bank lacks the ability to send the wire directly to the foreign account. In both of these examples, duplicate reporting will occur unless it is made clear that only one financial institution is required to file an information return. We recommend the statute make clear that the originating financial institution has the responsibility to file the information return, and that an intermediary financial institution should not be responsible for reporting. The intermediary financial institution does not have a direct relationship with the requestor of the wire and may not know the tax status of the person who requested the money transfer.

- **Definition of a “Foreign Financial Account”** – The term “foreign financial account” is not defined in the Internal Revenue Code or in the Treasury regulations thereunder. Moreover, the Foreign Bank and Financial Accounts (FBAR) definition of a foreign financial account is overly broad and ambiguous. We recommend defining “foreign financial account” by focusing on those transfers which would be most useful to the IRS. For example, if the intended target is the movement of money by or on behalf of a US person to a foreign account, then the term could be defined to include only accounts at an offshore location but without regard to whether the owner of the account is a foreign person.
- **Definition of “Transfer”** – It is our understanding the term “transfer” is intended to capture funds transfers (i.e., wire transfers) to foreign accounts. However, as currently drafted, the term “transfer” could be interpreted as including any transaction that moves funds to a foreign account, such as checks, credit card payments, and debits. Such a broad definition would require collecting data from many different platforms and, then or subsequently, incorporating that data into a firm’s tax reporting system. This is an extraordinarily expensive and difficult task that could take years to implement. We recommend clarifying that the term “transfer” is limited to wire transfers.

Even as limited to wire transfers, the proposal would capture an overwhelming number of transactions – the very large majority of which would not be useful to the IRS. As a result, we recommend excluding from the reporting requirements payments reportable under another section of the Code. Moreover, financial institutions could be given the option to exclude common commercial transactions, such as:

1. proprietary transfers (i.e., transfers by a financial institution to its own foreign accounts or foreign accounts of affiliates),
2. payments under notional principal contracts,
3. payments of gross proceeds on the sale of securities through a C.O.D. account,
4. the making and repayment of money loans,

5

5. transfers of cash collateral,
6. payments made for goods and services, and
7. payments made to foreign clearing organizations (e.g., Euroclear and Clearstream).

The exclusion of these common commercial transactions should be optional because financial institutions may not know the purpose of the transfer.

Finally, it is unclear what is meant by "indirect" transfers. If this term is retained, it should be clarified to refer to transfers occurring through intermediary financial institutions (i.e., if there are one or more financial institutions between the originating financial institution and the foreign financial account).

- **Related Transactions.** The reporting requirements are triggered if transfers exceed more than \$10,000 "in 1 or 2 or more related transactions." The term "related transactions" is not defined, and it is unclear how it should be interpreted. Moreover, there is no time frame designated for aggregation purposes. Theoretically, related transactions could occur several months apart making aggregation impossible. We believe the "related transactions" requirement is unnecessary if institutions report all transfers from the same originating account to an account outside the United States on an annual aggregated basis.
- **Definition of "US Person"** – The definition of a "US person" needs to be clarified. For tax purposes, a US person would include a resident alien. Under the USA PATRIOT Act, a customer who is a US person must be a US citizen. We recommend following the tax definition of US person under Code section 7701(a)(30) because it is more closely aligned with current procedures for information reporting.

Moreover, financial institutions should be allowed to rely on Forms W-9 or W-8BEN for purposes of determining whether an accountholder is a US person. In the absence of a Form W-9 or W-8BEN, financial institutions would need presumptions (such as under Code section 1441) to make this determination. In addition, Treasury should be given authority to establish rules for making such a determination when an agent of the account owner requests a transfer. Financial institutions must be able to rely on information received from agents because obtaining information directly from the principal may not be possible. Examples of such agents include investment advisors, asset managers, introducing brokers, trustees and holders of a power of attorney.

- **Transfers "At the Direction Of, On Behalf Of, or For the Benefit Of" Customer Who Is A US Person** – The requirement to report transfers "at the direction of, on behalf of, or for the benefit of a customer who is a US person" raises several questions and issues that are discussed below.

6

- o The term “at the direction of” is overly broad and would capture any wire transfer initiated by a US investment advisor, US trustee or US holder of a power of attorney, even if the transaction is made on behalf of a foreign person. Reporting these transactions would result in massive amounts of information to the IRS that would not assist in detecting or deterring tax evasion. As a result, financial institutions should not be required to report transfers at the “direction” of an agent that is a US person unless the principal is also a US person.
- o For tax reporting purposes, the beneficial owner of an account is the accountholder (i.e., the registered name on the account), and beneficial or legal ownership is determined through Forms W-8BEN and W-9. In the absence of these forms, there are presumptions under Code section 1441 for identifying US accountholders. Accordingly, financial institutions can determine whether a transfer is made “for the benefit of or on behalf of” a customer who is a US person if tax definitions and concepts are adopted.

However, for tax reporting purposes, a financial institution cannot determine whether a transfer is made “for the benefit of or on behalf of” someone *other* than the accountholder. Firms can determine beneficial ownership information beyond the accountholder through their AML due diligence efforts. However, “US ownership” is not considered a common risk for AML purposes. As a result, many AML systems do not highlight or flag US ownership as its own identifiable risk classification. In other words, US ownership information is obtained and evaluated for risk at account opening. However, many firms cannot easily retrieve and provide this information for tax reporting purposes. Moreover, marrying a firm’s AML and tax reporting systems is very challenging at this time because the nature of AML reporting is highly individualized and manual. In contrast, tax reporting is inherently mechanical and automated due to the large volume of transactions that must be reported on an annual basis. Finally, even if the tax and AML systems could be married, beneficial ownership information may not be readily available at many firms for legacy accounts that were opened prior to enactment of the USA PATRIOT Act. Firms did not routinely collect ownership information prior to the PATRIOT Act because the information was not required.

Accordingly, we recommend applying the reporting requirements to “transfers originating from an account in the name of a US person.” In addition, we recommend excluding accounts for which reporting would not be useful to the IRS. Specifically, the reporting requirements should not apply to transfers originating from an account identified as a US “exempt recipient” as defined in regulations under Code section 6049 (relating to information reporting on Form 1099). This would have the effect of excluding transfers by or for the benefit of US tax-exempt organizations, other US banks, other US registered broker-dealers, US mutual funds, etc.





- **Withholding Obligations** – We assume that wire transfers are exempt from backup withholding requirements. Subjecting transfers to backup withholding would be illogical and would create significant taxpayer anger if payments to foreign accounts were reduced by 28 percent – particularly for taxpayers who are paying bills or making other necessary payments.
- **Effective Date** – The reporting of cross-border wire transfers is a massive undertaking that presents significant systems and operational challenges. Accordingly, the proposal's December 31 effective date is unrealistic. The industry will be in a better position to recommend a more realistic effective date once the scope and obligations of the proposal are clarified. We also note that much of the information requested by the proposal, such as determination of an account's beneficial owner, may not be contained within firms' tax reporting systems. Although this information could be requested on a prospective basis for new accounts, firms would need time to collect the information with respect to existing accounts. Even on a prospective basis for new accounts, financial institutions need time to develop systems and modify business practices to gather, store and report the additional information needed for wire transfer reporting.

We appreciate the opportunity to comment on this proposal and look forward to working with you on initiatives to improve offshore tax compliance. If you have any questions, please feel free to call me at 202-962-7300.

Best Regards,

 (b)(6)
 (b)(6)

Managing Director
 Securities Industry and Financial Markets Association

- cc:  Chief Tax Advisor, Committee on Finance Majority Staff
 Deputy Staff Director and Chief Tax Counsel, Committee on Finance Minority Staff
 Tax Counsel, Committee on Finance Majority Staff
 Tax Counsel, Committee on Finance Minority Staff

(b)(6)



SWIFTStandards

Comparison Table

pac.008.001.01 FIToFICustomerCreditTransferV01

MT 103 Core Single Customer Credit Transfer

Fedwire Customer Transfer (CTR)

CHIPS Non-Bank Transfer

The SWIFTStandards Comparison Table provides an overview of the semantic equivalence between the ISO pac.008.001.01, SWIFT MT 103, Fedwire Customer Transfer and CHIPS Non-Bank Transfer message standards.

17 April 2008

Related documentation

- *SWIFT User Handbook, SWIFTStandards MT, relevant Message Reference Guides*
- *UNIFI (ISO 20022) Message Definition Report - Payments Standards - Clearing and Settlement and related XML schemas and instances*

The latest version of the SWIFT Message Reference Guides is available at www.swift.com.

The latest version of the UNIFI documentation is published on the www.iso20022.org website.

Legal Notices

Copyright

Copyright © S.W.I.F.T. SCRL ("SWIFT"), avenue Adèle 1, B-1310 La Hulpe, Belgium, 2008, or its licensors. All rights reserved. You may copy this publication within your organisation. Any such copy must include these legal notices.

Disclaimer

SWIFT supplies this publication for information purposes only, without any express or implied warranties as to its completeness, fitness for a particular purpose, frequency of updates, or absence of errors. The information in this publication may change from time to time. You must always refer to the latest available version.

Limitation of Liability

SWIFT excludes its liability for any damages (whether direct, indirect, special or consequential damages) caused by the use of the Comparison Tables.

Trademarks

SWIFT, S.W.I.F.T., the SWIFT logo, Sibos, SWIFTNet, SWIFTAlliance, SWIFTStandards, SWIFTReady, and Accord are trademarks of S.W.I.F.T. SCRL. Other SWIFT-derived service and product names, including SWIFTSolutions, SWIFTWatch, and SWIFTSupport, are tradenames of S.W.I.F.T. SCRL. SWIFT is the trading name of S.W.I.F.T. SCRL. Other product or company names in this publication are tradenames, trademarks, or registered trademarks of their respective owners.

	A	B	C	D	E	F	G	H	I
1	pacs.008.001.01 FIToFICustomer CreditTransferV01					MT 103 Core Single Customer Credit Transfer	Fedwire CTR	CHIPS Non-Bank	Comment
2	GroupHeader								
3	MessageIdentification					:20: Sender's Reference	{1520} IMAD	[320] Send Participant Reference	
4	CreationDateTime					-	-	-	
5	BatchBooking					-	-	-	
6	NumberOfTransactions					-	-	-	MT 103 and Fedwire/CHIPS CTR are single transaction messages.
7	ControlSum					-	-	-	
8	TotalInterbankSettlementAmount					:32A: Value Date/Currency/Interbank Settled Amount Subfield 2: Currency Subfield 3: Interbank Settled Amount	{2000} Amount Currency USD implicit	[260] Amount Currency USD implicit	With NumberOfTransactions equal to 1, TotalInterbankSettlementAmount is equal to the InterbankSettlementAmount.
9	InterbankSettlementDate					:32A: Value Date/Currency/Interbank Settled Amount Subfield 1: Value Date	{1520} IMAD First 8 characters	[201] Identification Tag Element 2: Value Date	
10	SettlementInformation								
11	SettlementMethod								The MT 103 allows for all settlement methods (albeit implicit). For CHIPS and Fedwire, the settlement method is CLRG.
12	CLRG					-	-	-	
13	COVF					-	-	-	
14	INDA					-	-	-	
15	INGA					-	-	-	
16	SettlementAccount					:53a: Option B Sender's Correspondent Subfield 1: PartyIdentifier			
17	ClearingSystem					-	-	-	The message is sent across the Fedwire or CHIPS system, so transparent.
18	InstructingReimbursementAgent					:53a: Option A, B or D Sender's Correspondent Subfield 2: BIC, Location or Name&Address.			
19	InstructingReimbursementAgentAccount					:53a: Option A, B or D Sender's Correspondent Subfield 1: PartyIdentifier			

	A	B	C	D	E	F	G	H	I
1	MX pacs.008.001.01 FIToFICustomerCreditTransferV01					MT 103 Core Single Customer Credit Transfer	Fedwire CTR	CHIPS Non-Bank	Comment
20	InstructedReimbursementAgent					:54a: Option A, B or D Receiver's Correspondent Subfield 2: BIC, Location or Name&Address	-	-	
21	InstructedReimbursementAgentAccount					:54a: Option A, B or D Receiver's Correspondent Subfield 1: PartyIdentifier	-	-	
22	ThirdReimbursementAgent					:55a: Option A, B or D Third Reimbursement Institution Subfield 2: BIC, Location or Name&Address	-	-	
23	ThirdReimbursementAgentAccount					:55a: Option A, B or D Third Reimbursement Institution Subfield 1: PartyIdentifier	-	-	
24	PaymentTypeInformation								
25	InstructionPriority					-	-	-	
26	ServiceLevel								
27	Code								
28	PRPT					-	-	-	
29	SEPA					-	-	-	
30	SDVA					:23E: Instruction Code Subfield 1: Instruction = SDVA			
31	Proprietary					-	-	-	
32	ClearingChannel								
33	BOOK					-	-	-	
34	MPNS					-	-	-	
35	RTGS					//RT in Subfield 1 of first party field present (:56a: Intermediary Institution or :57a: Account With Institution)	Default for Fedwire as RTGS system		
36	RTNS					-		Default for CHIPS as RTNS system	
37	LocalInstrument					-	{3600} Business Function Code		
38	CategoryPurpose								

21

	A	B	C	D	E	F	G	H	I
1	pacs.008.001.01 FIToFICustomer CreditTransferV01					MT 103 Core Single Customer Credit Transfer	Fedwire CTR	CHIPS Non-Bank	Comment
39				INTC		:23E: Instruction Code Subfield 1: Instruction = INTC	-	-	
40				CORT		:23E: Instruction Code Subfield 1: Instruction = CORT	-	-	
41				CASH		-	-	-	
42				DIVI		-	-	-	
43				GOVT		-	-	-	
44				HEDG		-	-	-	
45				INTE		-	-	-	
46				LOAN		-	-	-	
47				PENS		-	-	-	
48				SALA		-	-	-	
49				SECU		-	-	-	
50				SSBE		-	-	-	
51				SUPP		-	-	-	
52				TAXS		-	-	-	
53				TRAD		-	-	-	
54				TREA		-	-	-	
55				VATX		-	-	-	
56				WHLD		-	-	-	
57	InstructingAgent					MT Sender	{3100} Sender FI	[201] Identification Tag Element 3: Send Participant	
58	InstructedAgent					MT Receiver	{3400} Receiver FI	[211] Disposition Tag Element 1: Receive Participant	
59	Credit Transfer Transaction Information								
60	Payment Identification								
61	InstructionIdentification					:20: Sender's Reference	{3320} Sender Reference Number	[320] Send Participant Reference	
62	EndToEndIdentification					:70: Remittance Information Code: ROC	{4320} Reference for Beneficiary		
63	TransactionIdentification					-	-	-	

13

	A	B	C	D	E	F	G	H	I
1	MX pacs.008.001.01 FIToFICustomerCreditTransferV01					MT 103 Core Single Customer Credit Transfer	TR	CHIPS Non-Bank	Comment
64	PaymentTypeInformation								
65	InstructionPriority					-	-	-	
66	ServiceLevel								
67	Code								
68	PPPr					-	-	-	
69	SDPA					-	-	-	
	SDVA					:23E: Instruction Code			
70						Subfield 1: Instruction = SDVA			
71	Proprietary					-	-	-	
72	ClearingChannel								
73	BOOK					-	-	-	
74	MPNS					-	-	-	
	RTGS					//RT in Subfield 1 of first party field present (:56a: Intermediary Institution or :57a: Account With Institution)	Default for Fedwire as RTGS system		
75									
	RTNS					-	-	-	Default for CHIPS as RTNS system
76									
77	LocalInstrument					-	{3600}	-	Business Function Code
78	CategoryPurpose								
	INTC					:23E: Instruction Code			
79						Subfield 1: Instruction = INTC			
	CORT					:23E: Instruction Code			
80						Subfield 1: Instruction = CORT			
81	CASH					-	-	-	
82	DIVI					-	-	-	
83	GOVT					-	-	-	
84	HEDG					-	-	-	
85	INTE					-	-	-	
86	LOAN					-	-	-	
87	PENS					-	-	-	
88	SALA					-	-	-	
89	SECU					-	-	-	
90	SSBE					-	-	-	

4

	A	B	C	D	E	F	G	H	I
	pacs.008.001.01 FI To FI Customer Credit Transfer V01					MT 103 Core Single Customer Credit Transfer	Fedwire CTR	CHIPS Non-Bank	Comment
1									
91				SUPP	-	-	-	-	
92				TAXS	-	-	-	-	
93				TRAD	-	-	-	-	
94				TREA	-	-	-	-	
95				VATX	-	-	-	-	
96				WHLD	-	-	-	-	
97	InterbankSettlementAmount					:32A: Value Date/Currency/Interbank Settled Amount Subfield 2: Currency Subfield 3: Interbank Settled Amount	{2000} Amount Currency USD implicit	[260] Amount Currency USD implicit	
98	InterbankSettlementDate					:32A: Value Date/Currency/Interbank Settled Amount Subfield 1: Value Date	{1520} IMAD First 8 characters	[201] Identification Tag Element 2: Value Date	
99	SettlementTimeIndication								
100	DebitDateTime					:13C: Time Indication Code: SNDTIME			
101	CreditDateTime					:13C: Time Indication Code: RNCTIME			
102	SettlementTimeRequest								
103	CLSTime					:13C: Time Indication Code: CLSTIME			
104	AcceptanceDateTime								
105	PoolingAdjustmentDate								
106	InstructedAmount					:33B: Currency/Instructed Amount	{3710} Instructed Amount	[301] Charges Information Element 2: Instructed Amount	

15

	A	B	C	D	E	F	G	H	I
1	MX pacs.008.001.01 FIToFICustomer CreditTransferV01			MT 103 Core Single Customer Credit Transfer		Fedwire CTR	CHIPS Non-Bank	Comment	
107	ExchangeRate			:36: Exchange Rate	{3720} Exchange Rate	[301] Charges Information	Element 3: Exchange Rate		
108	ChargeBearer								
109			DEBT	:71A: Details of Charges					
				Code: OUR					
110			CRED	:71A: Details of Charges	{3700} Charges	[301] Charges Information	Element 1: Details of Charges (Code = 1)		
				Code: BEN	Details of Charges: B				
111			SHAR	:71A: Details of Charges	{3700} Charges	[301] Charges Information	Element 1: Details of Charges (Code = 2)		
				Code: SHA	Details of Charges: S				
112			SLEV	-	-	-	-		
113	ChargesInformation								
114	ChargesAmount			:71F: Sender's Charges (:71A: with code "BEN" or "SHA") or :71G: Receiver's Charges (:71A: with code "OUR")	{3700} Charges Currency Code Sender's Charges	[301] Charges Information	Element 4, 6, 8 or 10: Sending Charges		
115	ChargesParty							In the MT 103, Fedwire and CHIPS CTR the financial institution that has taken charges or to which charges are due is implicit to the payment chain and can within certain limits be understood from that payment chain.	
116	PreviousInstructingAgent			:72: Sender to Receiver Information Code: INS	{5200} Instructing FI	[520] or [522] Instructing Bank			

16

	A	B	C	D	E	F	G	H	I
1	pacs:008 FIToFICu Credit Tran					MT 103 Core Single Customer Credit Transfer	Fedwire CTR	CHIPS Non-Bank	Comment
117	PreviousInstructing Account				-		{5200} Instructing FI ID-Code: D	[522] Instructing Bank ID-Code: D	
118	InstructingAgent				MT Sender		{3100} Sender FI	[201] Identification Tag Element 3: Send Participant	
119	InstructedAgent				MT Receiver		{3400} Receiver FI	[211] Disposition Tag Element 1: Receive Participant	
120	IntermediaryAgent1				:56a: Option A, B, C or D Intermediary Institution Subfield 2: BIC, Location or Name&Address		{4000} Intermediary FI	[400] or [401] or [402] Intermediary Bank	
121	IntermediaryAgent1Account				:56a: Option A, B, C or D Intermediary Institution Subfield 1: PartyIdentifier		{4000} Intermediary FI ID-Code: D or U	[402] Intermediary Bank ID-Code: D or U	
122	IntermediaryAgent2				-		-	-	
123	IntermediaryAgent2Account				-		-	-	
124	IntermediaryAgent3				-		-	-	
125	IntermediaryAgent3Account				-		-	-	
126	UltimateDebtor				-		-	-	
127	InitiatingParty				-		-	-	
128	Debtor				:50a: Option A, F or K Ordering Customer Subfield 2: BICBEI or Name&Address		{5000} Originator	[500] or [502] Originator Information	
129	DebtorAccount				:50a: Option A, F or K Ordering Customer Subfield 1: Account		{5000} Originator ID-Code: D, T or U	[502] Originator Information ID-Code: D	
130	DebtorAgent				:52a: Option A or D Ordering Institution Subfield 2: BIC or Name&Address		{5100} Originator's FI	[510] or [512] Originator's Bank	

	A	B	C	D	E	F	G	H	I
1	MX pacs.008.001.01 FIToFICustomer CreditTransferV01					MT 103 Core Single Customer Credit Transfer	Fedwire CTR	CHIPS Non-Bank	Comment
131	DebtorAgentAccount					:52a: Option A or D Ordering Institution Subfield 1: PartyIdentifier	{5100} Originator's FI ID-Code: D or U	[512] Originator's Bank ID-Code: D or U	
132	CreditorAgent					:57a: Option A, B, C or D Account With Institution Subfield 2: BIC, Location or Name&Address	{4100} Beneficiary's FI	[410] or [411] or [412] Beneficiary's Bank	
133	CreditorAgentAccount					:57a: Option A, B, C or D Account With Institution Subfield 1: PartyIdentifier	{4100} Beneficiary's FI ID-Code: D or U	[412] Beneficiary's Bank ID-Code: D or U	
134	Creditor					:59a: Option A or No letter Beneficiary Customer Subfield 2: BICBEI or Name&Address	{4200} Beneficiary	[420] or [421] or [422] Beneficiary Information	
135	CreditorAccount					:59a: Option A or No letter Beneficiary Customer Subfield 1: Account	{4200} Beneficiary ID-Code: D, T or U	[422] Beneficiary Information ID-Code: D, T or U	
136	UltimateCreditor					-	-	-	
137	InstructionForCreditorAgent								
138	Code								
139			CHQB			:23E: Instruction Code Subfield 1: Instruction = CHQB	{6420} Method of Payment to Beneficiary Method of Payment Code: CHECK	[641] Beneficiary Advice Information Advice Code: Q	
140			HOLD			:23E: Instruction Code Subfield 1: Instruction = HOLD	{6410} Beneficiary Advice Information Advice Code: HLD	[641] Beneficiary Advice Information Advice Code: H	
141			PHOB			:23E: Instruction Code Subfield 1: Instruction = PHOB	{6410} Beneficiary Advice Information Advice Code: PHN	[641] Beneficiary Advice Information Advice Code: P	

18

	A	B	C	D	E	F	G	H	I
1	pacs.008.001.01 FIToFICustomer CreditTransferV01					MT 103 Core Single Customer Credit Transfer	FedWire CTR	CHIPS Non-Bank	Comment
142			TELB			:23E: Instruction Code Subfield 1: Instruction = TELB	{6410} Beneficiary Advice Information Advice Code: LTR, TLX or WRE	{641} Beneficiary Advice Information Advice Code: C	
143		InstructionInformation				:23E: Instruction Code Subfield 2: Additional Information (and Subfield 1: Instruction is "HOLD", "PHOB" or "TELB")	{6410} Beneficiary Advice Information Advice Information (and Advice Code = CHECK, HLD, PHN, LTR, TLX or WRE)	{641} Beneficiary Advice Information Advice Information (and Advice Code = Q, H, P or C)	
144						:72: Sender to Receiver Information Code: ACC	{6400} Beneficiary's Information	{640} Beneficiary's Bank Advice Information	
145	InstructionForNextAgent								
146		Code	PHOA						
147						:23E: Instruction Code Subfield 1: Instruction = PHOI	{6210} Intermediary FI Advice Information Advice Code: P, IN	{621} Intermediary Bank Advice Information Advice Code: P	
148						:23E: Instruction Code Subfield 1: Instruction = PHON	{6310} Beneficiary's FI Advice Information Advice Code: PHN	{631} Beneficiary's Bank Advice Information Advice Code: P	
149			TELA			:23E: Instruction Code Subfield 1: Instruction = TELI	{6210} Intermediary FI Advice Information Advice Code: LTR, TLX or WRE	{621} Intermediary Bank Advice Information Advice Code: C	
150						:23E: Instruction Code Subfield 1: Instruction = TELE	{6310} Beneficiary's FI Advice Information Advice Code: LTR, TLX or WRE	{631} Beneficiary's Bank Advice Information Advice Code: C	

19

	A	B	C	D	E	F	G	H	I
1	pacs.008.001.01 FIToFICustomer CreditTransferV01					MT 103 Core Single Customer Credit Transfer	Fedwire CTR	CHIPS Non-Bank	Comment
151	Instruction Information					:23E: Instruction Code Subfield 2: Additional Information (and Subfield 1: Instruction is "PHOI" or "TELI")	{6210} Intermediary FI Advice Information Advice Information (and Advice Code = PHN, LTR, TLX or WRE)	[621] Intermediary Bank Advice Information Advice Information (and Advice Code = P or C)	
152						:23E: Instruction Code Subfield 2: Additional Information (and Subfield 1: Instruction is "PHON" or "TELE")	{6310} Beneficiary's FI Advice Information Advice Information (and Advice Code = PHN, LTR, TLX or WRE)	[631] Beneficiary's Bank Advice Information Advice Information (and Advice Code = P or C)	
153						:72: Sender to Receiver Information Code: REC	{6100} Receiver FI Information or {6500} FI to FI Information	[610] Receive Bank Advice Information or [650] General Advice Information	
154						Purpose	-	-	-
155	Regulatory Reporting					:77B: Regulatory Reporting	-	-	
156	Related Remittance Information					-	-	-	
157	Remittance Information					:70: Remittance Information	{6000} Originator to Beneficiary Information	[600] Originator to Beneficiary Information	

02

Submitted Updated 6 July 2007

Country	Wire Transfer In	Volumes In	Wire transfers Out	Volumes Out
Albania				
Andorra				
Anguilla				
Antigua and Barbuda				
Argentina	Yes	No figures	Yes	No figures
Aruba	No	-	No	-
Australia	Yes	~4.9m	Yes	~7.1m
Austria	No	-	No	-
Bahamas	No	-	No	-
Bahrain	Yes	23	Yes	4
Barbados				
Belgium	No	-	No	-
Bermuda	No	-	No	-
Bolivia	No	-	No	-
Bosnia-Herzegovina	Yes	No figures	Yes	No figures
Brazil				
British Virgin Islands	Yes	2	No	-
Bulgaria	No	-	No	-
Canada	Yes	9,000,000 (both in & out)	Yes	9,000,000 (both in & out)
Cayman Islands	No	-	No	-
Chile	No	-	No	-
Colombia	Submitted	Submitted	Submitted	Submitted
Cook Islands	Yes	8337 (both in & out - July 2003)	Yes	8337 (both in & out - July 2003)
Costa Rica				

Croatia	Yes	No figures	Yes	No figures
Cyprus	No	-	No	-
Czech Republic				
Denmark	No	-	No	-
Dominica	Yes	5	Yes -	5
Dominican Republic				
Egypt				
El Salvador				
Estonia	No	-	No	-
Finland	Yes	No figures	Yes	No figures
France	No	-	No	-
Gibraltar				
Germany	Yes	5192	Yes	13694
Greece				
Guatemala	No	-	No	-
Guernsey	No	-	No	-
Honduras				
Hong Kong	Yes	No figures	Yes	No figures
Hungary				
Iceland				
Indonesia	No	-	No	-
Ireland	No	-	No	-
Isle of Man	No	-	No	-
Israel	Yes	46,623	Yes	25,831
Italy	Yes	1800 billion Euros	Yes	2200 billion Euros
Japan	No	-	No	-
Jersey	No	-	No	-
Korea (Republic of)				

Latvia	No	-	No	-
Lebanon	No	-	No	-
Liechtenstein	No (Only if suspect)		No (Only if suspect)	-
Lithuania	Yes	No figures	Yes	No figures
Luxembourg	No	-	No	-
Macedonia	No	-	No	-
Malaysia	No	-	No	-
Malta				
Marshall Islands				
Mauritius	Yes	No figures	No	-
Mexico	Yes	Recently included for banks- no details yet	Yes	Recently included for banks- no details yet
Monaco	No	-	No	-
Montenegro				
Netherlands				
Netherlands Antilles	Yes	2336	Yes	-
New Zealand	No	-	No	-
Norway	Yes	No figures	Yes	No figures
Panama	No	-	No	-
Paraguay				
Peru	No	-	No	-
Philippines	Yes	337,186	Yes	456,365
Poland	No	-	No	-
Portugal				
Qatar	No	-	No	-
Romania	Yes	No figures	Yes	No figures
Russia	Yes	No figures	Yes	No figures
San Marino	No	-	No	-

Serbia	No	-	No	-
Singapore	No	-	No	-
Slovakia				
Slovenia				
South Africa	Yes	No figures	Yes	No figures
Spain				
St Kitts & Nevis				
St Vincent & the Grenadines	Yes	60	Yes	10
Sweden				
Switzerland	No	-	No	-
Taiwan	No	-	No	-
Thailand				
Turkey				
Ukraine	Yes	4322	Yes	8784
United Arab Emirates				
United Kingdom	No	-	No	-
United States	No	-	No	-
Vanuatu				
Venezuela				

(b)(5)

[Redacted]

(1) Q: How long must FIs keep funds transfer records under 1033.33?

A: See 31 CFR 103.33(d) – not to exceed five years – but the rule refers to 103.26 relating to orders by the Secretary calling for additional recordkeeping or reports

(b)(5)

[Redacted] for retaining records/reports in the BSA - see also 103.18(d) [DI SAR]; 103.29(c) [purchase of monetary instruments \$3,000 - \$10,000]; 103.121(b)(3)(ii) [CIP].

[Redacted]

(b)(5)

FFIEC Banks Secrecy AML Examination Manual states that records must be maintained for five years. The reference is made with respect to originator banks

[Redacted]

(b)(5)

In SR VII, (Role of the Intermediary Financial institution – #13), if an intermediary institution is unable to pass on domestically (technical difficulties) all the originator information it received from a cross-border wire, the intermediary institution must retain the information it received for five years. See SR VII link below.

(2) Q: Which FATF SR relates to threshold?

A: Revised Interpretive Note to SR VII says that due to the potential terrorist financing posed by small wire transfers, countries should aim for the ability to trace all wire transfers and should minimize thresholds without driving such transactions underground. The interpretive note says that countries may adopt a de minimus threshold not above \$1,000 US or Euros. FATF recognizes that it will take time to make the necessary regulatory changes to the threshold but represents that the period should not extend beyond December 2006.

<http://www.fatf-gafi.org/dataoecd/34/56/35002635.pdf>

(3) Q: What is the interplay with the Travel Rule and SR VII?

A: SR VII aims to ensure that basic information on the originator of wire transfers is immediately available to appropriate law enforcement, FIUs, and beneficiary financial institution. This is the same aim of our Travel Rule. SR VII represents that cross-border wire transfers should be accompanied by accurate, meaningful originator information.

The information that must travel (“complete originator information”) under SR VII includes:

- Name of the originator
- Account # if there is one, or a unique reference #

25

- Address or national identity number or customer identification number or date or place of birth

For wire transfers below threshold, although countries are not obligated to, they may nevertheless require incoming cross-border wire transfers to contain full and accurate originator information.

[REDACTED] (b)(5)

Beneficiary Institution – No Travel Rule duties

SR VII states that beneficiary institutions should have effective procedures in place to identify incoming wires with incomplete originator information.

[REDACTED] (b)(5)

SR VII relies on enforcement mechanisms and decisions to sever business relationships to weed out non-complying institutions.

Threshold (Level)

[REDACTED] (see 09/06). Points presented by the commenters were:

- o Lowering or eliminating the \$3,000 threshold would increase industry burden, especially for smaller institutions without automated systems.
- o The Advance Notice does not sufficiently articulate the benefits to law enforcement to justify the burden to the industry.
- o The Advance Notice does not sufficiently detail why the current threshold is inadequate for law enforcement or how it hinders investigations.
- o Law enforcement is overburdened with the current volume of BSA data and would likely not have the resources to investigate increases in records.
- o The proposal could drive wire transfer transactions to unregulated sectors causing a lack of transparency. Especially with respect to MSBs, the proposal would likely affect those that need the services the most – the immigrant population making low value transfers.
- o Since the threshold has not been adjusted in over ten years, it has already been lowered by inflation.
- o In practice, many banking and non-banking financial institutions are already collecting originator information on wire transfers below the threshold. However, many still anticipate increased operational and other costs.
- o Many are concerned that a reporting requirement for wires is imminent and strongly oppose such a reporting requirement, especially for an expanded volume of transactions that would result from lowering or eliminating the current recordkeeping threshold.

- The Feasibility Study presented by FinCEN to Congress on October 2006 concludes that “the basic information already obtained and maintained by US financial institutions pursuant to the Funds Transfer Rule, including the \$3,000 recordkeeping threshold (emphasis added), provides sufficient basis for meaningful analysis”.
- Appendix H and Appendix J to the report, which list the hardware and software requirements and provide a preliminary work breakdown schedule and labor and hardware cost (@\$17MM and @6MM, respectively), were calculated based on a volume of transactions reported at the \$3,000 threshold.
- The March 2006 Notice and Request for Comments issued by FinCEN to obtain background information about the collection of data on CBWT also took the \$3,000 threshold as baseline. Only one aspect of one question (out of 15 contained in the request) asked banks to determine if the costs involved would vary significantly if the threshold was increased to \$10,000, or eliminated altogether. Only one out of the three answer letters published with the Feasibility Study addresses a potential threshold change directly: the ABA letter stated that “... thresholds – as long as there are no aggregation requirements – are not particularly complicating system wise ...”.

[REDACTED]

(b)(5)

(b)(5)

[REDACTED]

There were no answers from MSBs published with the Feasibility Study.
o The November 2007 CBWT survey distributed to @300 financial institutions, which registered @80 answers, stated that the threshold and content of the information to be reported were identical to the recordkeeping requirements; all the volume and reporting cost information surveyed was collected based on a \$3,000 reporting threshold.

[REDACTED]

[REDACTED]

(b)(5)

[REDACTED]

[REDACTED]

Threshold (effect of reduction on Executive Order 12866 certification)

- o Based upon the potential reporting requirement as described for the survey, the responding depository institutions indicated that they would need to report data on about one of every five of the electronic funds transfers they process within the United States.
- o Further, these depository institutions indicated that including all cross-border electronic funds transmittals valued at less than \$3,000 would increase the total to approximately one in every three electronic funds transfers processed in the United States and would therefore increase their costs of reporting
- o The responding money transmitters indicated that they would need to report data on about one in every 100 of all the electronic funds transmittals they process within the

[REDACTED]

United States. These money transmitters indicated, however, that including all cross-border electronic funds transmittals valued at less than \$3,000 would significantly increase the total number reportable and therefore could significantly increase their costs.

- The next largest group of respondents noted that international CBFT business currently conducted in the United States could move away from the use of the U.S. dollar to another currency, increase the use of cover payments, or create other competitive disadvantages. (29 respondents)
- Customers may move to an alternative method for conducting transactions, such as an informal fund transfer systems, which could reduce revenues for the financial institution. (12 respondents)
- Processing of fund transfers could be slowed, the overall efficiency of the U.S. payments system could be diminished, and costs to customers could increase. (12 respondents)

[REDACTED]

(b)(5)

Exemption for proprietary systems:

- According to information obtained during the survey, most/all money transmitters use proprietary systems to process individual transactions, and use the banking system to settle the net amounts owed to/owed by the individual agents for the global amounts processed.

[REDACTED]

(b)(5)

Message vs. payment:

[REDACTED]

(b)(5)

Types of CBWT to report

- There was consensus about exempting from the first stage CBWT such as those performed through intra-book movements (simultaneous credits and debits of customers' accounts).

[REDACTED]

(b)(5)

Definition of transmittal of funds subject to reporting/recordkeeping

- The current Funds Transfer Rule exempts from recordkeeping those transfers effected through systems subject to the Electronic Funds Transfer Act, funds made through an automated clearing-house, an automated teller machine, or a point-of-sale system, as these are not included in the definition of 'transmittal of funds'.

[REDACTED]

[REDACTED]

(b)(5)

[REDACTED]

(b)(5)

[REDACTED]

(b)(5)

[REDACTED]

(b)(5)

FinCEN, in consultation with Claes-Farnell International, conducted a study of the implications and benefits of the first reporting requirement. [REDACTED]

(b)(5)

The study determined the following:

- The individual average estimated cost of implementing the CBETF periodic report would consist of \$93,500 per year for large banks, and \$12,000 for small banks.
- The proposal will impact 300 banks (2% of all banks); including 110 large banks and 190 small banks (1.5% of small banks).
- The average estimated cost of implementing the CBETF-periodic report for large money transmitters would be 300,000 for the first year and 50,000 each following year.
- The average cost of implementing the CBETF-periodic report for small money transmitters would be \$20,000 per year.
- The proposal will impact 700 money transmitters (4% of all money transmitters); including 6 large money transmitters and 694 small money transmitters (4% of small money transmitters).
- Total impact of the first proposal will be \$28,245,000 for the first year and \$26,757,000 for each following year.

[REDACTED]

[REDACTED]

(b)(5)

(b)(5)

MEMORANDUM FOR [REDACTED] (b)(5)(b)

FROM: (b)(6) [REDACTED]

SUBJECT: *Comment Summary – Joint Advance Notice of Proposed Rulemaking Reviewing the \$3,000 Wire Threshold*

In June 2006, the Board of Governors of the Federal Reserve System (“Board”) and FinCEN (collectively, the “Agencies”) published a joint advance notice of proposed rulemaking (“Advance Notice”) regarding the \$3,000 threshold that triggers a recordkeeping requirement for certain financial institutions engaging in wire transfers. See 71 FR 35564 (June 21, 2006). Specifically, 31 C.F.R. § 103.33 requires banks and nonbank financial institutions to collect, retain, and transmit certain information on funds transfers and transmittals of funds in amounts of \$3,000 or more. This memorandum provides a short background of the Advance Notice, summarizes the comments received,

[REDACTED] (b)(5)

I. Background

The Advance Notice proposes lowering the threshold or eliminating the threshold altogether, which would be consistent with recent revisions to the Financial Action Task Force (“FATF”) recommendation on wire transfers.¹ Prior to publishing the Advance Notice, the Agencies sought input from law enforcement on the effect of lowering or eliminating the current threshold. FinCEN requested anecdotal evidence from law enforcement regarding whether the financial institutions’ collection of additional originator information on wire transfers in amounts under the \$3,000 would prove useful to law enforcement. The intent was for the Agencies to provide a preliminary justification to industry for the proposal. The Advance Notice includes a section, *Benefit to Law Enforcement*, which is based on the input we received. In addition, the Agencies asked more pointed questions of law enforcement in the Advance Notice seeking more

¹ See Revised Interpretative Note to Special Recommendation VII: Wire Transfers (June 10, 2005) (FATF recommends a de minimis threshold of no higher than \$1,000). FATF is an international, inter-governmental body that seeks to promote international policies to combat money laundering and terrorist financing. Special Recommendation VII (“SR VII”) addresses the complete and accurate originator information on international funds transfers and related messages.

(b)(5)(c)

comprehensive information on the benefits of greater access to records on wire transfers in low dollar amounts, specifically wire transfers below the current \$3,000 threshold.

II. Summary of Comments

The comment period closed on August 21, 2006. To date, the Agencies have received 36 comment letters, none of which were from law enforcement. The majority of the commenters opposed lowering and eliminating the current threshold. Of the comment letters, 15 were from depository institutions, 15 from financial institutions trade or other associations (consisting of national and state banking associations, national credit union associations, clearing house, money transmitter associations, and a money services businesses ("MSB") association), 3 from money transmitters, 2 from individuals, and 1 from a financial privacy research center.

The prevailing concerns and comments regarding the proposal are as follows:

- Lowering or eliminating the \$3,000 threshold would increase industry burden, especially for smaller institutions without automated systems.
- The Advance Notice does not sufficiently articulate the benefits to law enforcement to justify the burden to the industry.
- The Advance Notice does not sufficiently detail why the current threshold is inadequate for law enforcement or how it hinders investigations.
- Law enforcement is overburdened with the current volume of BSA data and would likely not have the resources to investigate increases in records.
- The proposal could drive wire transfer transactions to unregulated sectors causing a lack of transparency. Especially with respect to MSBs, the proposal would likely affect those that need the services the most – the immigrant population making low value transfers.
- Since the threshold has not been adjusted in over ten years, it has already been lowered by inflation.
- In practice, many banking and non-banking financial institutions are already collecting originator information on wire transfers below the threshold. However, many still anticipate increased operational and other costs.
- Many are concerned that a reporting requirement for wires is imminent and strongly oppose such a reporting requirement, especially for an expanded volume of transactions that would result from lowering or eliminating the current recordkeeping threshold.

(b)(5)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(b)(5)

MEMORANDUM FOR

[REDACTED]

(b)(6) (b)(6)
Page 4

[REDACTED]

(b)(5)

[REDACTED]

Comment Summary

Lowering or Eliminating the Current \$3,000 Wire Threshold Recordkeeping Requirement (31 C.F.R. 103.33)

Joint Advance Notice of Proposed Rulemaking - 71 FR 35564 (June 21, 2006)

Name of the Commenter	Oppose	Does Not Oppose	Comments
Amarillo National Bank [Texas]	Yes		<ul style="list-style-type: none"> -Originate/receive about 275 wires daily for established customers -4% b/w \$2,000 - \$3,000 -5.5% b/w \$1,000 - \$2,000 -14% are less than \$1,000 -Require same ID & collect same information for all wires -Lowering/eliminating - wld not affect operations, price or service -Proposal appears to be a shotgun approach -Better to have focused requests
American Bankers Association [The largest banking trade association in the country]	No need to change regs but – prefer lowering recordkeeping rqmt to CBWT reporting rqmt		<ul style="list-style-type: none"> -Many banks already collect info that satisfies the proposal -burden to small banks -FATF SR VII – limited to CBWT – not domestic transfers -oppose <u>reporting</u> rqmt
America's Community Bankers [National trade association for community banks]		As long as: (1) any change meets "high degree of usefulness" (2) FI's have time to comply	<ul style="list-style-type: none"> -Many banks already collect info that satisfies the proposal -Oppose CBWT <u>reporting</u> rqmt -Need 1 yr. to comply
Boyle, Eric [relative of a founding father]	Yes		<ul style="list-style-type: none"> -Will violate privacy rights -Will increase cost of services -Will permit circumventing due process
California Bankers Association [Non-profit organization representing depository FIs in California]	Yes		<ul style="list-style-type: none"> -Threshold should be raised not lowered -Wants more info on usefulness to LE -Wld increase cost of service & limit availability of wire service

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Name of the Commenter	Oppose	Does Not Oppose	Comments
Center for Financial Privacy and Human Rights [Public interest research center]	Yes		-Drive business underground -Loss of financial privacy & services -Insufficient justification - Questions need by LE
Citizens Bank (TX) 2 comments: (1) Carol Simmons (2) Ellen Shankles	Yes		-“NO, NO, NO” -Unnecessary, additional burden and expense
The Clearing House [Conglomerate of banks that provide payment services world-wide] *comment dated 9/8/06		Supports eliminating the threshold altogether – easier than 2 different standards	-if banks have automated systems that comply with the wire rules regardless of dollar amount, no additional burden to reduce or eliminate the threshold
Commerce Bancshares, Inc. [bank holding company with 3 subsidiaries]		Does not anticipate an increased burden	-Prefers eliminating to lowering- wld have to train staff on new threshold -Collects info even on wires below current threshold -Lowering/eliminating – wld not affect the price or type of service -Majority of wires – below threshold
Commerce Bank Harrisburg	Yes		-May drive transactions underground -Wld overburden LE & lead to defensive SAR filing -95% of wires below threshold -Costly to monitor new thresh
Commerce Bank (Mt. Laurel, NJ)	Yes		-Will cause further structuring -\$ will shift out of regulated sector – go underground -Unlikely LE will have resources to investigate increase in records and SARS
Community Bank of Georgia (Baxley, GA)	Yes		-Wld not increase effectiveness to LE -big burden for a small bank

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Name of the Commenter	Oppose	Does Not Oppose	Comments
Credit Union National Association (CUNA) [Represents about 90% of the state and federal credit unions]	Yes		<ul style="list-style-type: none"> -oppose any new <u>reporting</u> reqmt (including CI VT—esp. real-time) -review burden vs. benefit – insufficient justification -may not impact price/services -Approx. 40%-50% below \$3,000 -Approx. 30%-40% below \$2,000 -Approx. 20%-30% below \$1,000 -Wires for established customers -More information collected on wires above \$3,000 -Wld increase burden substantially - esp. 4 CUs w/ manual processes
Envios [Money Transmitter – New York]		Commenter represented that it would not really be affected.	<ul style="list-style-type: none"> -Most of its business is below current threshold & below even \$1,000 -The same info is collected for all transactions however, only ID is required for trans above \$2,000 -Price would not be affected but operations may increase
The Evangeline Bank & Trust Co. – Louisiana		Recommends eliminating the threshold altogether.	<ul style="list-style-type: none"> -Already comply with proposal
Fernandos Check Cashing	Yes		<ul style="list-style-type: none"> -Customers send mortgage payments thru moneygram -Generally, payments over \$1,000 -Proposal – puts an undue burden on money transfer agents -Wld be “worthless information”
Financial Service Centers of America (FISCA) [National trade association for MSBs - majority of the members are \$ transmitter agents]	Eliminating the threshold – unduly burdensome	Lowering the threshold – no significant detrimental affect	<ul style="list-style-type: none"> -90% of remittances below \$350 -Current practice, many \$ transmitters voluntarily record originator info on trans below \$3,000 & some below \$1,000 -Eliminating threshold wld drive trans underground or other means (\$ orders, stored value, courier, informal value transfer systems) -Questions value to LE

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Name of the Commenter	Oppose	Does Not Oppose	Comments
The Financial Services Roundtable [Nat'l trade association representing members in banking, the securities and insurance industries & others]		No objection— so long as no new info gathering obligations are created	-Members already collect the data for all transmittals -Rqmt to collect new data wld increase operational costs
First National Bank of Wayne (Nebraska)	Yes		-Majority of wires are 4 bank's own business -About 15% of wires - 4 consumers -Of these -50% below \$1,000 (mostly from parents to students) -Wires are 4 established customers -Pricing may increase up to \$5 -Change wld not produce results worth the cost -Criminals wld change behavior
Food Marketing Institute (FMI) [Association for food retailers and wholesalers] (MSBs)	Yes		-LE wld be overburdened – can't adequately analyze current data -Supermarket MSBs wld be burdened – labor & data storage
Georgia Credit Union League (GCUL) [state trade association and one member of the network of state leagues that make up the Credit Union National Association]	Yes		-Would be no benefit to LE -Increased compliance burden -Ensure BSA data is currently being used by LE to full potential -May lead to higher operating expenses for smaller institutions -already overburdened -can't support without justification
Gunnison Bank [Colorado]	Yes		If threshold lowered to \$1,000-160% increase in volume-burden

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Name of the Commenter	Oppose	Does Not Oppose	Comments
Independent Community Bankers of America (ICBA) [represents community banks of all size and charter types in the nation]			<ul style="list-style-type: none"> -Wires for established customers -Wires below \$3,000 – varies - 4 some it's small % -others 60% -Most use manual systems for tracking wires (keeping records) -Most follow the same procedures for all wires regardless of amount -Cld affect cost-effective services -Cld drive transfers underground -Greatest impact on wires below \$1,000, esp. to foreign countries
Mississippi National Banker's Bank [a banker's bank- having a customer base of other banks]	Yes		<ul style="list-style-type: none"> -Minimally impacted by proposal -Burdensome to its community bank customers -Burdensome for non-automated banks -Would affect pricing for community banks and could drive transactions underground
Missouri Corporate Credit Union	Yes		Wld impact member CUs' operations dramatically
National Association of Federal Credit Unions (NAFCU) [Trade association that represents federal credit unions]	Yes		<ul style="list-style-type: none"> -Greater volume of data may diminish usefulness to LE like defensive SARs -Cld be tremendous burden to CU & affect payment operations but wld not impact price or type of service
National Money Transmitters Association, Inc. [membership consists of licensed money transmitters]	Yes		<ul style="list-style-type: none"> -Consumers wld object to showing ID for lower amounts (undocumented immigrants & others with privacy, ID theft concerns) -Burdensome & not beneficial -The lower the ID threshold- more transactions will go underground

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Name of the Commenter	Oppose	Does Not Oppose	Comments
Navy Federal Credit Union [“Nation’s largest natural person credit union”]	Yes		<ul style="list-style-type: none"> -45% of wires -- below \$3,000 -34% of wire -- below \$2,000 -30% of wires -- below \$1,000 -Wires for established customers -Policies differ by \$ amt of wire -Price & service not impacted -Agencies need to obtain more data on value to law enforcement -Maximize current BSA data -Oppose a reporting requirement
New York State Credit Union League, Inc. and Affiliates [Trade association that represents credit unions in the state of New York]	Yes		<ul style="list-style-type: none"> -Significant amt of incoming and outgoing wires are below \$3,000 -Increased recordkeeping burdensome -If rule is promulgated, shld be tailored to types of transactions, e.g. CBWT vs. domestic wires
Northwest Corporate Credit Union		Not a significant burden to collect/retain info on all funds transfers	<ul style="list-style-type: none"> -However, if there is an expansion of SAR reporting threshold – wld be burdensome -If it was required to obtain personal beneficiary information – burdensome
The Money Services Round Table (TMSRT) [Represents national non-bank funds transmitters]		Although it would be an increased burden - ok with lowering threshold to \$1,000 if can abolish the requirement to obtain SSN	<ul style="list-style-type: none"> -MSBs wld incur increased costs of verifying/recording add'l data -O.k. w/ \$1,000 threshold but abolish rqmt to record SSN - verify thru other means (customers unlikely to have SSNs) -Below \$1,000, risk driving transactions underground – immigrants suspicious of efforts to collect personal ID
Thomason, Cindy M [Compliance Officer of a “small community bank in central Oklahoma”]	Yes		<ul style="list-style-type: none"> -Benefit to law enforcement does not seem to outweigh burden to financial institutions -Proposal wld not help limit crime -Rule should consider asset size

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Name of the Commenter	Oppose	Does Not Oppose	Comments
Thomason, Cindy M [Compliance Officer of a "small community bank in central Oklahoma"]	Yes		-Benefit to law enforcement does not seem to outweigh burden to financial institutions -Proposal wld not help limit crime -Rule should consider asset size
Vantage Point Federal Credit Union [Brook Park, Ohio]	Yes		-Additional regulatory burden without reducing crimes -Already overburdened
Visions Federal Credit Union [Endicott, New York]	Yes		-36% of incoming wires are below \$3,000 -76% of outgoing wires are below \$3,000 -Wires for established customers -Keep same records for all wires -No immediate impact cost/service -Already overburdened
The Warrington Bank (Pensacola, FL)	Yes		-Currently, collecting data for wires above \$1,000 -More difficult to ID structuring -Burdensome and could lead to higher pricing -Consumers will resort to other means
WesCorp [Corporate credit union or a credit union for credit unions - providing wire transfer services]		The threshold proposal would have little impact on WesCorp.	-Comply with current regulations for all wire transfers - regardless of amount -Wires below \$2,000 - .018% -Wires below \$1,000 - .068% -No impact on price, service, or operations
Wisconsin Bankers Association [trade association representing nationally chartered depository institutions in Wisconsin]	Yes		-Wld increase operational costs -Add'l records wld flood agencies & make it more difficult to distinguish illegal transactions -Shld evaluate how LE can more effectively use current data

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Appendix A
Glossary of Terms

Add'l – additional

Amt – amount

CBWT – cross-border wire transfers

Cld – could

CU – credit union

FATF – Financial Action Task Force is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

FATF SR VII - Financial Action Task Force special recommendations address international best practices in combating terrorist financing. Special recommendation VII requires financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent.

FI – financial institutions

High degree of usefulness – The Bank Secrecy Act authorizes the Secretary of the Treasury to require financial institutions to keep records and file reports that the Secretary determines have a high degree of usefulness in criminal, tax, or regulatory matters.

ID – identification

Info – information

Joint advance notice of proposed rulemaking – The Board of Governors of the Federal Reserve System and FinCEN are reviewing the threshold in 31 C.F.R. 103.33 that requires banks and nonbank financial institutions to collect and retain information on funds transfers and transmittals of funds. See 71 FR 35564 (June 21, 2006).

LE – law enforcement

MSB – money services businesses

Comment Summary
Lowering or Eliminating the Current
Wire Threshold Recordkeeping Requirement

Regs – Bank Secrecy Act regulation 31 C.F.R. 103.33

Rqmt – requirement

SAR – suspicious activity reports

Shld – should

SSN – social security number

Trans – transactions

Wires – funds transfers or transmittal of funds

Wld – would

(b)(6)
From: [REDACTED]
Sent: Monday, July 28, 2008 10:44 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: AP IMPACT: Buried loot a mystery for authorities (b)(6)

AP IMPACT: Buried loot a mystery for authorities

By MATT APUZZO and ALICIA A. CALDWELL, Associated Press Writers Mon Jul 28, 6:20 AM ET

The businessman arrived at the Treasury Department carrying a suitcase stuffed with about \$5.2 million. The bills were decomposing, nearly unrecognizable, and he asked to swap them for a cashier's check. He said the money came from Mexico.

Money like this normally arrives in an armored truck or insured shipping container after a bank burns or a vault floods. It doesn't just show up at the visitor's entrance on a Tuesday morning. But the banking habits of Franz Felhaber had stopped making sense to the government long ago.

For the past few years, authorities say, he and his family have popped in and out of U.S. banks, looking to change about \$20 million in buried treasure for clean cash.

The money is always the same — decaying \$100 bills from the 1970s and 1980s.

It's the story that keeps changing:

_ It was an inheritance.

_ Somebody dug up a tree and there it was.

_ It was found in a suitcase buried in an alfalfa field.

_ A relative found a treasure map.

No matter where it came from or who found it, that buried treasure stands to make someone rich.

It could also send someone to jail.

—
Felhaber is a customs broker, a middleman.

His company, F.C. Felhaber & Co., is just minutes away from the bridge between El Paso, Texas, and Ciudad Juarez, Mexico. Tens of billions of dollars of Mexican goods cross that bridge each year, aided by people such as Felhaber who navigate the customs bureaucracy.

Customs brokers don't own the stuff that comes into the United States. They just make sure it gets here.

So it is with the \$20 million. Felhaber says the money is not his. A Mexican relative, Francisco Javier Ramos Saenz-Pardo, merely sought help exchanging money that had been buried for decades, Felhaber says.

"To be very clear on this matter: In the beginning, I was not told what it was," Felhaber said in one of several telephone interviews with The Associated Press.

Money petrifies after sitting underground that long and Felhaber said it looked like a brick of adobe. The Treasury will exchange even badly damaged money, but Felhaber said Saenz-Pardo did not want to handle the process himself.

"Imagine a Mexican family bringing money that is damaged and the government calling it a drug deal," Felhaber said.

If the goal were to avoid unwarranted attention, he went about it all wrong. Rather than making a simple — albeit large — exchange at the Treasury, Felhaber allegedly began trying to exchange smaller amounts at El Paso-area banks, raising suspicion every time.

The first stop was the Federal Reserve Bank in El Paso, where authorities say Felhaber appeared with an uncle, Jose, and an aunt, Esther. In her purse, Esther carried \$120,000. She told bank officials there were millions more, discovered while digging to expand a building in Juarez, according to U.S. court records filed by U.S. Immigration and Customs Enforcement.

Banks normally refer such requests to the Bureau of Engraving and Printing, an arm of the Treasury. But employees worried that, with so much cash, the three might be robbed on their way home. So, the bank accepted the money and wired \$120,000 to an account in his uncle's name, Jose Carrillo-Valles, according to a government affidavit.

Felhaber was back at it again weeks later, this time at a Bank of America branch. Customs officials say he unsuccessfully tried to persuade a bank vice president to dispatch an armored truck to the Mexican border to pick up millions of dollars.

Felhaber denies that conversation took place. But he is tough to pin down on details. At times he seems specific on a point ("There is a \$20 million inheritance,") only to contradict himself minutes later, saying the amount is "nowhere near that" and he has no idea where the money came from.

Soon after the Bank of America visit, a man bearing a striking resemblance to Felhaber walked into a Bank of the West branch. This time, however, authorities say the customer identified himself as Ken Motley and said he discovered millions while excavating a tree in Chihuahua, Mexico.

Bank employees refused to exchange any money, despite two follow-up phone calls — once with a Spanish accent, once without — try to set up an exchange.

The mysterious Ken Motley also appeared at the First National Bank, telling employees that a friend had discovered \$20 million buried in an alfalfa field, investigators say.

Felhaber says he is not Ken Motley.

Customs investigators say a Bank of the West employee identified Felhaber's picture as that of Ken Motley.

"That's an absolute lie," Felhaber said. "That would be a horrendous miscarriage of justice."

It's unclear which transaction caught investigators' attention. Most of the tens of thousands of exchanges of mutilated money each year are routine. Natural disasters create a lot of inquiries. Children of the Depression have kept money out of banks, only to see it eaten by rodents in their attics or destroyed in fires. A surprising number of people accidentally shred greeting cards with money inside.

But authorities say there are warning signs that trigger investigations. Making a series of small exchanges is one. Bringing mutilated money from abroad is another.

"That is one of the things we are extra concerned about: This process being used to launder money from illegal activities," said Leonard R. Olijar, the chief financial officer of the Bureau of Engraving and Printing. "That's one of our factors that we use to make a case suspicious."

Immigration and Customs Enforcement agents questioned Felhaber in October 2005. According to a government summary of that interview, Felhaber said he believed the money was the result of a 1970s Mexican land deal. The money was buried in a coffin, he said, until Saenz-Pardo — the relative who brought him the money in the first place — discovered a map leading him to the buried treasure.

Felhaber said he didn't want to do anything illegal and was merely getting a cut of whatever he exchanged.

He now says he was mistaken in his interviews with investigators.

"I told them, 'I suspect this is where it's from but I didn't know,'" he said. "They take you to your word like you're supposed to remember every single thing every single time."

Maybe it was the visit from investigators or maybe someone realized the bank visits weren't working, but Felhaber apparently changed strategies.

In January 2006, the Bureau of Engraving and Printing received a package containing about \$136,000 from Jose Carrillo-Valles, Felhaber's uncle. Felhaber's business was listed as the return address. The letter explained the money had been stored in a basement for 22 years.

Though customs officials were suspicious by then, there was no clear evidence of a crime, just a lot of unanswered questions. So, two months later, the Treasury mailed a check, which was deposited into Carrillo-Valles' account.

Following the money, investigators interviewed Carrillo-Valles and his wife. Each denied ever sending or receiving the money, according to a government affidavit.

As for the \$120,000 wired to Jose's account from the Federal Reserve a year earlier, they allegedly said it was an inheritance. Esther said Jose's mother had recently died.

Authorities don't believe the inheritance story. For starters, they say Jose's mother was still alive when the \$120,000 was exchanged. They also traced a wire transfer from Jose's account to someone named Saenz-Pardo shortly after it was deposited.

Customs investigators now believed Carrillo-Valles was acting as an intermediary, taking a cut of the money and sending the rest to Saenz-Pardo or someone else in Mexico.

Twice, reporters called Carrillo-Valles on his cell phone to ask about the arrangement and confirm his discussions with investigators. First, he said he did not speak English. When a Spanish-speaking reporter called back, he said he could not hear her, and hung up.

In April 2007, the case moved from being suspicious to becoming a criminal investigation. Immigration and Customs Enforcement officials called the Justice Department, saying Felhaber had just arrived in person at the Bureau of Engraving and Printing with about \$1.2 million.

It's not illegal to find money. Depending on where it's found, there might be a bureaucratic process to follow or taxes to be paid, but the discovery itself is not a crime.

There are strict rules, however, about bringing money into the United States. Import documents identified the \$1.2 million as belonging to Jose Carrillo-Valles. Based on their investigation so far, authorities believe that was a lie — a violation that carries up to five years in prison.

But Washington federal prosecutor William Cowden decided to wait. Maybe Felhaber would return with even more.

It paid off. This April, Felhaber was back at the Treasury, this time with a suitcase containing \$5.2 million. Investigators say they have found no import documents filed for this deal, a violation of cash smuggling laws that also carries up to five years in prison.

Prosecutors moved in. Felhaber's two Treasury visits gave them probable cause to seize the money — both the \$1.2 million and the \$5.2 million.

They told a federal magistrate in June that they suspected it was all drug money that had been buried or hidden inside a wall for decades.

"Given that the money is coming north from Mexico, that both conflicting and cockamamie stories have been told about its origins, and that all the stories of how it got to be found are fantastical, I strongly suspect that the Felhaber currency is the proceeds of illegal bulk narcotics sales," ICE investigator Stephen A. Schneider told the magistrate.

Felhaber says he's still not sure what all the fuss is about. At times he says he has no idea where the money came from, but he is always certain it has nothing to do with drugs.

None of the documents filed in federal court accuses Felhaber or his relatives of being involved in drugs. They leave open the possibility that somebody merely came across a cache of drug money, forgotten or abandoned in the Mexican desert.

In the coming weeks, the Justice Department plans to seek criminal forfeiture of the seized \$6.4 million. That means Felhaber and his family will have the opportunity to come to Washington to ask for their money back.

If they do, they'll have to explain where it came from. And they'll have to sort through some of the inconsistent stories for a federal judge. Felhaber bristles at the suggestion there have been inconsistencies.

"The story has never changed," he said. "I don't know how it's changed."

Cowden, the federal prosecutor, said he doesn't know what to expect.

"Some of these cases, nobody ever comes forward," he said.

If so, the buried treasure will become government property.

Or at least some of it. Perhaps there is another \$14 million out there, muddy and waiting to be exchanged.

Does Felhaber know if there's any money left?

On that, it's hard to get a straight answer.

Associated Press writer Alicia Caldwell reported from El Paso, Texas.

(b)(6)
[REDACTED]
From:
Sent:
To:
Cc:
Subject:

(b)(6)
Monday, June 02, 2008 9:47 AM
[REDACTED]
CQ: Card Traffic Flying Under Regulatory Radar
(b)(6)

** CQ WEEKLY **

* Card Traffic Flying Under Regulatory Radar * By Phil Mattingly, CQ Staff

Federal agencies monitoring criminal financial transactions are exasperated in their efforts to track what might be called the installment-plan approach to plotting terrorist activity: the use of prepaid "stored value" cards to finance communications and other operations by groups planning to attack the United States.

"A person can purchase and load about 40 cards with \$2,500 each on them," said Dave Thompson, the assistant director of the Financial, Narcotics and Public Safety Division of the Immigration and Customs Enforcement (ICE) division of the Homeland Security Department. "They can transport them across our borders, and if an ICE inspector identifies them, there really exists no authority to seize them, unless we can determine that they are linked to criminal activity."

No one knows for sure how many stored value cards are in the hands of terrorists or other criminals, since their untraceability is the very basis of their becoming a financial instrument of choice for wrongdoers. What is clear, however, is that such cards are proliferating in the increasingly cashless consumer economy, all the more because the "unbanked" population, made up in large measure of illegal immigrants and only occasional workers, is likewise growing by leaps and bounds. Network-branded stored value cards -- with the logos of Visa, MasterCard, American Express and the like -- had a combined cash value of \$26.8 billion in 2006. The Mercator Advisory Group, an independent research firm monitoring financial trends, estimates that figure will rise almost sevenfold by 2016, to \$181.6 billion.

At the same time, the cards are so loosely regulated that it's all but impossible for federal authorities to monitor their transactions.

"Right now, we're working dozens of cases where we've identified criminal organizations using these cards," Thompson said. "We obviously have some good reporting requirements at our border when a courier would take cash over, and we have great programs in place to counter smuggling of cash by criminal organizations through technology and other initiatives," said Thompson. But when it comes to the government's ability to track criminal use of stored value cards, "we're looking at this as a real vulnerability."

Lawmakers and federal regulators have only haltingly addressed the threat -- in part because the issuers of the cards have put up an effective campaign to keep new controls at bay. When the Federal Reserve proposed rules in 2004 for monitoring usage of the cards most vulnerable to terrorist usage, financial institutions created such a torrent of complaints and opposition that the Fed scrapped the rules entirely. And as Congress and the Bush administration take a fresh look at the stored value threat now, industry advocates are again issuing reports and launching lobbying efforts to keep the status quo.

* The Paperless Chase * At first blush, the cards wouldn't seem to offer a daunting regulatory challenge. Among the broad new powers granted the Treasury and Justice departments after the Sept. 11 attacks was permission to sort through e-mails, telephone records and financial records to monitor and stop the flow of funds into the United States from people abroad who might be seeking to finance terrorism. And laws and regulations to combat money laundering, starting with the 1970 Bank Secrecy Act and extending through the 2001 anti-terrorism law known as the Patriot Act, require financial institutions to report unusual customer transactions, including all those involving more than \$10,000 in cash or cash equivalents, such as money orders or wire transfers. The goal is to create a paper trail that law enforcement agents can use to show patterns of criminal activity. But stored value cards are an invention of this decade and aren't mentioned in those laws and regulations.

"Terrorist financiers typically live public lives, with all that entails: property, occupation, family and social position," Stuart A. Levey, Treasury's undersecretary for terrorism and financial intelligence, told the Senate Finance Committee last month. "Being publicly identified as a financier of terror threatens an end to that 'normal' life."

But that investigative approach assumes, wrongly, that terrorism financiers are using traditional financial institutions. In the main, such figures are shunning "bricks-and-mortar and highly regulated institutions that have people looking for anomalies in transactions,"

said David Gilles, a forensic analyst for Deloitte Financial Advisory Services LLP. "They're always looking for other ways of moving money."

Stored value cards offer just such an alternative. Unlike a deposit or withdrawal at a traditional bank, the cards can generally be purchased anonymously at travel offices, money-service centers or convenience stores, over the telephone or on the Internet. (Some issuers require registration of large-sum cards, but for proprietary reasons industry officials declined to describe the standard procedure.) The cards can also be drained of their cash value through a series of anonymous purchases, so in some ways they're similar to the disposable cell phones with stolen numbers that drug dealers and terrorists often use to avoid having their calls traced.

It's easiest for would-be terrorist financiers or run-of-the-mill crooks to mask their activities by using "open loop" stored value cards: the sort that are as good as cash at almost any retailer, and can also be used to obtain cash from an ATM. (A "closed loop" card, in contrast, is one that can be used to make only one kind of transaction: a Best Buy gift card, for example, or a SmarTrip card for riding the Washington Metro system.)

* Regulatory Impasses * The cards can also be replenished by taking cash to many convenience stores or banks, or by arranging for direct deposit -- and that convenience has prompted some businesses, particularly those with far-flung or fast-traveling workers, to use them as a means of delivering paychecks or travel expenses. Since 2004, the Defense Department has used the cards to pay soldiers and Marines in Iraq and Afghanistan, and the Federal Emergency Management Agency used them to distribute emergency aid to victims of Hurricane Katrina in 2005.

But the cards' wide circulation is also what makes them so hard to regulate. When Max Baucus, the Montana Democrat who chairs Senate Finance, asked Levey last month about plans to regulate prepaid cards more stringently, the Treasury official said, "It's going to be a difficult thing to regulate, because there's no easy point of regulation. . . . And thus far, we haven't successfully regulated it."

That's not because federal officials aren't paying attention. No fewer than seven agencies that have oversight responsibility for financial crimes have issued reports indicating that stored value cards can play a prominent role in criminal activity. The most recent, issued last year, was on the need to improve the detection of money laundering. Issued by the departments of Treasury, Justice and Homeland Security, it recommended that a working group draft new regulations to be implemented by the Treasury's Financial Crimes Enforcement Network. Options are now being researched, network spokesman Steve Hudak says.

Congress hasn't been riding herd on the issue much, either. Last year, the top Republican on the House Judiciary Committee, Lamar Smith of Texas, proposed legislation that would formally label stored value cards as "monetary instruments," which would bring them under the same federal reporting requirements that apply to cash, money orders, traveler's checks, wire transfers and the like. Texas Republican John Cornyn has a companion bill in the Senate, but neither measure has seen legislative action.

The sprawling financial network that touches these cards presents some serious definitional problems for would-be regulators: With more than a dozen kinds of enterprises, ranging from corporate payroll offices to global banks and credit card companies, processing transactions using stored value cards, where do regulators concentrate their efforts? "It's very hard to draw lines and definitions and distinctions of how these products work," Hudak said.

Industry advocates are very mindful that any new federal regulation could represent additional expenses in people, hardware and software. So industry advocates are making a renewed case that the criminal threats associated with the cards are best handled through the current system of industry self-regulation. In February, the Network Branded Prepaid Card Association, which represents three dozen suppliers of such cards, released a report on proposals to combat money laundering, concluding that the industry can effectively police the problem itself.

By law, the association's Terry Maher says, institutions such as Visa and MasterCard must file reports on any suspicious activity while monitoring especially large or suspicious currency transactions. Association members have lately been lobbying Congress to drive these points home, Maher said. They're also talking with officials at the Treasury and ICE to keep them apprised of the state of industry security measures. The aim of such meetings, he said, is "to again inform everybody that this isn't the Wild West. These are issued by highly regulated financial institutions."

Still, critics such as Thompson say that industry practices aren't sufficient to keep pace with the scale of the threat. "Right now, there are no reports because it's not a requirement," he says of efforts to monitor the volume of illicit uses for stored value cards. "There's really nothing we can do about it right now."

FOR FURTHER READING: Smith's bill is HR 3156; Cornyn's is S 1860; terrorism financing, 2007 CQ Weekly, p. 1572; Patriot Act (PL 107-56), 2001 CQ Almanac, p. 14-3; Bank Secrecy Act (PL 91-508), 1970 CQ Almanac, p. 884.

	SWIFT MT103	103.33
Originator Name	X	X
Originator Address	X	X
Amount of the transfer	X	X
Execution date	X	X
Payment Instructions	X	X
Beneficiary Name	X	X (1)
Beneficiary Address	X	X (1)
Beneficiary Account Number	X	X (1,2)
Originator Account Number	X	X (1,2)
Specific Identifier		X (1)
Beneficiary's Financial Institution	X	X
Originator Financial Institution	X	X

Notes:

1. If available.
2. When originating a transfer, the FI must keep the account number of the beneficiary. When receiving, the FI must record the account number of the recipient.

Traffic in millions of messages

Data : 1st Quarter 2008

1	MT103	Single Customer Credit Transfer	Instructs a funds transfer.	20.45	10.7 %	13.0 %
2	MT535	Statement of holdings	Reports at a specified time, the quantity and identification of securities and other holdings which the account servicer holds for the account owner.	15.81	24.3 %	10.1 %
3	MT950	Statement message	Provides balance and transaction details of an account to the account owner.	15.47	18.5 %	9.8 %
4	MT300	Foreign exchange confirmation	Confirms information agreed to in the buying/selling of two currencies.	12.67	17.8 %	8.1 %
5	MT541	Receive against payment	Instructs a receipt of financial instruments against payment. It may also be used to request a cancellation or pre-advise an instruction.	10.88	12.7 %	6.9 %
6	MT910	Confirmation of credit	Advises an account owner of a credit to its account.	10.15	14.7 %	6.5 %
7	MT543	Deliver against payment	Instructs a delivery of financial instruments free of payment. It may also be used to request a cancellation or pre-advise an instruction.	9.80	19.1 %	6.2 %
8	MT940	Customer statement message	Provides balance and transaction details of an account to a financial institution on behalf of the account owner.	9.38	14.7 %	6.0 %
9	MT202	General Financial Institution Transfer	Requests the movement of funds between financial institutions.	7.32	14.0 %	4.7 %
10	MT900	Confirmation of debit	Advises an account owner of a debit to its account.	5.72	23.2 %	3.6 %
	Others			39.48	21.7 %	25.1 %

Total

157.14	17.8 %	100.0 %
---------------	---------------	----------------

Data : Total billable traffic

52

Chapter 5

Reports of International Funds Transfer

35 - Every month, the Entities need to remit to the Secretary, per request of the Commission, taking no more than 15 available days after the last day of the previous month, a report of each international transfer of funds, for which each individual Client or User has received or sent, totaling an amount greater or equal to 1,000 USD or the foreign currency equivalence that is used.

The Entities should provide the information, mentioned in the last paragraph, through electronic means and in the reporting format of funds transferred, issued by the Secretary.

In the case of those Entities whose clients or users have not made any transfer of funds during the corresponding month, they simply need to remit, in the terms and under the format specified in the preceding paragraph, a report in which one must fill the fields related to the identification of the entities themselves and the corresponding month, leaving the remaining empty fields contained in that format.

36 – In addition to the Dispositions indicated in paragraph 35, relating to the international transfer of funds for the payment of remittances, that the entities receive directly from abroad or through money transmitters (referred to in Article 95 of the General Law of Organizations and Auxiliary Credit Activities) and that the entities process as direct payers in amounts equal to or in excess of \$1,000 USD or its foreign currency equivalent, these entities also must specify the following information in the reports that they submit in terms of what is indicated in the present disposition:

I. In the case that the recipient is an individual:

Fathers last name, mother's maiden name and First name(s) without abbreviations; date of birth, and, in the case that it meets what is established in paragraph 16 of the present Dispositions, the Unique Number of the Population Registration, and/or Federal Registration of Contributors Key or the series number of the Advanced Electronic Signature, when it is applicable.

II. In the case that the recipient is a business/entity:

Line of business, social activity or object, in accordance to what is established in paragraph 16 of the present Disposition, and Federal Registry of Contributors Key or the series number of the Advanced Electronic Signature, when it is applicable.

In both cases, the Entity should provide other information required in the referred format in paragraph 35 of the present Disposition, even if the matter involves a transfer received directly from abroad or through a transmitter of money of those previously mentioned.

UNCLASSIFIED

Australian Transaction Reports
and Analysis Centre
Zenith Centre, 821 Pacific Highway
Chatswood, Sydney, NSW
Telephone +612 9950 0055



Australian Government
AUSTRAC

Correspondence
PO Box 5516
West Chatswood, NSW 1515, Australia
Facsimile +612 9950 0072
www.austrac.gov.au

Our Reference: 81313

20 August 2010

(b)(6)
[Redacted]
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, Virginia, 22183
UNITED STATES

Dear (b)(6)

Re: Request for meeting to discuss new intelligence/analytical systems

First I would like to thank you once again for your hospitality towards (b)(6) and myself in what was a very informative visit to Fin CEN in June. Please accept the enclosed gift as a token of our appreciation.

As mentioned in our discussions, AUSTRAC received funding in the recent budget for the largest change program to its intelligence systems since the implementation of its enquiry system in the late 1990s. Over the next four years AUSTRAC will research, procure, and implement new intelligence systems. The implementation will have implications for all our partner agencies in relation to their access, types of information available and the forms of intelligence provided by AUSTRAC. Equally, the intelligence products provided to our international partners will also be improved.

AUSTRAC is looking for a strategic partner to provide advanced analytical systems and tools and we are exploring a number of commercial off-the-shelf packages. In this regard AUSTRAC is currently engaging with several vendors and we intend to pilot their capabilities within the financial intelligence environment. AUSTRAC is also keen to meet with relevant domestic and international partners who may have purchased or are considering purchasing similar analytical tools with a view to learning from their experiences.

During my recent visit to the USA it became clear that FinCEN are currently doing some work around new analytics tools. Therefore, AUSTRAC would like to arrange a follow up meeting to gather additional information in this space. It is envisaged these discussions will greatly inform the evaluation process. We would be interested in gathering feedback on your experiences, use to date, effectiveness, and any other relevant point of discussion including:

- What business problem you were attempting to solve by implementing commercial, analytical solutions/products?
- What parts of your business will be using products?
- What comparisons were made when making a decision to purchase/which other vendors were considered?
- What components of the product suite are being considered?
- What other technologies and analytical techniques are being engaged and to what effect within the broader US law enforcement and security environment?

UNCLASSIFIED

54

UNCLASSIFIED

AUSTRAC is intending to send business and IT representatives to meet with various contacts in the USA and Canada during the week beginning Monday September 13, 2010. The AUSTRAC representatives include:

[REDACTED]

With FinCEN's support, AUSTRAC is very keen to engage colleagues from the Financial Transactions and Reports Analysis Centre (Canada) (FINTRAC) in tri-lateral discussions on these issues. We are yet to confirm the availability of our colleagues from FINTRAC pending your support. We can advise that AUSTRAC also intends to meet with representatives from the US Department of Justice - Organised Crime Drug Enforcement Task Force - Fusion Centre.

If you require any further information please contact [REDACTED] via the telephone or email address noted above or via [REDACTED]. I look forward to hearing from you.

Yours sincerely,

[Handwritten signature]
[REDACTED]

55



AML/CFT Expert Group

Revised draft 3 March 2007

AMLEG 07/03rev2

Transparency in payment messages

64



Australian Government
Australian Transaction Reports
and Analysis Centre

OFFICE OF THE CHIEF EXECUTIVE OFFICER

Ref: *NJJ*

8 February 2008

(b)(6)
[REDACTED]
Financial Crimes Enforcement Network
United States Department of the Treasury
Post Office Box 39
Vienna Virginia 22183
USA
(b)(6)
[REDACTED]

Re: International Wire Transfers

I refer to my previous discussions with you and [REDACTED] regarding this matter.

It is my understanding that the Financial Crimes Enforcement Network ("FinCEN") study on the capture of international wire transfers/cross border wire transfers recognises that the reporting of international wire transfers are both technically feasible for the US Government to adopt, and a valuable tool in your Government's ongoing efforts to combat money laundering ("ML") and terrorist financing ("TF"). You indicated to me that FinCEN is currently preparing submissions to the US Treasury which include FinCEN's "inclusive and incremental approach"¹ to resolving outstanding technical and policy issues regarding the mandatory reporting of cross-border wire transfers.

The purpose of this letter and its attachments is to alert you to the Australian government's long-held view of the significant value of the reporting of international wire transfers to AUSTRAC, not only in terms of our domestic law enforcement and revenue matters, but also in facilitating international cooperation in following the money trail associated with transnational and organised crime, and terrorism financing.

The value of this data is confirmed from AUSTRAC's extensive experience over 16 years in collating and disseminating such information, both domestically and internationally. AUSTRAC can see where the money goes overseas, and from where it comes, but international cooperation in tracking the funds of criminals is severely hampered because very few other countries have adequately considered the value of the collection of this information for domestic and international investigations. It is hoped that the USA will see this value and others will follow the USA lead, resulting in the identification and prosecution of the most significant criminals, who move their funds around the world.

¹ FinCEN Media Release dated 17 January 2007.

Although I will elaborate on this in more detail later it must be said at the outset that from an "Intelligence perspective", AUSTRAC's FIU strongly considers international wire transfers a critical component of its financial analysis and intelligence operations. Indeed, international wire transfer reports provide a comprehensive understanding of the *total* suspect financial activity. This means the collection of reports such as threshold deposit and withdrawal transactions, which only provide the FIU with details of the ML '*placement activity*' in most cases can be linked to the wire transfers reports to gain a complete understanding of the entities and networks linked to the ML activity. Organised crime groups increasingly operate in numerous jurisdictions across the globe environment and the collection of international wire transfer reports' information becomes an integral component of the FIU's analysis in order to fully understand and detect ML activity. The collection of international wire transfer by an FIU enables it to 'join the dots', and detect the *layering and integration* stages of ML often linked to the placement activity.

In ML cases linked to tax evasion using tax haven jurisdictions, or drug importations or trade based money laundering matters, the financial activity will normally encompass deposit and withdrawal activity followed by wire transfers to overseas jurisdictions as part of a *layering and integration* processes whereby the funds are moved offshore in a round robin transaction scenario only to return if some other shape or form. In the case of drugs, the funds may simply be sent offshore to pay for the illicit drugs following the placement stages. In both of these examples, collection of the international wire transfer information is the only method available and MOST critical to the FIU in being able gain a full picture and understanding of the financial activity as part of its analysis.

AUSTRAC's Role

As Australia's Financial Intelligence Unit (FIU), AUSTRAC collects, analyses, and disseminates financial intelligence to 34 law enforcement, national security, revenue and social justice agencies, and to 49 overseas FIUs. This financial intelligence comes from the reporting to AUSTRAC of a range of financial transaction reports from the financial sector and non-banking financial sectors. Those reports include suspicious transaction reports, referred to as SUSTRs in Australia and which are similar to suspicious activity reports (SARs) in the US. We also collect cross border significant cash reports (ICTRs) and significant cash reports (SCTRs). Most importantly, we also capture all customer-based international wire transfers into and out of Australia, which we refer to as international funds transfer instructions (IFTIs). In our experience, the mandatory reporting of international wire transfers has provided AUSTRAC and our partner agencies with a vital and rich source of intelligence which has been instrumental in instigating, contributing and leading to the prosecution of individuals and organisations for many and varied serious crimes, both in Australia and overseas.

History

Australia first introduced mandatory reporting of international wire transfers in 1992 after a report by the Australian Government in 1991 on capital flight from Australia was linked to tax evasion. The report noted that international wire transfers were the most common way in which funds were channelled from Australia, and that the then current cash transactions monitoring system did not detect or monitor such transfers. The report recommended the mandatory reporting of *all* international wire transfers to AUSTRAC to assist in tracking money being wired to or from overseas, to assist investigations of offences of Australian laws and cooperation in overseas investigations.

Two decisive factors which led to the collection of that data was that the data was already in electronic form, and the reporting entities advised that the cost would be minimised because of its electronic format, and if there was no threshold requirement. In fact, the reporting entities indicated that the cost would be significantly less than the programs for reporting of SARs and significant cash.

In contrast, a transaction reporting threshold would have required the technical development of systems by each reporting entity, and also extensive staff training concerning the threshold levels. The response to these issues in Australia was a low cost technological solution developed and provided by AUSTRAC to reporting entities which was virtually seamless to their daily business and required very little cost on their part. As it merely duplicated and then extracted the data from the technology systems of the reporting entities, there was no need for staff training. A bonus of the system was that international wire transfers were reported in real-time. These vital considerations enabled a quick and successful implementation of international wire transfer reporting requirements at very little cost to government or reporting entities.

Legislation

Legislative requirements regarding international wire transfers are contained in sections 3, and 17B to 17F of the *Financial Transactions Reports Act 1988* (FTR Act). Further prescribed details in relation to international wire transfers are contained in regulation IIAA of the *Financial Transaction Reporting Regulations 1990*.

In essence the FTR Act requires "cash dealers" in Australia to report international wire transfers for monies being telegraphically transferred or wired into or out of Australia. International wire transfers are reportable for *any amount*, whether paid for by cash or otherwise. It is only the reporting entity at the initial point of receipt of the international wire transfers in Australia, or at the point of the transmission from Australia who is required to report the international wire transfers. The maximum penalty for a person failing to submit an international wire transfer to AUSTRAC is imprisonment for up to two years²

These requirements have been included in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.³ (AML/CTF Act) which will supersede the FTR Act provisions in December 2008.

The FIU

AUSTRAC now receives 16 million financial transaction reports ("FTR") per year⁴, a very high volume of data compared with many FIUs around the world. This is due to the mandatory reporting of international wire transfers, in addition to the much smaller volumes of reports of suspicious activities, significant cash transactions and cross-border currency movements.

² Section 28(4) of the FTR Act.

³ The AML/CTF Act came into effect on 13 December 2006, and was introduced to ensure that money laundering and terrorism financing risk in Australia is identified, managed and mitigated. As a result of the staggered implementation dates of the AML/CTF Act, the provisions relating to international wire transfers do not commence until 12 December 2008, and the FTR Act provisions continue in force until that time. For further details regarding the AML/CTF Act please refer to AUSTRAC's website www.austrac.gov.au.

⁴ See page 33 of the AUSTRAC Annual Report 2006-7 ("Report"). For that year 15,740,744 financial transaction reports were received, at approximately 60,500 per day.

Importantly volume is not an issue as technology solutions are readily available to capture much larger volumes of data than these, and at relatively little cost. The volume is also important in AUSTRAC's analytical work, as our data mining tools are more effective on larger volumes of data. The AUSTRAC database currently contains about 90 million transaction reports. Although the volume of international wire transfers collected in Australia is significantly lower than the potential number of reports in the US, this should not be a deterrent to the capture of *all* wire transfers by FinCEN. As indicated, technology solutions to capture those volumes are readily available at relatively low cost.

More than 99.7 percent⁵ of reports of financial transactions are submitted to AUSTRAC via the AUSTRAC developed secure reporting system, "EDDSWeb"⁶. Moreover, it is AUSTRAC policy where the volume of reports exceeds 250 per year, a reporting entity *must* report electronically. This method ensures higher levels of quality and timeliness of reports, and allows fast and accurate correction of data quality issues, as reports may be returned to reporting entities for correction via EDDSWeb.

Maintaining the software is simple, as it is only one program that is provided to all reporting entities and is managed by *one* person at AUSTRAC. AUSTRAC could make this technology available to FinCEN.

EDDSWeb was developed by, and is fully maintained by AUSTRAC. It is provided free of charge to all reporting entities. The importance of this software is that it captures the SWIFT format, and similar formats, so little work is needed by the reporting entities to put it in place.

For smaller entities, such as alternative remittance services, AUSTRAC accepts international wire transfers via a batch file transfer format which requires the reporting entities to implement their own systems for converting the non-SWIFT data to the proper format prior to submitting the reports to AUSTRAC. AUSTRAC requires mandatory data fields that must be included in the international wire transfers report. Reporting entities can report by batch file and single report via a web-faced interface operated by AUSTRAC. The interface enables institutions to upload prepared files automatically, and provides an interface for the manual upload of prepared batch files, and a form for extremely low volume reporting institutions to submit data. AUSTRAC has also developed, and distributes to financial institutions, a Microsoft Excel macro that can convert certain electronic data to the AUSTRAC systems.

In Australia, the largest four banks account for approximately 80 % of the reports of international wire transfers, with a second group of approximately 20 financial institutions comprising the majority of reporting institutions, and a large number of smaller entities reporting very small volumes. The cost to all, including AUSTRAC, is minimal.

Reports Received at AUSTRAC since 2001

The quantity of financial transaction reports received by AUSTRAC continues to increase significantly. As noted above, the database currently comprises about 90 million reports. Notably, international wire transfers provide the largest volume of financial transaction reports received with more than 50 million reports received over the past 5 years.

⁵ Report at page 40.

⁶ EDDSWeb is the acronym for Electronic Data Delivery Service.

For the year 2006-07, a total of 13,017,467 international wire transfers were received⁷, a 14 % increase from 2005. Figures for international wire transfers and other financial transaction reports are listed in the following table.

Type of Report	2002-03	2003-04	2004-05	2005-06	2006-07
SARs	8,054	11,484	17,212	24,801	24,440
Significant cash	1,979,446	2,056,617	2,288,373	2,416,427	2,675,050
Cross border cash	28,274	25,579	26,172	27,755	23,351
International wire transfers	7,493,765	8,685,843	10,243,774	11,411,961	13,017,467
Total Reports	9,509,539	10,779,523	12,575,531	13,880,994	15,747,744⁸

Advantages

AUSTRAC has been capturing international wire transfers now for 16 years. What AUSTRAC can categorically say is that Australian law enforcement, national security and revenue programs have benefitted *greatly* from the capture of international wire transfers, as have a number of agencies in other countries through our law enforcement and FIU cooperation programs.

The value of the international wire transfer data, and its linkages in the AUSTRAC database to all of the other report types, can be found in the following table with more than 9 million searches on the database over the past 5 years by approximately 2,500 AUSTRAC and specified personnel from the law enforcement, national security, revenue and social justice agencies. It has assisted in more than 10,000 investigations, and provided tax revenue, directly derived from intelligence from the data, of more than \$400 million. Most of these investigations and the revenue results involved intelligence from international wire transfers.

Database Searches	873,815	1,225,388	2,063,869	2,546,372	2,348,363
Investigations	1,544	1,743	2,224	1,582	1,529
Taxation Revenue	AUD 99 million	AUD 72 million	AUD 62 million	AUD 91 million	AUD 87 million

⁷ See page 36 of the Report.

⁸ There were 589,528 name searches undertaken by partner agencies.

69

Some of the advantages of the collection, analysis and dissemination of international wire transfer information are:

- International wire transfers are attractive to businesses because the service is a secure, quick and trusted means by which to send funds overseas. As international wire transfers do not involve the actual movement of currency, they are a rapid, reliable and secure method for transferring funds without the risks associated with moving physical currency. For the same reasons that apply to legitimate businesses, they are also attractive to criminals. The huge volumes of international wire transfers moving around the world daily, and the ability to indicate some legitimacy to the transactions through the financial sector, assist the criminals in layering and integrating their illicit funds, and those funds being transmitted for illegitimate purposes such as for terrorism financing. Data mining processes applied to this data when captured in one location can readily identify these criminals in the extensive amount of data.
- Terrorism is often financed by the movement of low value sums from participants in various countries. For example, reports on the 9/11 bombings in the US have indicated that as little as \$500,000 was used to finance the attacks and that the money arrived in the US in numerous small value wire transfers from other countries. These transfers rang no alarm bells and were not identified until after US authorities began their investigations. The collection of all value international wire transfers and application of appropriate data mining techniques may have uncovered some of these transactions prior to the events of 9/11.
- The linking of other types of financial transaction reports to international wire transfer reports in a single database provides significant benefits in indentifying criminal activity. For example, a SAR which has been reported by a financial institution may not be enough in itself to alert law enforcement authorities about a criminal act. However, linking of that SAR to other report types, and in particular, to international wire transfers may provide a clearer picture of what may be occurring and the individuals and countries involved. International wire transfers may highlight the layering stage of money laundering which is not always apparent in other report types.
- International wire transfers provide a vital source of intelligence to law enforcement because of:
 - the ease of capture;
 - data they contain; and
 - the quantity of such transfers sent around the world on a daily basis.
- Through the use of data mining technologies, large volumes of international wire transfers provide the FIU with a greater ability to detect patterns of criminal behaviour and low value transactions which may have been overlooked.
- The use of international wire transfers in Australia, has been very successful in identifying numerous criminals not previously known to law enforcement agencies and has assisted greatly in intelligence led policing (see Attachment A).
- International wire transfers not only increase the extent of intelligence available to law enforcement agencies, but also enable the enhanced exchanges of vital intelligence between FIUs worldwide. Some type of international wire transfers reportage occurs in Argentina, Brazil, Canada, the Cook Islands, Ireland, Russia, South Africa, Switzerland, and the Netherlands.

- The Financial Action Task Force on money laundering (FATF) in its 40 + 9 Recommendations has addressed the issue of international wire transfers, although to a very limited degree in its Special Recommendation VII suggesting that “financial institutions, including money remitters, should conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information” such as name, address and account number. In addition, FATF Recommendation 19 states: “Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.” In both cases, the FATF has not gone far enough in addressing this issue. These solutions are useful, but only provide for records to be maintained and only assist law enforcement after the crime has been detected, the criminals have been identified by law enforcement and the location of each transaction has been identified by some other means. Very few criminals and very few of their transactions can be located merely through the collection of information in this way. Law enforcement will not know with which reporting entity the information is held and when and what transactions have occurred. When they eventually get that information, if they do, the money will likely have been dispersed globally and not be locatable. Reporting at the time of the transfer significantly enhances the ability of the law enforcement agencies to follow and intercept the funds.
- An addendum to the FATF requirements is that AUSTRAC, rather than the reporting entities, can ensure that Australian and overseas entities are including the required “originator information” in all international wire transfers into and out of Australia. As AUSTRAC has all of the reports of international wire transfers into and out of Australia, simple software analysis can indicate whether the information is in the international wire transfer. If it is not being included, AUSTRAC can provide advice to the reporting entities that it is not being included by them or their “correspondents” overseas and the reporting entities can take steps to ensure it is included. If the failure to include the information in international wire transfers continues, the FATF can be alerted to that fact and appropriate follow up can be pursued by the FATF members.
- Costs for reporting of international wire transfers would be minimal to industry and FinCEN. Banks and non-bank financial institutions already have this information in an electronic format. The cost to AUSTRAC is minimal given the quality of information available, and the benefits it provides to investigating agencies and their results, together with benefits to international law enforcement. For example, AUSTRAC’s FIU’s direct costs are approximately AUD 7 million per year. International relations and intelligence capability costs are an additional AUD 2 million per year. The intellectual technology component comprises an estimated AUD 5 million.⁹ Costs to set up access to the data in partner agencies, for approximately 2400 users, would include the cost of the computer/software connection and training at approximately AUD5 million. Leasing and administrative costs would amount to a further AUD5 million.

⁹ It should be noted that all directorates within AUSTRAC utilise this service.

- The positive results for Australian law enforcement have been significant. AUSTRAC information contributed to the Australian Taxation Office assessments in 2006-7 of AUD 87 million alone.¹⁰ In 2004-05, AUSTRAC international wire transfer information assisted law enforcement agencies to identify drugs to the street value of more than AUD 1 billion, stopping those drugs from coming into Australia and being sold on Australian streets, and consequently stopping the laundering of that amount of funds in Australia, much of which would have been sent off-shore. As international wire transfers are kept for a minimum of 8 years by AUSTRAC, it is a resource which can be utilised in an investigation at *any* stage.
- As the information is only captured when it is in Australia, that is the last point before it leaves Australia or the first point once it has entered Australia, concerns as to ownership of the information, reporting of the information, or use of the information, have never been raised by other countries.

Privacy

The collection of such significant volumes of data raises major concerns with regard to security and the privacy of the information in international wire transfers. Security of premises and personnel is paramount at AUSTRAC. Information held by AUSTRAC is securely protected, and disseminated, only in accordance with the law. Access to the database is tightly controlled and access only allowed for specific purposes both for AUSTRAC personnel, and the personnel of agencies that can have access to the data.

The dissemination of information by AUSTRAC is carefully controlled to ensure that breaches of privacy do not occur. The official information AUSTRAC holds is protected according to the requirements of the *Privacy Act 1988* and *Commonwealth Protective Security Manual*. AUSTRAC continues to maintain the integrity of its information by conducting regular audits and inspections of all classified information to ensure that current standards are maintained, and to ensure that there is not any improper use or disclosure of information.

There are also a number of safeguards and measures in place under legislation to protect official information held by AUSTRAC employees.¹¹ The legislation provides for penalties if an AUSTRAC employee improperly disseminates information obtained during the course of their duties.

The FTR Act and AML/CTF Act both provide for certain designated people from partner agencies to have access to financial transaction reports for the purposes of performing that agency's functions and powers *only*.¹² Sanctions apply if such a person discloses such AUSTRAC information for an improper purpose. AUSTRAC also maintains logs of all access to its data by AUSTRAC staff and by partner agencies with online staff. Education programs and guidelines have also been issued by AUSTRAC regarding how FTR information may be used, and for privacy and security awareness.

¹⁰ See Report at page 61.

¹¹ See section 25 of the FTR Act and Part 11, Division 4 of the AML/CTF Act.

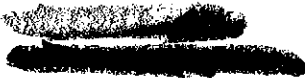
¹² See section 25 FTR Act, section 70 *Crimes Act 1914*, section 10 *Public Service Act 1999* and section 2.1 of the *Public Service Regulations*.

AUSTRAC has also formally recognised the sharing of FTR via memorandums of understanding ("MOU"). While not legally binding documents, these MOUs are rested within a good faith relationship. MOUs provide the framework within which the AUSTRAC CEO grants access to FTR information and financial intelligence information. In addition, to ensure correct usage of the data, the MOUs contain provision for feedback information advising AUSTRAC of the number of investigations value added, and the value of tax assessments assisted by AUSTRAC Financial transaction reports. AUSTRAC has entered into MOUs with 34 partner agencies and 49 overseas FIUs.

Summary

The mandatory reporting of all customer-based international wire transfers into and out of Australia, has provided AUSTRAC and its partner agencies with an invaluable source of financial intelligence. Tangible evidence is supplied in the number of investigations undertaken by AUSTRAC's law enforcement, national security, revenue and social justice partners, and the amount of taxation revenue resulting directly from use of the information. Proactively identifying criminals in Australia and overseas, through their financial transactions including information as to dates of transactions, locations of transactions, addresses, associates in Australia and overseas, and having this information in real time, has been vital in the investigation and prosecution of the most notorious criminals, both known, and previously unknown, in Australia and in many overseas countries. Issues such as privacy and costs have been resolved inexpensively and to the satisfaction of all parties.

Yours sincerely

A large, dark, irregular redacted area covering the signature and name of the sender.

Working Group on Terrorist Financing and Money Laundering

COVER PAYMENTS AND IMPLICATIONS FOR SR VII (WIRE TRANSFERS)

Discussion paper by the Secretariat

FATF-XXI

Interested delegations are asked to provide comments on this discussion paper by e-mail to the FATF Secretariat (secretariat@fatf-gafi.org) no later than 21 August 2009 (close of business).

 (b)(6)

JT03268239

COVER PAYMENTS AND IMPLICATIONS FOR SR VII (WIRE TRANSFERS)

Discussion paper by the Secretariat

I. INTRODUCTION

1. In May 2009, the Basel Committee on Banking Supervision (the Basel Committee) issued guidance on the issue of cover payments: *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*.¹ This Basel Guidance describes the role of supervisors, and originator, intermediary and beneficiary banks in enhancing the transparency of payment messages related to cover payments.

2. At its June 2009 meeting, the Working Group on Terrorist Financing and Money Laundering (WGTM) heard a presentation from the Basel Committee on this guidance and related industry initiated upcoming changes to the S.W.I.F.T. payment message system which will come into effect in November 2009. The WGTM had a preliminary discussion of the issues and agreed to study the Basel Guidance for the purpose of identifying potential implications for the implementation of Special Recommendation VII (SR VII) on wire transfers. The Secretariat, in co-ordination with interested delegations, was directed to prepare a background paper that identifies these issues, including possible options for resolving them, for further discussion by the WGTM in October.

3. This paper summarises the preliminary issues that were raised at the June 2009 WGTM meeting. Interested delegations are invited to submit to the Secretariat proposals for resolving the issues identified in this paper, and any additional issues/proposals that should be discussed in relation to cover payments and the implementation of SR VII.

II. HOW COVER PAYMENTS WORK

4. A cover payment is a particular type of payment from one financial institution to another through one or more correspondent banks. In the case of a wire transfer ordered by a customer, the cover payment mechanism is often used where the ordering financial institution (FI) and beneficiary FI do not have a banking relationship that allows them to settle their payments with each other directly. The following description explains how the cover payment mechanism works in practice and highlights implementation issues that were raised by the private sector.

- (a) The originator instructs his/her bank (the ordering FI) to send a wire transfer to the beneficiary.
- (b) The ordering FI sends an MT103 payment message directly to the beneficiary FI, thereby informing it of the payment. The MT103 payment message is capable of including full originator information.

¹ This guidance paper is available on the website of the Bank for International Settlements at the following link: <http://www.bis.org/publ/bcbs154.pdf>

- (c) The cover payment settlement process occurs separately through the corresponding banking network. To settle the transaction, the ordering FI sends an MT202 payment message to its correspondent bank instructing that a transfer be made to the beneficiary's bank (*i.e.*, the cover payment). The MT202 message was designed for FI-to-FI transfers and is incapable of carrying any originator information relating to the underlying transaction(s) that the settlement payment is intended to cover, or the associated originator(s) and beneficiary(ies).
- (d) Pursuant to the MT202 message, the ordering FI's correspondent bank then either settles the payment either directly with the beneficiary FI (if they have a relationship that would allow them to do so) or through the beneficiary FI's correspondent bank.

5. The cover payment process creates the following implementation issues. Intermediary FIs in the cover payment settlement process do not receive the MT103 payment message which is sent directly from the ordering FI to the beneficiary FI. Intermediary FIs in the settlement payment chain only receive the MT202 message which does not contain any originator or beneficiary information relating to the underlying transactions. This creates a lack of transparency for intermediary FIs that impedes their ability to accurately assess the risks associated with the correspondent and clearing operations, and to comply with legal obligations, such as with targeted financial sanctions (*e.g.*, freezing the funds of persons/entities designated pursuant to United Nations Security Council Resolutions), especially when applicable lists differ among the different jurisdictions.

6. The new S.W.I.F.T. MT202COV message type, which will be implemented in November 2009, will allow originator and beneficiary information to be included in the cover payment message in mandatory fields, thereby enhancing the transparency of such payments in relation to intermediary FIs involved in the cover payment settlement process. In practice, the new S.W.I.F.T. system will automatically block transactions that do not carry information in the required fields.

III. ISSUES RELATING TO THE IMPLEMENTATION OF SR VII

7. To date, the following issues relating to cover payments and the implementation of SRVII have been identified.

Issue #1 – Obligations on ordering financial institutions

8. SR VII requires an ordering FI to include, in the message or payment form accompanying the wire transfer, full originator information that has been verified for accuracy in accordance with the standards set out in Recommendation 5. Although the new S.W.I.F.T. MT202COV message type will allow such information to be included in the cover payment message, this will not address situations where the ordering FI is using an amended cover payment form (*i.e.*, a payment form that does not have the same standards as the MT202COV).

Issue #2 – Obligations on intermediary financial institutions

9. SR VII requires an intermediary FI to ensure that all originator information which accompanies a wire transfer is retained with the transfer. However, in practice, intermediary FIs cannot conduct a proper assessment of the risks associated with the correspondent and clearing operations, or ensure compliance with targeted financial sanctions, without confirming that all mandatory fields in the payment message are completed with meaningful information (*i.e.*, ensuring that the mandatory fields are not completed with a meaningless combination of letters or symbols) and screening sanctions lists against that information.

Issue #3 – Beneficiary information

10. SR VII does not require that information identifying the beneficiary of the transaction be included with the wire transfer. The reason is that SR VII envisages a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering FI to the beneficiary FI either directly or through one or more intermediary FIs (e.g., correspondent banks). This is because, in practice, the beneficiary information is always included in such cases, so that the beneficiary FI will know to whom the wire transfer must be paid. However, when using the cover payment mechanism, an intermediary FI may never see originator or beneficiary information and may, therefore, assume that the payment is an inter-bank transaction.

IV. NEXT STEPS

11. Interested delegations should submit to the Secretariat proposals for resolving the above issues, and any additional issues not yet identified in this paper no later than the **close of business on Friday 21 August 2009**. All submissions will be posted to the WGTM secure website. Based on the comments received, this paper will be revised and re-circulated to the WGTM for discussion at its October 2009 meeting.

FATF Secretariat
24 July 2009

(b)(6)
FW MEPS demand explanation on US plan to monitor all money transfers

Sent: Tuesday, September 28, 2010 9:50 AM

(b)(6)
Subject: FW: MEPS demand explanation on US plan to monitor all money transfers

-----Original Message-----

[REDACTED] (b)(6)
Subject: MEPS demand explanation on US plan to monitor all money transfers

FYI Article from EU Observer:

MEPs demand explanation on US plan to monitor all money transfers VALENTINA
POP Today @ 09:24 CET

EUOBSERVER / BRUSSELS - The EU commission and MEPs have requested clarifications from Washington on reported plans to expand an anti-terrorism programme targeting financial transactions - a move that would render void the long-debated "Swift agreement" enacted in August. "We urgently seek clarifications from the US if these plans are an infringement of the Swift agreement and the EU commission promised to demand further information on it," Dutch Liberal MEP Sophie in't veld told this website on Monday evening (27 September) after a closed-door meeting with commission officials.

Earlier that day, the Washington Post reported that the Obama administration was looking into expanding existing anti-terrorism programs targetting bank transfers to the extent that a long-debated agreement with the EU, dubbed the "Swift agreement," would no longer be valid. Under current rules, US officials can request European data relevant to a specific terrorist investigation from the Society for Worldwide Interbank Financial Telecommunication (Swift). The request needs to be approved by the EU's police co-operation unit, Europol, and has to meet certain requirements.

But if the new plans go into effect, the Washington Post said: "transactions between European and US banks would be captured regardless of whether there is a substantiated need."

Responding to the news, Ms in't veld said: "We are all getting a bit tired of being taken by surprise all the time. The US is our friend and ally, so we shouldn't be treated this way."

Set up in the aftermath of the terrorist attacks on New York and Washington in 2001, the "Terrorism Finance Tracking Program" was initially a covert operation, tapping Swift data without the Europeans knowing about it. It was only when the story broke, in 2006, that Washington engaged in basic negotiations with the EU, while keeping the programme up and running.

Using its new powers, acquired when the Lisbon Treaty came into force, the European Parliament in February struck down the interim agreement, interrupting the data flow for half a year. A final agreement was subsequently negotiated by the EU commission, with extra privacy and oversight provisions,

[REDACTED] (b)(6)
Sent: Monday, January 05, 2009 7:05 PM

[REDACTED] (b)(6)
Subject: NYT Article
[REDACTED] (b)(6)

January 5, 2009

Kidnappings in Mexico Send Shivers Across Border

By SAM DILLON

FELIPE ANGELES, Mexico — Four hooded men smashed in the door to the adobe home of an 80-year-old farmer here in November, handcuffing his frail wrists and driving him to a makeshift jail. They released him after relatives and friends paid a \$9,000 ransom, which included his life savings.

The kidnapping was a dismal story of cruelty and heartbreak, familiar all across Mexico, but with a new twist: the daughter of this victim lived in the United States and was able to wire money to help assemble his ransom, the farmer, who insisted that he not be identified by name, said in an interview.

A string of similar kidnappings, singling out people with children or spouses in the United States, so panicked this village in the state of Zacatecas that many people boarded up their homes and headed north, some legally and some not, seeking havens with relatives in California and other American states.

“The relatives of Mexicans in the United States have become a new profit center for Mexico’s crime industry,” said Rodolfo García Zamora, a professor at the Autonomous University of Zacatecas who studies migration trends. “Hundreds of families are emigrating out of fear of kidnap or extortion, and Mexicans in the U.S. are doing everything they can to avoid returning. Instead, they’re getting their relatives out.”

The reported rush into the United States by people from the state of Zacatecas is another sign that Mexico’s growing lawlessness is a volatile new factor affecting the flow of migrant workers across America’s border. The violence is adding a new layer of uncertainty to the always fraught issue of Mexican emigration, already in flux because of the economic downturn in the United States.

Academics and policy makers on both sides of the border, who are watching closely for shifts in migration patterns, say it is too early to know the long-term impact of either the drug-related violence or the loss of jobs by thousands of migrant workers in the United States. But so far, earlier predictions of an exodus of out-of-work Mexicans back to their hometowns seem to have been premature.

Instead, it appears that the pattern in the state of Zacatecas — where many people have family in the United States — may be a good indicator of what is happening throughout Mexico. The country’s spiraling criminality appears not only to be keeping some Mexicans in the United

States, but it may also be leading more Mexicans to flee their country. "It's a toxic combination right now," said Denise Dresser, a political scientist based in Mexico City. "Mexicans north of the border are facing joblessness and persecution, but in their own country the government can't provide basic security for many of its citizens."

The extraordinary increase in violence in Mexico in recent years has resulted in part from President Felipe Calderón's war against drug lords. His campaign to arrest the leaders of the cartels and the military officers and law enforcement officials they have compromised has unleashed factional fighting among rival drug groups, as well as violence against the government.

Traditionally, most of Mexico's criminal violence has been concentrated in northern border cities like Tijuana where cocaine enters the United States. But law and order have been deteriorating in many regions; and heartland states like Michoacán, Jalisco and Zacatecas, which are the homes of millions of migrants to the United States and are longtime drug smuggling routes, are now also reporting spikes in killings and kidnappings.

Jerez, a town of 60,000 a few miles northwest of Felipe Angeles in Zacatecas, was until recently a calm place, largely untouched by organized crime, said Abel Márquez Haro, a grocery wholesaler.

But recently, scores of men driving Chevrolet Suburbans and carrying automatic rifles established a menacing presence, threatening residents on the street and extorting businesspeople. The identities of the men remain a mystery, but many people in the town say they assume they are traffickers who have abandoned another Mexican state, perhaps to avoid an army crackdown.

On Nov. 10, a dozen of the gunmen arrived at Mr. Márquez's warehouse, dragging him out, bashing him and several employees with rifle butts and then hauling him away. He was held blindfolded for 30 hours as the kidnapers demanded \$500,000 for his freedom, Mr. Márquez said in an interview. Eventually his family agreed to a smaller ransom, Mr. Márquez said. When his son delivered the money, the kidnapers released Mr. Márquez but seized his son, demanding a second ransom, which the family also paid, Mr. Márquez said.

He is trying to sell his business, he said, and hopes to relocate to some safer city in Mexico. But he said that a friend who witnessed his kidnapping was so rattled that he had since gone to live with a brother in California.

Residents described several other recent kidnappings and extortions across the state of Zacatecas: a cattleman held until a daughter in Las Vegas sent money to help pay a \$35,000 ransom; a rancher who was tied to a tree during a five-day period of captivity; a car-parts dealer who avoided capture by immediately paying gunmen the ransom they demanded.

Those who live in the region say such crimes — and the attention they receive on Spanish-language television in the United States — appear to have frightened not only those who live here year-round. Most years at Christmastime, hundreds of men in cowboy hats who work north of the border return to Jerez, jamming the streets with pickup trucks and cars with California and Illinois license plates and reuniting with old friends and family in the town square.

This holiday season, Jerez and surrounding towns have had few migrants return. And demographers based in Jalisco and Michoacán said in interviews that few migrants had returned to those states either.

Those reports surprised many who study immigration, including Douglas S. Massey, a sociology professor at Princeton University.

“What I thought would be happening this Christmas is that more migrants would go home to Mexico than usual and just stay there,” Dr. Massey said. Surveys of Mexican migrants that he conducted last summer in North Carolina after a large poultry processing plant closed there showed that “people were heading back to Mexico because they couldn’t find another job” and because federal raids had spread so much fear among migrants, he said.

“People were saying, ‘If it’s a matter of surviving day to day, I’d rather do that in Mexico,’ ” Dr. Massey said.

Other experts also expected to see larger than usual flows of Mexicans home this Christmas. A caucus of Mexican legislators who specialize in migration issues predicted in October that some three million Mexicans might return from the United States as a result of the recession. But the same group reported in a study released in late December that in fact fewer migrants seemed to have returned this holiday season than in previous years, in part because of what they delicately termed “the insecurity in Mexico.”

And in Felipe Angeles, the flow of people ran north rather than south at year-end.

Residents here were so frightened by the kidnappings of the octogenarian and of about a dozen other people who lived in or near this village in recent months that hundreds of them set up a roadblock with their tractors and trucks on the main highway here last month. They demanded that the army send troops to protect them. Soldiers were deployed to patrol the town for a few days, but that did not leave the residents feeling secure.

“The kidnappers were targeting people with relatives in the United States, because they knew these families have money,” said Santana Lujan, a local farmer who participated in the blockade. “It’s left a psychosis of fear and worry.”

A teacher who spoke on the condition of anonymity estimated that of the town’s 400 houses, about 200 were now vacant, with 50 of them emptied in recent weeks. About half of the departing families left for the United States, he said, while the rest sought safety elsewhere in Mexico.

In an interview, the 80-year-old man who was kidnapped trembled when describing his six-day captivity. He said he was repeatedly kicked by his captors.

His daughter has since urged him to go live with her in the United States, but he said he felt too old to emigrate.

“But many people have left,” he said, “and more are going to leave.”

(b)(6)
RE Washington Regulatory Update

Sent: Wednesday, March 05, 2008 1:33 PM

(b)(6)
Subject: RE: Washington Regulatory Update

Money Laundering: Bankers Taking On Goods-Based Fraud A new anti-money laundering tool incorporated by SAS charts irregularities on clients' import/export invoices and improves the overall compliance infrastructure

Bank Technology News | Saturday, March 1, 2008

By Glen Fest

Asking banks to track potential anti-money laundering activity through traded goods is easier mandated than done.

Since 2005, the FFIEC exam manual has required institutions to have a policy or process to monitor letter-of-credit or international supply-chain activity flowing through their systems. A long-time tax dodge, trade-based fraud came under tighter scrutiny more recently as a potential source of in-bound terrorist financing via the balance of value from over- or under-priced imports and exports.

But bankers have struggled since in managing their charge, say financial forensic experts. A major problem is the lack of in-house expertise to interpret the data sets of prices, companies, products and countries that the FFIEC expects them to document.

"Banks should have the information contained in US custom documents," says John Zdanowicz, a Florida International University professor and an oft-cited authority on offshore money movement.

Zdanowicz learned cross-border trade financiers' anxiety first-hand last year when members of the Florida International Bankers Association flooded him with questions (after a Web seminar) on how they could better develop and document their price acumen for clients' traded goods. Having just completed research on a \$2 million U.S. Treasury grant on tax-avoidance transfer pricing trends, Zdanowicz used the work to put together an international pricing system software package for institutions that provides analytic risk assessment models to examine trade invoices.

With the inclusion of tax evasion and other illicit cross-border funding activity, Zdanowicz thinks abnormal trade pricing is moving \$190 billion offshore each year. The amount coming in is about \$240 million. Zdanowicz once estimated the U.S. loses \$53 billion in tax revenue each year to abnormally-priced goods.

His new global price profiling system went live last year as an online tool offered through his own company - International Trade Alert - and in an alliance with anti-fraud software firm SAS Institute, which will market the price profile system alongside its more standard watchdog activities (such as watchlist checking, wire-transfer monitoring, etc.).

Although uptake of the price profiling system has been limited to a pilot with an unnamed California institution, SAS AML solutions director David Stewart says he's discussed with several top-tier banks the need "to automate [trade AML] processes, with a need to digitize a lot of information that today is either experiential or lies within a letter of credit."

Another AML compliance firm, Fortent, is working with user groups to in hopes of developing a trade-transaction tracking tool by the end of the year, according to Fortent chief scientist Michael Recce. "It's easy to automate checks against OFAC watchlists and suspicious regional origins," says Recce.

RE Washington Regulatory Update

"What's hard to look for is appropriate pricing, or appropriate countries of origin and destination."

Zdanowicz' price profiling system uses regularly updated U.S. customs data to gather a price database on all goods from all nations. The system statistically profiles all known prices for those goods—only those that fall below five percent or above 95 percent get flagged for overview.

The models measure not only price-to-quantity, but also price-to-product. Banks can more easily determine if an invoice for a shipment of watches is spurious if they know whether it contains Swiss masterpieces or a pile of cheap knockoffs. Zdanowicz' company produces product and country trade reports culled from data of U.S. customs districts. Zdanowicz also recently co-developed for U.S. Customs an abnormal weight detection system, which at some point might be added to the pricing profile system.

Without new technology, most banks find that tracking product and country-of-origin particulars requires manual intervention that can't be wrapped into existing automated AML compliance suites. Some international trade-finance operations at global money-center banks sift through 10,000 letters-of-credit daily, by hand. So while not "knee-deep" in technology, says Aite Group senior analyst Nancy Atkinson, "Trade finance people are aware they need to be watching this." (c) 2008 Bank Technology News and SourceMedia, Inc. All Rights Reserved. <http://www.banktechnews.com> <http://www.sourcemedia.com>

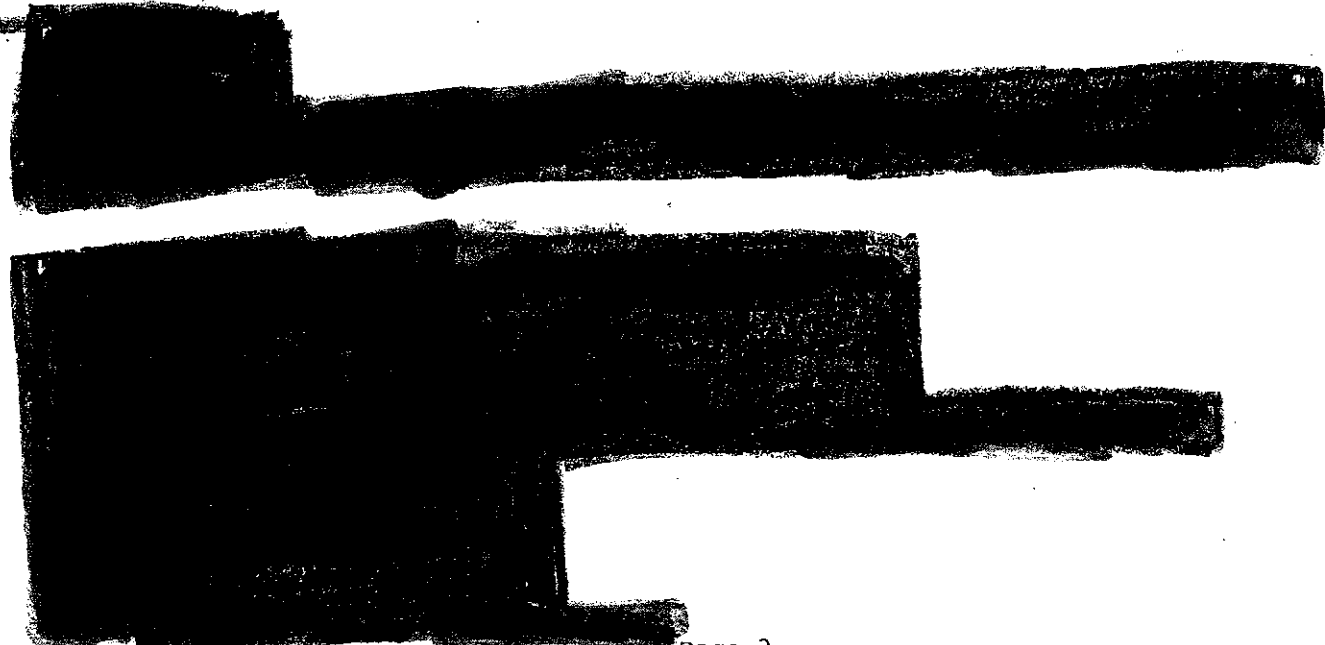
© 2008 American Banker and SourceMedia, Inc. All Rights Reserved. SourceMedia is an Investcorp company. Use, duplication, or sale of this service, or data contained herein, except as described in the subscription agreement, is strictly prohibited.

For information regarding Reprint Services please visit:
<http://www.americanbanker.com/reprint-services-rates.html>

-----Original Message----- (b)(6)

Sent: Wednesday, March 05, 2008 1:32 PM (b)(6)

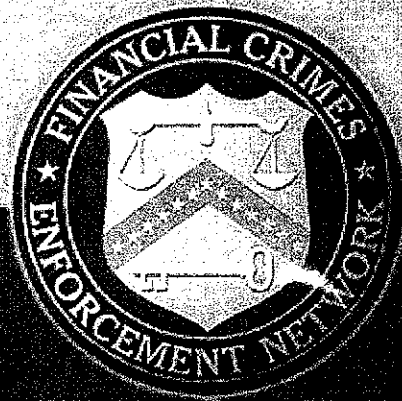
Subject: Fw: Washington/Regulatory Update



83

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS COVER PAYMENTS

James H. Freis, Jr. – Director
16th Egmont Group Plenary Session and Working Group Meetings
(... May - June 2008)



TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS

PRESENTATION GOALS

Goal:

High-level review of the application of transparency principles to the processing of cover payments, a specific type of cross-border wire transfer transactions.



85

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS

TRANSPARENCY

From its beginning, anti-money laundering/counter-terrorism financing strategies sought to increase transparency in all financial transactions.

- Complete identification of the parties to and increased information about the purpose of a financial transaction contribute to a better protection of the financial system against abuse.

- Increased transparency improves risk assessment at financial institutions, by facilitating due diligence/enhanced due diligence on customers and correspondent banks, and contributing to more precise user profiling and transaction testing.

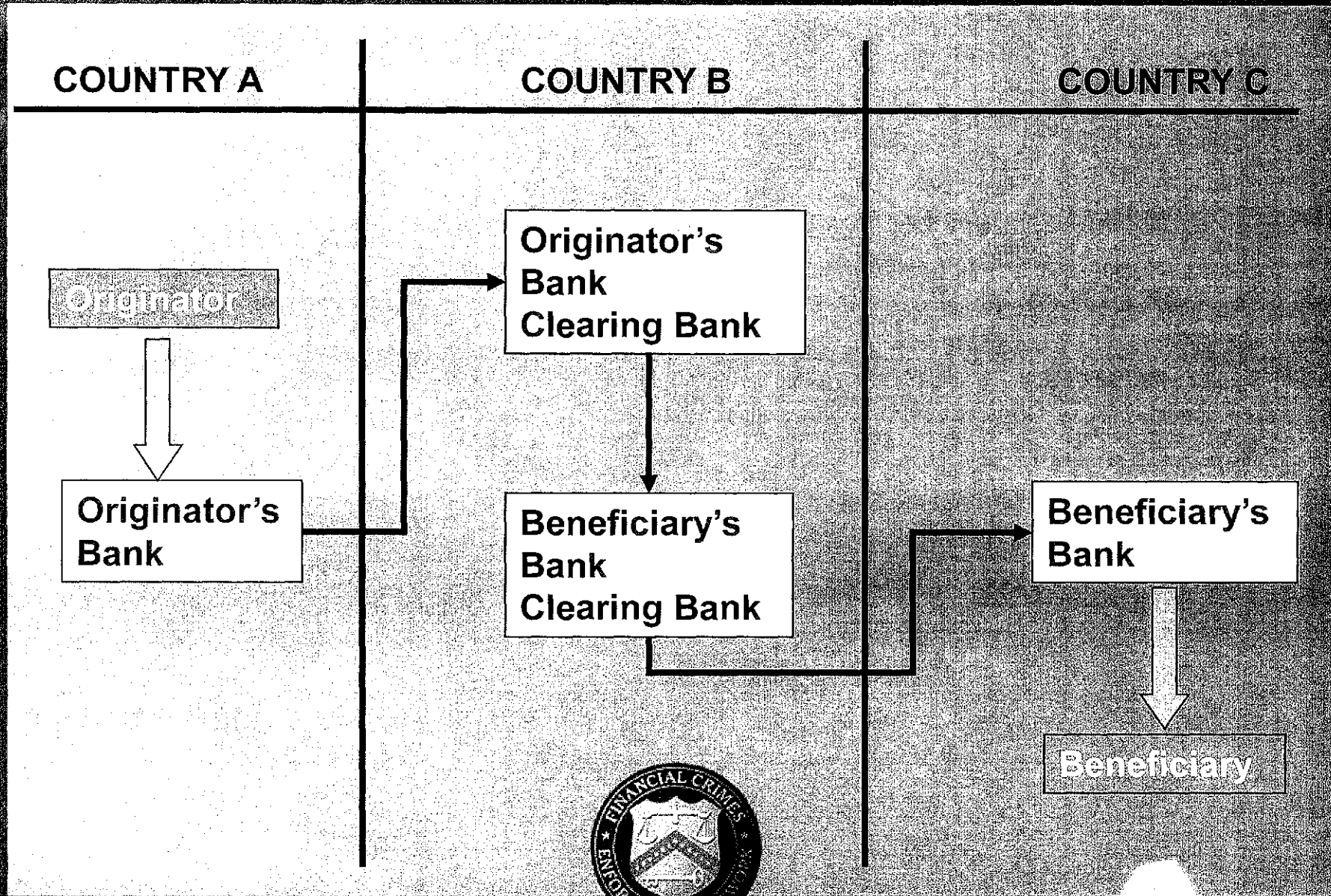
- Increased transparency helps in the prevention, detection, and correction of abuse of financial systems, by enriching the information provided to law enforcement and financial intelligence units.



9/8

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS

CROSS-BORDER WIRE TRANSFERS



13

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS

INTERNATIONAL MESSAGING STANDARDS

SWIFT

- SWIFT is a widely used international secure messaging system for delivering cross-border payment instructions.
- SWIFT supplies secure, standardized messaging services and interface software that create a uniform formatting platform.
- SWIFT's uniform formatting platform allows for straight-through processing (STP) by participating banks.



TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS INTERNATIONAL MESSAGING STANDARDS

SWIFT MESSAGE TYPES

THIRD-PARTY PAYMENTS (MT 103)

- Used for payments made on behalf of third parties.
- Has the capacity to carry full information about originator, beneficiary, and sender-to-receiver information

INTER-BANK PAYMENTS (MT 202)

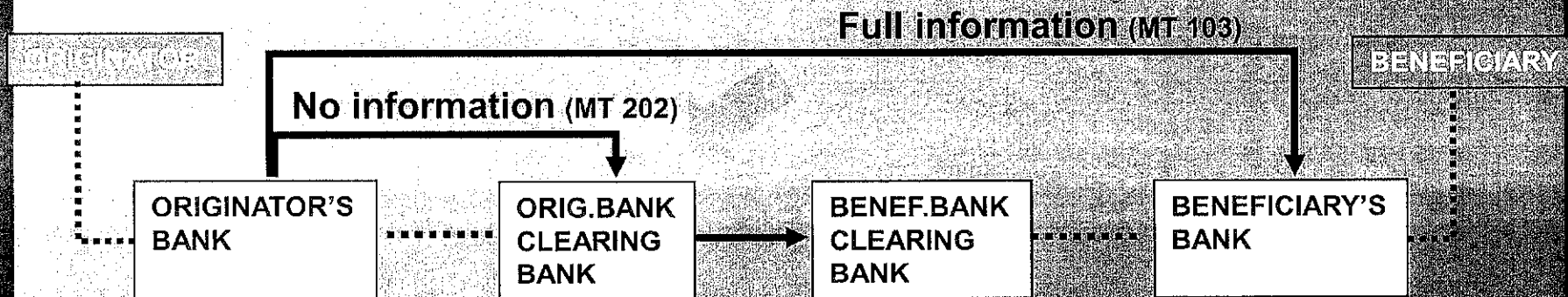
- Used for payments made by one bank, directly or through a correspondent bank, to another bank, on its own behalf.
- Has the capacity to carry very limited information.



TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS

COVER PAYMENTS - DEFINITION

In wire transfers involving cover payments, the payment order and the reimbursement instructions for the payment order are sent separately, and contain different levels of transactional information:



- **First Message (from Originator's Bank to Beneficiary's Bank)**
giving full details about the originator and beneficiary of the transfer
- **Second Message (from Originator's Bank to Intermediary Bank)**
giving minimal or no details about the originator and beneficiary



TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS COVER PAYMENTS - IMPACT ON TRANSPARENCY

**BY MASKING THE IDENTITY OF ORIGINATORS,
FINAL BENEFICIARIES, OR BOTH, COVER
PAYMENTS CONSTITUTE A HIGH BSA/AML RISK:**

- THEY INTERFERE WITH DOMESTIC TRANSFER
RULES**
- THEY VIOLATE GLOBAL TRANSPARENCY
PRINCIPLES (SUCH AS FATF SPECIAL
RECOMMENDATION NO. 7 ON WIRE TRANSFERS)**
- THEY MIGHT BE USED TO FOSTER MONEY
LAUNDERING AND TERRORIST FINANCING**



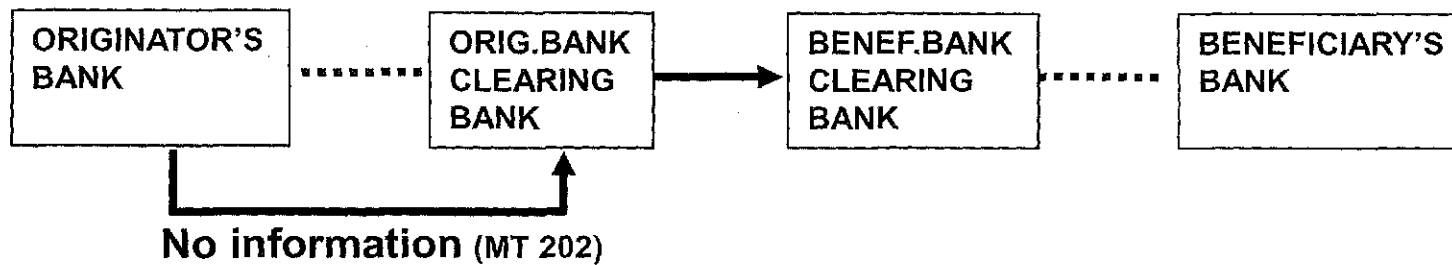
TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS COVER PAYMENTS -STANDARDS MODIFICATION TIMELINE

Mid-2006	Industry identifies vulnerability of cover payments to abuse.
Early 2007	Industry sets global payment messaging best practices.
Mid-2007	Industry petitions SWIFT for modification to message standards.
Late 2007	SWIFT proposes new message standard to members and request country vote.
Early 2008	New message standard approved by SWIFT members.
Late 2009	New SWIFT message standard goes live.



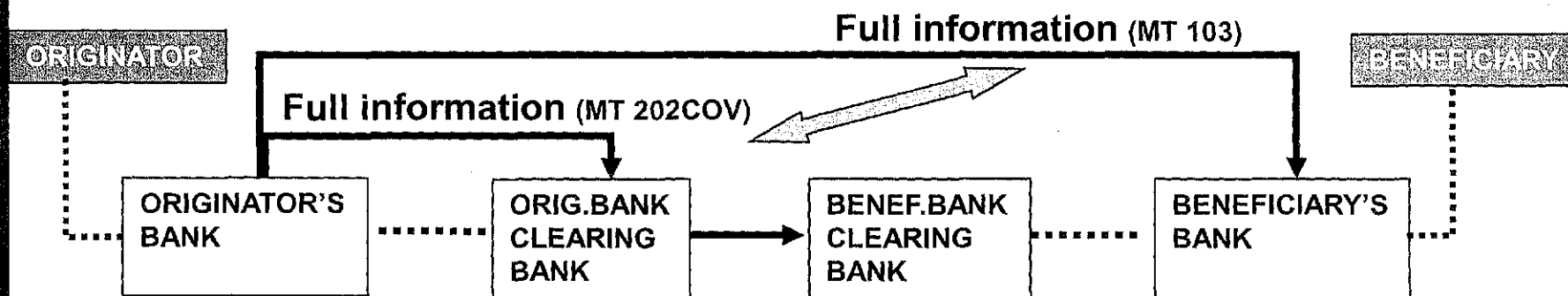
TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS MESSAGING STANDARD MODIFICATIONS – APPLICATION

INTER-BANK TRANSFER



THIRD-PARTY TRANSFER

92



TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS MESSAGE STANDARDS MODIFICATION - RELEVANCE

COVER PAYMENTS STANDARDS MODIFICATION

Importance of the modification in the standard:

- Exponential increase in transparency for all parties involved in the transaction

Importance of the process through which the modification was requested

- Modification of standards spearheaded by industry
- Seeking to upgrade a serviceable, widely-adopted payment method
- In order to gain improved regulatory transparency



74

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS FINANCIAL INDUSTRY'S GLOBAL PRINCIPLES

Wolfsberg Group/TCH Statement on Payment Message Standards:

Four payment message principles to be observed by all financial institutions:

Financial institutions should not

- omit, delete or alter information
- use any particular payment message for the purpose of obscuring information

Financial institutions should

- cooperate with other financial institutions
- encourage their correspondent banks to follow these principles.



95

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS DOMESTIC PAYMENT SYSTEMS- ADAPTATION

DOMESTIC PAYMENT SYSTEMS

- Domestic electronic payment systems (1) , currently may be able to provide pass-through capabilities for existing international message standards (SWIFT third-party transfer –MT 103- or inter-bank transfer –MT 202 – standards).
- They may have to undergo modifications to provide the same pass-through capabilities for the new standard (SWIFT enhanced cover payment inter-bank transfer – MT 202 COV – standard).

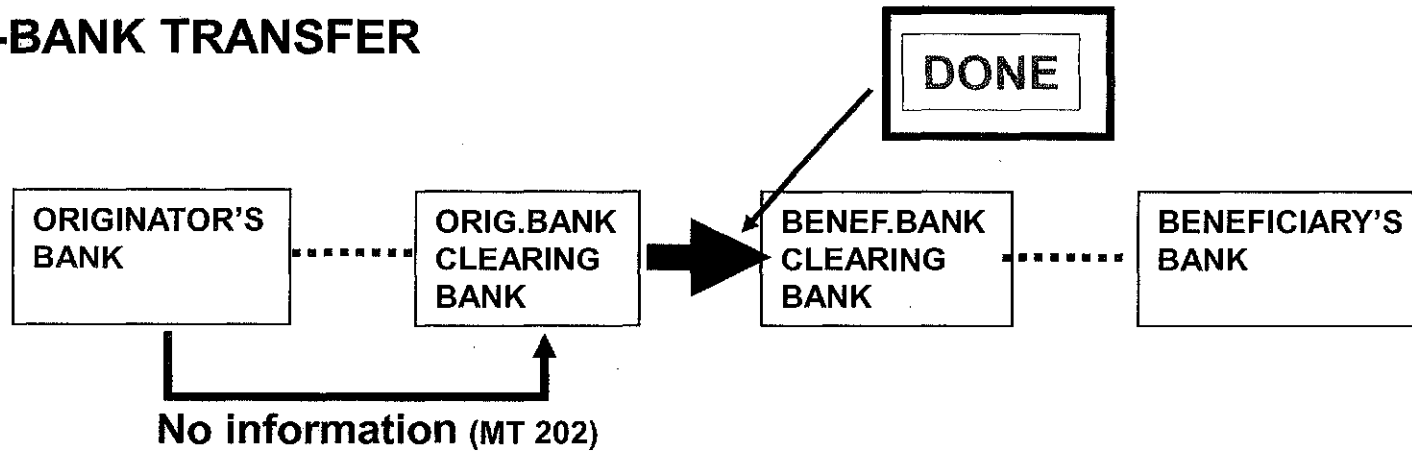
(1) Such as:

CHIPs, Fedwire, ACH, in the US
SEPTA, in the European Union
BOJ-Net, Zengin, in Japan

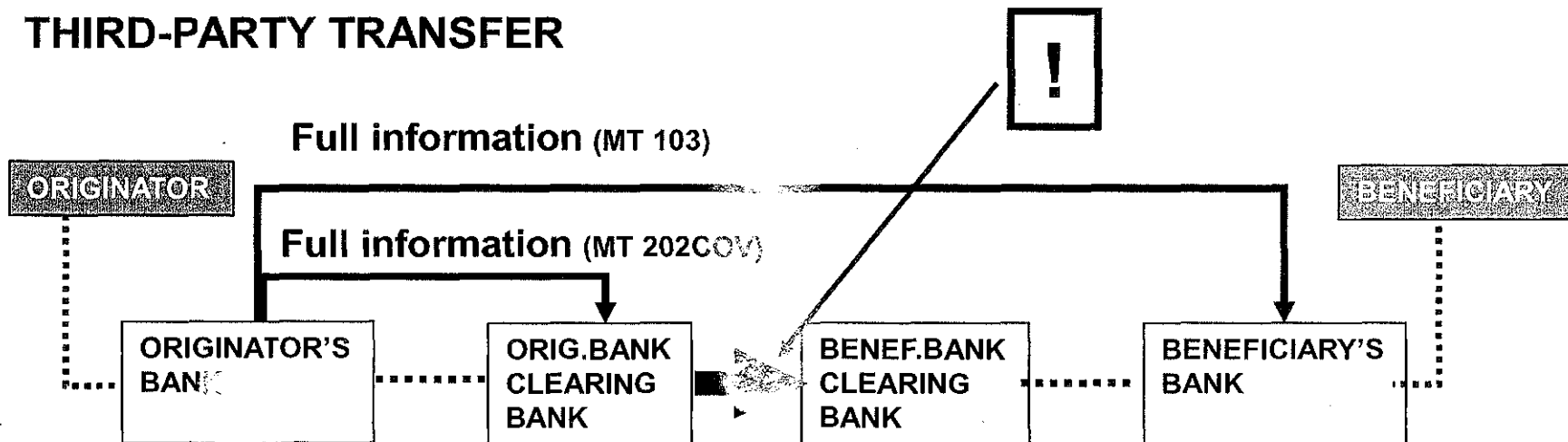


TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS DOMESTIC PAYMENT SYSTEMS - ADAPTATION

INTER-BANK TRANSFER



THIRD-PARTY TRANSFER



97

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS EXPECTED END RESULT

**NEW GLOBAL PAYMENT MESSAGE PRINCIPLES AND NEW
COVER PAYMENT MESSAGE STANDARDS CAN BE EXPECTED
TO PROVIDE INCREASED TRANSPARENCY**

Individual financial institution	Due diligence/enhanced due diligence User profiling and transaction testing Risk assessments.
Domestic/ Global financial system	Information provided to law enforcement and financial intelligence units. Prevention, detection, and correction of abuse of financial systems

**ONLY IF UNIVERSALLY ADOPTED, AND USED CORRECTLY
AND CONSISTENTLY IN EVERY JURISDICTION.**



AD

TRANSPARENCY IN CROSS-BORDER WIRE TRANSFERS COVER PAYMENTS

**James H. Freis, Jr. – Director
16th Egmont Group Plenary Session and Working Group Meetings
(... May - ... June 2008)**



(b)(5);(b)(6)

From: [redacted]
Sent: Friday, October 15, 2010 10:05 AM
To: [redacted]
Subject: FW: Meeting with SWIFT

FYI.

From: [redacted]@swift.com]
Sent: Thursday, October 14, 2010 5:39 PM
To: [redacted]
Cc: [redacted]
Subject: FW: Meeting with SWIFT

Hello [redacted] as you can see from the below, [redacted] is taking a leadership role from the SWIFT side regarding the new FinCEN regulation. I would like to introduce you to [redacted] and further our discussions as we recently agreed.

From: [redacted]
Sent: Thursday, October 14, 2010 5:25 PM
To: [redacted]
Cc: [redacted]
Subject: Meeting with SWIFT

Dear [redacted]

In 2007, you and members of the FinCEN team met with [redacted] and a team from SWIFT. The objective was to learn about SWIFT messaging and product capabilities.

Your proposed Rule on Cross Border Electronic Transmittal of Funds was released the week of September 27, 2010 and is now in the 90 day comment period.

We are receiving inquiries from the financial community on a business and technical level. If possible, we would like to arrange a meeting with your team to discuss the following:

1. The SWIFT FinInform reporting model that can be configured to transmit the MT 103 and MT 202 COV messages based upon Country BIC codes
2. The Money Transmitter Reporting model and the use of standard reporting formats via SWIFT Alliance Lite, a web based SWIFT model.
3. The central data repository that will receive and become the data warehouse for the Cross Border payment messages which are then used for further analytics.

We do not wish to do anything outside of the process outlined in the Proposed Rulemaking, but we believe such a session would better enable us to answer questions from the financial community as well as providing you with a current understanding of SWIFT and its messaging.

Please let me know if we can schedule such a meeting.

Regards,

100

(b)(6)



Standards - Banking Initiatives
SWIFT Pan Americas
7 Times Square
New York, New York 10036
NY Tel: +1 212 455 1853
Mobile: +1 347 803 0639

This e-mail and any attachments thereto may contain information which is confidential and/or proprietary and intended for the sole use of the recipient(s) named above. If you have received this e-mail in error, please immediately notify the sender and delete the mail. Thank you for your co-operation. SWIFT reserves the right to retain e-mail messages on its systems and, under circumstances permitted by applicable law, to monitor and intercept e-mail messages to and from its systems.

Please visit <http://www.swift.com> for more information about SWIFT.

sibos 2010 Association
Market Infrastructures in Latin America:
Innovating their way into the future
Now from Chile, Brazil and Mexico
LEARN more >

(b)(6)

[REDACTED]

From: [REDACTED]

Sent: Thursday, September 30, 2010 7:21 AM

[REDACTED]

Subject: Cross-Border NPRM Question

[REDACTED]

I understand you have some questions regarding the recent NPRM published by FinCEN. I would be happy to discuss. Feel free to email me or call at the number below.

[REDACTED]

Appendix C: Business Use Cases

Federal Bureau of Investigation (FBI)

Reactive Analysis: Terrorist Financing Investigations

Business Objective

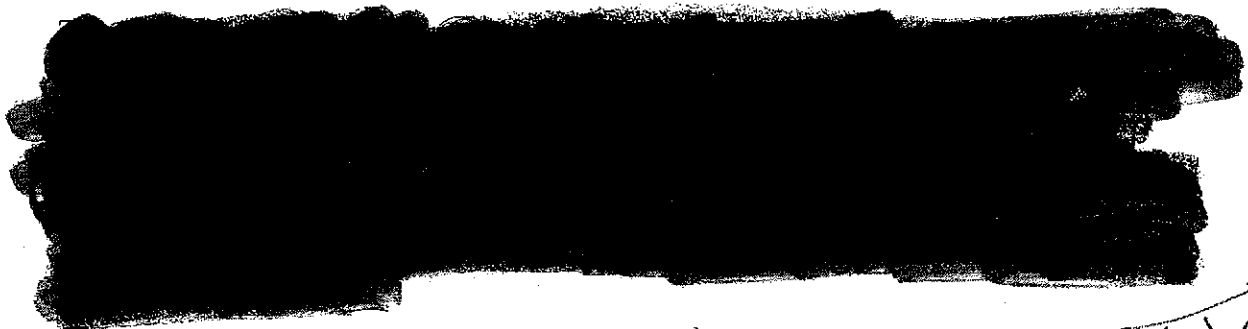
Improve the efficiency of FBI analysts investigating targets suspected of engaging in terrorist financing.

Background and Description

In its effort to safeguard the United States, the FBI works to defend our nation against terrorist and foreign intelligence threats and to enforce our country's criminal statutes. To defend our nation against terrorist and foreign intelligence threats, the FBI has established three national security priorities: counterterrorism, counterintelligence, and cybercrime.

As part of the National Security Branch, the FBI's Counterterrorism Division leads a vast national and international campaign dedicated to defeating terrorism. Working with partners in the Law Enforcement, intelligence, military, and diplomatic communities, the Counterterrorism Division works to neutralize terrorist cells and operatives in the United States and to help dismantle terrorist networks worldwide. The priorities of the Counterterrorism Division include the detection, disruption, and dismantling of terrorist sleeper cells in the United States, the identification and prevention of acts of terrorism by individuals with a terrorist agenda acting alone, and the interdiction of terrorist support networks, including financial support networks, both domestically and abroad.

Building on the FBI's expertise in conducting complex criminal financial investigations and long-established relationships with the financial services sector, the Counterterrorism Division established the Terrorism Financing Operations Section (TFOS) to centralize efforts to track and shutdown terrorist financing, exploit financial information in an effort to identify previously unknown terrorist cells, and recognize potential terrorist activities and planning.



(b)(5), (b)(7)

Stakeholders/Beneficiaries

Federal Bureau of Investigation (FBI)

Proactive Analysis: Disrupting Transnational Organized Crime Syndicates

Business Objective

Improve the ability of FBI analysts to proactively identify new targets suspected of engaging in money laundering associated with transnational organized crime syndicates.

Background and Description

In its effort to safeguard the United States, the FBI works to defend our nation against terrorist and foreign intelligence threats and to enforce our country's federal criminal statutes. To defend our nation against terrorist and foreign intelligence threats, the FBI has established three national security priorities: counterterrorism, counterintelligence, and cybercrime. To enforce the criminal laws of the United States, the FBI has established five criminal priorities: white-collar crime, public corruption, civil rights, major thefts/violent crime, and organized crime.

One of the most significant criminal priorities of the FBI is organized crime. Transnational organized crime syndicates strangle free enterprise and raise the level of violence, fraud, and corruption in cities throughout the United States. To combat this threat, the FBI employs a range of investigative capabilities, including undercover operations, intelligence analysis, and the power of racketeering statutes to assist in the disruption and dismantling of organized crime syndicates. Working closely with international partners, the FBI seeks to dismantle syndicates with global ties by identifying and disrupting the financial networks used to launder the proceeds generated from organized crime.

(b)(5); (b)(7)

[REDACTED]

[REDACTED]

United States Immigration and Customs Enforcement (ICE)

Proactive Analysis: Trade-Based Money Laundering Investigations

Business Objective

Improve the ability of ICE analysts to proactively identify new targets suspected of engaging in trade-based money laundering.

Background and Description

In their efforts to identify and eliminate customs fraud and trade-based money laundering, the United States Immigration and Customs Enforcement (ICE) has established Trade Transparency Units (TTUs) worldwide. These TTUs have enhanced international cooperative investigative efforts to combat activities designed to exploit vulnerabilities in the United States financial and trade systems.

As formal international financial systems become more highly regulated and transparent, criminal entities have resorted to alternative means of laundering illicit proceeds. Fraudulent practices in international commerce allow criminals to launder illicit funds while avoiding taxes, tariffs, and customs duties.

(S)(S)
(b)(7)

[REDACTED]

Stakeholders/Beneficiaries

[REDACTED]

Assumptions & Constraints

[REDACTED]

United States Immigration and Customs Enforcement (ICE)

Reactive Analysis: Transnational Money Laundering Investigations

Business Objective

Improve the efficiency of ICE analysts investigating targets suspected of engaging in illicit financial activity.

Background and Description

In their effort to protect the United States against terrorist attacks, ICE targets the people, money, and materials that support terrorism and other criminal activities. As part of that effort, ICE agents and analysts aggressively seek to destroy the financial infrastructure that criminal organizations use to earn, move, and store illicit funds.

As formal financial systems become more regulated and transparent, criminal entities have resorted to alternative and increasingly complex means of moving and laundering illicit proceeds. To combat such threats, ICE conducts sophisticated analysis to identify illicit financial activity.

[REDACTED]

(b)(5)
(7)

Stakeholders/Beneficiaries

[REDACTED]

Assumptions & Constraints

[REDACTED]

Department of the Treasury Financial Crimes Enforcement Network

Reactive Analysis: Improved BSA Link Analysis Capabilities

Business Objective

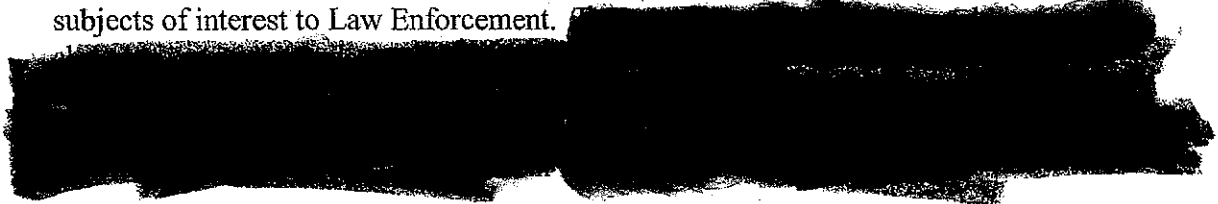
Improve the ability of FinCEN analysts to identify and link BSA records with subjects of interest to Law Enforcement.

Background and Description

In its effort to safeguard the financial system from the abuses of financial crime, the Financial Crimes Enforcement Network (FinCEN) works to detect and deter money laundering, terrorist financing, and other illicit activity. To combat these threats, FinCEN administers the Bank Secrecy Act (BSA). The BSA requires all financial institutions to maintain appropriate records and to file reports that are used in criminal, tax, and regulatory investigations. BSA filings aid Law Enforcement agencies in the investigation of suspected criminal activity such as narcotics trafficking, income tax evasion, and money laundering.

As formal financial systems become more regulated and transparent, criminal entities have resorted to alternative and increasingly complex means of moving and laundering illicit proceeds. To combat these threats, FinCEN conducts advanced analysis of BSA records to support Law Enforcement agencies in the detection and deterrence of illicit financial activity.

To support Law Enforcement, FinCEN analysts conduct sophisticated analysis, cross-referencing multiple disparate data sources, to identify financial transactions indicative of money laundering, terrorist financing, or other illicit activity. The identification of these transactions is often dependent on the ability of FinCEN analysts to link BSA records with subjects of interest to Law Enforcement.



Stakeholders/Beneficiaries



(b)(5)
(b)(7)

Department of the Treasury Financial Crimes Enforcement Network

Proactive Analysis: Shell Company International Fund Flow Identification

Business Objective

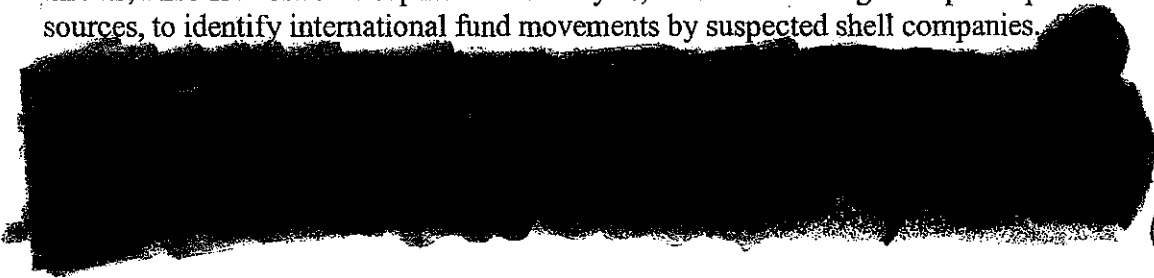
Improve the ability of FinCEN analysts to proactively identify international fund movements by suspected shell companies.

Background and Description

In its effort to safeguard the financial system from the abuses of financial crime, the Financial Crimes Enforcement Network (FinCEN) works to detect and deter money laundering, terrorist financing, and other illicit activity. To combat these threats, FinCEN administers the Bank Secrecy Act (BSA). The BSA requires all financial institutions to maintain appropriate records and to file reports that are used in criminal, tax, and regulatory investigations. BSA filings aid Law Enforcement agencies in the investigation of suspected criminal activity such as terrorist financing, money laundering, and narcotics trafficking.

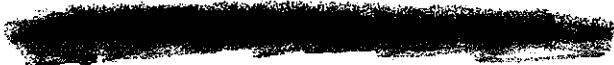
As formal financial systems become more regulated and transparent, criminal entities have resorted to alternative and increasingly complex means of moving and laundering illicit proceeds. These entities often seek to exploit vulnerabilities in the United States financial system by using vehicles such as shell companies. By virtue of the ease of formation and the absence of ownership disclosure requirements, shell companies, generally defined as business entities without active business or significant assets, are attractive vehicles for those seeking to launder money or conduct illicit financial activity. While shell companies may have legitimate commercial uses, the lack of transparency in the formation process poses vulnerabilities to the financial system both domestically and abroad.

The use of shell companies as parties in international funds transmittals allows for the movement of billions of dollars in funds by unknown beneficial owners and may be used to facilitate financial crimes such as terrorist financing and money laundering. To combat these threats, FinCEN conducts sophisticated analysis, cross-referencing multiple disparate data sources, to identify international fund movements by suspected shell companies.



(S) (b) (5)

Stakeholders/Beneficiaries



Department of the Treasury Financial Crimes Enforcement Network

Proactive Analysis: Identification and Assessment of Illicit Transnational Currency Flows

Business Objective

Improve the ability of FinCEN analysts to proactively identify and assess illicit transnational currency flows.

Background and Description

In its effort to safeguard the financial system from the abuses of financial crime, the Financial Crimes Enforcement Network (FinCEN) works to detect and deter money laundering, terrorist financing, and other illicit activity. To combat these threats, FinCEN administers the Bank Secrecy Act (BSA). The BSA requires all financial institutions to maintain appropriate records and to file reports that are used in criminal, tax, and regulatory investigations. BSA filings aid Law Enforcement agencies in the investigation of suspected criminal activity such as terrorist financing, money laundering, and narcotics trafficking.

FinCEN conducts sophisticated analysis of BSA data to provide strategic analytical support to Law Enforcement through the identification of trends, patterns, and issues associated with illicit financial activity. Strategic analysis products are intended to assist partners in the improvement of money laundering prevention and detection programs while providing support for the enforcement of anti-money laundering laws and regulations. Through the strategic analysis of BSA data, FinCEN seeks to identify newly emerging or inadequately understood money laundering methodologies, examine geographic, industry, and other systemic money laundering vulnerabilities, and provide support to federal, state, local, and international Law Enforcement agencies investigating complex financial crimes.



Stakeholders/Beneficiaries



(b)(5)
(b)(7)

Drug Enforcement Administration (DEA)

Proactive Analysis: Controlled Substance Investigations

Business Objective

Improve the ability of DEA analysts to proactively identify new targets suspected of engaging in narcotics trafficking and drug related money laundering.

Background and Description

In its effort to enforce our nation's controlled substance laws and regulations, the Drug Enforcement Administration (DEA) works to bring to justice those organizations involved in the growing, manufacture, or distribution of controlled substances destined for illicit traffic in the United States. Through the investigation and preparation for prosecution of criminals, drug gangs, and other major violators of controlled substance laws, the DEA seeks to reduce the availability of illicit controlled substances on the domestic and international markets.

To combat the illicit trafficking of controlled substances in the United States, the DEA manages a national drug intelligence program to collect, analyze, and disseminate strategic and operational drug intelligence information. Such intelligence is essential to the DEA's efforts to interdict the distribution of narcotics and disrupt and dismantle drug trafficking organizations. A critical component of these efforts is the DEA's ability to detect and deter the laundering of proceeds generated from the sale of illicit drugs.

As formal financial systems become more regulated and transparent, drug trafficking organizations have resorted to diversified and increasingly complex means of laundering the proceeds from the sale of illicit drugs. These entities often seek to exploit vulnerabilities in the United States financial system to launder funds and transport the proceeds overseas or repatriate those proceeds back into the United States for integration and use.

(S/L)
2/1/10



Stakeholders/Beneficiaries



Drug Enforcement Administration (DEA)

Reactive Analysis: Controlled Substance Investigations

Business Objective

Improve the efficiency of DEA analysts investigating targets suspected of engaging in narcotics trafficking and drug related money laundering.

Background and Description

In its effort to enforce our nation's controlled substance laws and regulations, the Drug Enforcement Administration (DEA) works to bring to justice those organizations involved in the growing, manufacture, or distribution of controlled substances destined for illicit traffic in the United States. Through the investigation and preparation for prosecution of criminals, drug gangs, and other major violators of controlled substance laws, the DEA seeks to reduce the availability of illicit controlled substances on the domestic and international markets.

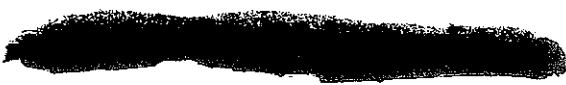
To combat the illicit trafficking of controlled substances in the United States, the DEA manages a national drug intelligence program to collect, analyze, and disseminate strategic and operational drug intelligence information. Such intelligence is essential to the DEA's efforts to interdict the distribution of narcotics and disrupt and dismantle drug trafficking organizations. A critical component of these efforts is the DEA's ability to detect and deter the laundering of proceeds generated from the sale of illicit drugs.

As formal financial systems become more regulated and transparent, drug trafficking organizations have resorted to diversified and increasingly complex means of laundering the proceeds from the sale of illicit drugs. These entities often seek to exploit vulnerabilities in the United States financial system to launder funds and transport the proceeds overseas.

(S)(G)
(6)(7)



Stakeholders/Beneficiaries



Assumptions & Constraints

United States Immigration and Customs Enforcement (ICE)

Proactive Analysis: Trade-Based Narcotics Investigations

Business Objective

Improve the ability of ICE analysts to proactively identify new targets suspected of engaging in narcotics trafficking.

Background and Description

In their efforts to identify and eliminate customs fraud and trade-based money laundering, the United States Immigration and Customs Enforcement (ICE) has established Trade Transparency Units (TTUs) worldwide. These TTUs have enhanced international cooperative investigative efforts to combat activities designed to exploit vulnerabilities in the United States financial and trade systems.

Along the Southern border, criminal enterprises have exploited these vulnerabilities to facilitate the illicit drug trade. To combat this threat, ICE TTUs, in conjunction with Customs authorities in several South American countries, conduct proactive analysis of CBFT data and existing United States and foreign trade data to support counter-narcotics cases.

(b)(5)
(b)(7)

[REDACTED]

Stakeholders/Beneficiaries

[REDACTED]

United States Customs and Border Protection (CBP)

Reactive Analysis: Contraband Interdiction at United States Borders

Business Objective

Improve the ability of CBP Officers to interdict individuals attempting to transport contraband into or out of the United States.

Background and Description

In its effort to protect the borders of the United States, the United States Customs and Border Protection (CBP) agency works to safeguard our nation by preventing terrorists and terrorist weapons from entering the country while facilitating the flow of legitimate trade and travel.

To safeguard our nation's borders, CBP has established inspection sites at all United States ports of entry and conducts specialized secondary inspections focused on combating terrorism. CBP works to protect America and its citizens by carrying out additional missions, such as controlling the borders by apprehending individuals attempting to enter the United States illegally and stemming the flow of illegal drugs and other contraband by using more effective and innovative approaches to interdiction.

To stem the flow of illicit goods across United States borders, CBP conducts additional screening of passengers that may pose a threat to our nation's security. This screening process, combined with innovative analysis of flight and financial information, such as CBFT data, aims to interdict individuals seeking to transport illicit goods into or out of the United States.

Stakeholders/Beneficiaries

[REDACTED]

(S)(S)
(S)(S)

Office of the Attorney General of Arizona

Proactive Analysis: Money Transmitter Data Relating to Human Trafficking Investigations

Business Objective

Improve the ability of analysts from the Office of the Attorney General of Arizona, the Financial Crimes Task Force, and cooperating agencies to proactively identify entities engaging in human and drug trafficking.

Background and Description

In its effort to promote justice and protect the citizens of Arizona, the Office of the Attorney General of Arizona has teamed with the Department of Homeland Security, the Phoenix Police Department, and the Arizona Department of Public Safety to investigate and aggressively and fairly prosecute criminal and civil racketeering/asset forfeiture cases within the state.

The Financial Crimes Task Force is responsible for the investigation of crimes in specialized areas of the law covered under the Attorney General's statutory criminal jurisdiction, including narcotics investigations, money laundering, white-collar crimes, and human trafficking.

As the trafficking of illegal immigrants into Arizona by "coyote" criminal organizations has become more aggressive, the Financial Crimes Task Force and the Office of the Attorney General of Arizona have initiated new strategies to combat it. The Attorney General has established a Border Trafficking Team specializing in the prosecution of cases related to human smuggling and drug importation. This twenty-plus-member team is handling the recent prosecution of more than a dozen coyotes under new state laws applicable to human trafficking.

Another key step has been to strike at the smugglers' financial underpinnings. Working with banks, money transmitters, the courts, and federal, state, and local Law Enforcement, the Financial Crimes Task Force has targeted funds transmittals that are vital to these smuggling operations. In the past three years, the Financial Crimes Task Force has arrested over 160 smugglers, stopped more than 12,400 funds transmittals, and seized more than \$15 million in funds.

(b)(5)
(b)(7)



Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

Proactive Analysis: Interdiction of Transnational Firearms Trafficking

Business Objective

Improve the ability of ATF special agents and intelligence analysts to proactively identify new entities suspected of engaging in transnational firearms trafficking.

Background and Description

In its effort to prevent terrorism, reduce violent crime, and safeguard the United States, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) works to reduce crime involving firearms and explosives, acts of arson, and the illegal trafficking of alcohol and tobacco products.

To assist in the prevention of violent crimes involving firearms, ATF seeks to combat the illicit trafficking of firearms across the borders of the United States. The level of violence along the United States' southern border has risen sharply over the past several years, resulting in numerous gun-related homicides. The violence is often perpetrated by drug trafficking organizations vying for control of trade routes into the United States and engaging in turf battles for disputed distribution territories. To combat this threat, the ATF has strategically focused its investigative, intelligence, and training expertise to suppress firearms trafficking and deny firearms, the "tools of the trade," to transnational criminal organizations.

(6)(b)(5)
7



Stakeholders/Beneficiaries



Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

Proactive Analysis: Disruption of Interstate Tobacco Diversion Operations

Business Objective

Improve the ability of ATF agents and analysts to proactively identify new entities suspected of engaging in interstate tobacco diversion operations.

Background and Description

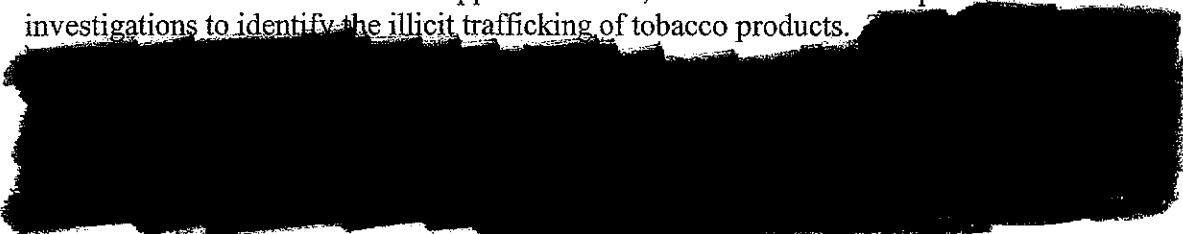
In its effort to prevent terrorism, reduce violent crime, and safeguard the United States, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) works to reduce crime involving firearms and explosives, acts of arson, and the illegal trafficking of alcohol and tobacco products.

The trafficking of contraband tobacco products is a global problem; contraband cigarettes are believed to be the number-one black market commodity in the world. There are diversion schemes occurring on every continent in the world, and the estimates of tax loss due to diversion in the United States alone total billions of dollars each year. Through the avoidance of state and federal excise taxes, criminal organizations are able to generate enormous profits from the diversion of tobacco products. Over the past several years, criminal organizations have resorted to alternative and increasingly complex means of generating illicit profits from tobacco diversion, including state-to-state diversion schemes, grey market schemes (exportation of the product and illegal re-importation), and the elaborate counterfeiting of cigarettes and cigarette tax stamps. Of significant concern is the use of tobacco diversion operations to fund terrorist organizations. Since 2002, the ATF has conducted two tobacco diversion investigations resulting in the conviction of individuals for providing material support to terrorist organizations.

In order to prevent the loss of billions of dollars in annual tax revenues and detect, disrupt, and dismantle terrorist financial support networks, the ATF conducts sophisticated investigations to identify the illicit trafficking of tobacco products.

Stakeholders/Beneficiaries

(5/9/9)
117



Department of the Treasury Office of Foreign Assets Control (OFAC)

Reactive Analysis: Narcotics Sanctions Investigations pursuant to E.O. 12978 and the Kingpin Act

Business Objective

Improve the ability of OFAC sanctions investigators to investigate foreign persons for potential derivative designations that are linked to significant foreign narcotics traffickers designated by OFAC under Executive Order 12978 or identified by the President of the United States under the Foreign Narcotics Kingpin Designation Act.

Background and Description

In its effort to support United States foreign policy and national security goals, the Office of Foreign Assets Control (OFAC) works to administer and enforce economic and trade sanctions against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC seeks to achieve this mission by imposing controls on transactions and freezing foreign assets under United States jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

To combat the significant threat posed by international narcotics traffickers to our nation, the President of the United States may impose sanctions pursuant to Executive Order 12978 (Colombian drug cartels) or the Foreign Narcotics Kingpin Designation Act ("Kingpin Act"). The purpose of E.O. 12978 and the Kingpin Act is to deny significant foreign narcotics traffickers, their related businesses, and their operatives access to the United States financial system and all trade and transactions involving United States companies and individuals. The Kingpin Act authorizes the President to take these actions when he determines that a foreign narcotics trafficker presents a threat to the national security, foreign policy, or economy of the United States.

The long-term effectiveness of E.O. 12978 and the Kingpin Act is enhanced by the Office of Foreign Assets Control's authority to make derivative designations of foreign individuals and entities that are owned or controlled by or are materially assisting, financial supporting, or providing goods or services in support of the narcotics trafficking activities of designated narcotics traffickers. This authority broadens the scope of application of the economic sanctions against designated kingpins to include their businesses and operatives. To date, OFAC has named 26 Colombian drug traffickers pursuant to E.O. 12978 and the President has named a total of 68 Kingpins. OFAC has designated over 1,800 entities and individuals in over 40 separate sanctions investigations since 1995.

(S)
(S)
(S)
(S)
(S)



Department of the Treasury Financial Crimes Enforcement Network

Reactive Analysis: Special measures against entities of "Primary Money Laundering Concern" - USA PATRIOT Act Section 311 Analysis

Business Objective

Improve the effectiveness of future USA PATRIOT Act Section 311 actions by analyzing the impact of past actions on designees.

Background and Description

In its effort to safeguard the financial system from the abuses of financial crime, the Financial Crimes Enforcement Network (FinCEN) works to detect and deter money laundering, terrorist financing, and other illicit activity. To combat these threats, FinCEN administers the Bank Secrecy Act (BSA). The BSA requires financial institutions to maintain appropriate records and to file reports that are used in criminal, tax, and regulatory investigations. BSA filings aid Law Enforcement agencies in the investigation of suspected criminal activity such as narcotics trafficking, income tax evasion, money laundering, and terrorist financing.

The USA PATRIOT Act made a number of amendments to the BSA intended to facilitate the prevention, detection, and prosecution of money laundering and terrorist financing. Section 311 of the USA PATRIOT Act grants the Secretary of the Treasury authority, after finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transactions, or type of account is of "primary money laundering concern," to require domestic financial institutions and domestic financial agencies to take certain "special measures" against the primary money laundering concern designed to increase information gathering or prohibit transactions with the designee.

Since 2002, the Department of the Treasury has strategically utilized the power of Section 311 to isolate rogue actors of primary money laundering concern that present significant risks to the integrity of both domestic and international financial systems.

Stakeholders/Beneficiaries

(b)(5)
(b)(7)
(D)

[REDACTED]

[REDACTED]

Internal Revenue Service Criminal Investigation (CI)

Reactive Analysis: Tax Evasion Investigations

Business Objective

Improve the efficiency of CI analysts investigating targets suspected of engaging in tax evasion.

Background and Description

In its effort to foster confidence in the tax system and compliance with the law, Internal Revenue Service Criminal Investigation (CI) serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes.

CI's investigative jurisdiction includes tax, money laundering, and Bank Secrecy Act statutes. While other federal agencies share investigative jurisdiction over money laundering and several Bank Secrecy Act violations, the IRS is the only federal agency that can investigate potential criminal violations of the Internal Revenue Code.

Maintaining public confidence in the fairness of the tax system is vital to effective tax administration. In the United States, compliance with the tax laws relies heavily on self-assessment of taxes through voluntary compliance. When individuals and corporations make deliberate decisions not to comply with the law, they face the possibility of a civil audit or criminal investigation which could result in prosecution and possible jail time. Publicity of these convictions provides a deterrent effect that enhances voluntary compliance.

The overall compliance rate achieved under the United States revenue system is quite high. For the 2001 tax year, the IRS estimates that over 86 percent of tax liabilities were collected. Nevertheless, an unacceptably large amount of the tax that should be paid every year is not, such that compliant taxpayers bear a disproportionate share of the revenue burden, giving rise to the "tax gap." The gross tax gap was estimated to be \$345 billion in 2001. This deliberate noncompliance by taxpayers undermines public confidence and threatens the ability of the IRS to effectively administer our nation's tax system.

To combat this threat, CI special agents and analysts conduct complex analysis, cross-referencing multiple disparate data sources, to identify sophisticated schemes to defraud the government of tax revenue.

Stakeholders/Beneficiaries

Internal Revenue Service Small Business/Self-Employed (SB/SE) Division

Proactive Analysis: Identification of Individuals Abusing Offshore Tax Havens

Business Objective

Improve the ability of IRS SB/SE analysts to identify individuals abusing offshore tax havens.

Background and Description

The mission of the IRS Small Business/Self-Employed (SB/SE) Division is to protect the public interest by applying the tax law with integrity and fairness. The SB/SE Division works to achieve this mission by educating and informing customers of their tax obligations, developing educational products and services, and helping customers understand and comply with applicable tax laws. The SB/SE Division has developed several initiatives, such as the Abusive Tax Scheme Program, to help ensure compliance with these laws.

The Abusive Tax Scheme Program was developed by the IRS to identify taxpayers who exploit the secrecy laws of offshore jurisdictions in an attempt to conceal assets and income subject to tax by the United States. These jurisdictions are commonly referred to as "tax havens" because they offer financial secrecy and impose little or no tax on income from sources outside their jurisdiction. Currently, more than 30 countries aggressively market themselves as tax havens. The exploitation of these offshore tax havens by United States citizens has resulted in the loss of billions of dollars in tax revenue. In an effort to address the loss of revenue through these tax havens, the IRS has established an Offshore Compliance Initiatives Group as part of the Abusive Tax Scheme Program.

The Offshore Compliance Initiatives Group conducts sophisticated analysis to proactively identify taxpayers engaged in the exploitation of offshore tax havens.

(b)(5)
[REDACTED]

Stakeholders/Beneficiaries

[REDACTED]

United States Secret Service (USSS)

Reactive Analysis: Identity Theft and Credit Card Fraud Investigations

Business Objective

Improve the efficiency of United States Secret Service agents investigating targets suspected of engaging in identity theft and credit card fraud.

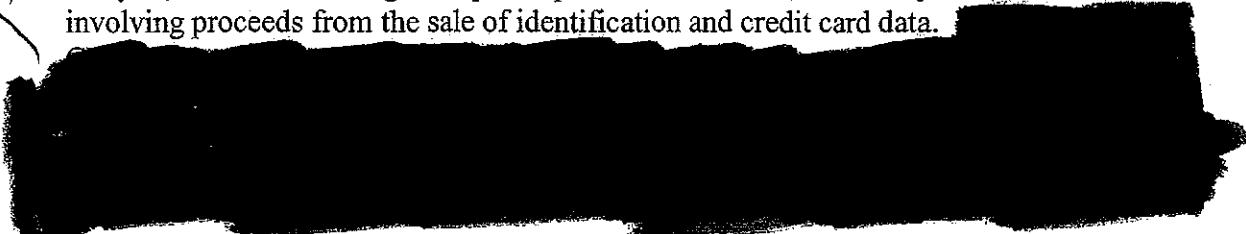
Background and Description

In an effort to carry out its dual missions of protection and criminal investigations, the United States Secret Service works to both safeguard our nation's leaders and investigate violations of laws related to counterfeiting, financial crimes, and computer-based attacks on the United States' banking and telecommunications infrastructure.

The primary investigative mission of the Secret Service is to safeguard the payment and financial systems of the United States. Historically, this has been accomplished through the enforcement of counterfeiting statutes to preserve the integrity of United States currency, coin, and financial obligations. Since 1984, the Secret Service's investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, fraud involving electronic funds transmittals, and identification fraud.

To combat identity theft and credit card fraud, Secret Service agents conduct sophisticated analysis, cross-referencing multiple disparate data sources, to identify financial transactions involving proceeds from the sale of identification and credit card data.

(b)(6)
(b)(7)(C)



Stakeholders/Beneficiaries



United States Securities and Exchange Commission (SEC)

Reactive Analysis: Foreign Corrupt Practices Act Investigations

Business Objective

Improve the efficiency of Securities and Exchange Commission attorneys investigating entities suspected of violating the Foreign Corrupt Practices Act (FCPA).

Background and Description

In its effort to maintain the integrity and vitality of America's securities markets and protect the interests of investors, the Securities and Exchange Commission (SEC) works to maintain fair, orderly, and efficient markets, facilitate capital formation, and administer federal laws governing United States securities.

The SEC works to promote fair and efficient capital markets through an effective and flexible regulatory environment. The SEC seeks to sustain an environment that will facilitate innovation, competition, and capital formation to ensure the growth of our nation's economy. The SEC works to detect problems in the securities markets, prevent and deter violations of federal securities laws, and alert investors to possible wrongdoing.

Crucial to the SEC's effectiveness is its enforcement authority. Each year the SEC brings hundreds of civil enforcement actions against individuals and companies for violations of the securities laws. The SEC's Division of Enforcement is responsible for conducting investigations into possible violations of the federal securities laws, and where warranted, prosecuting such violations. In fiscal year 2007, the SEC initiated 776 investigations, 262 civil actions, and 394 administrative proceedings covering a wide range of issues, including insider trading, accounting fraud, violations by broker-dealers, fraud related to mutual funds, and bribery by representatives of United States companies to foreign government officials.

During SEC investigations in the mid-1970s, hundreds of United States companies admitted to making questionable or illegal payments to foreign government officials, politicians, and political parties. Congress enacted the Foreign Corrupt Practices Act (FCPA) in 1977 to end the bribery of foreign officials and to restore public confidence in the integrity of the American business system. The anti-bribery provisions of the FCPA make it unlawful for a person, entity, and certain foreign issuers of securities, to make a payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person. The FCPA also applies to foreign firms and persons who take any act in furtherance of such a corrupt payment while in the United States. When it was enacted, the FCPA directly amended the Securities and Exchange Act of 1934 to require certain issuers of securities to keep detailed books, records, and accounts which accurately record corporate payments and transactions. This amendment charged the SEC with also enforcing, for purposes of the FCPA, certain internal accounting requirements of public companies. Under a complimentary statutory framework, the SEC and the Department of Justice are responsible for enforcing the provisions of the FCPA.

Department of the Treasury Financial Crimes Enforcement Network

**Proactive Analysis: Unregistered Money Services Businesses (MSBs)
Identification**

Business Objective

Improve the ability of FinCEN analysts to identify targets suspected of operating as unregistered MSBs.

Background and Description

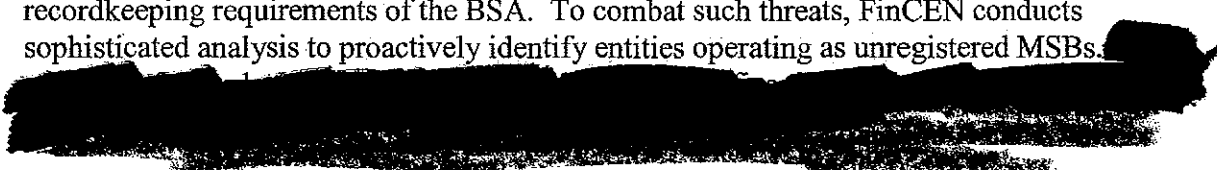
In its effort to safeguard the financial system from the abuses of financial crime, the Financial Crimes Enforcement Network (FinCEN) works to detect and deter terrorist financing, money laundering, and other illicit activity. Through cooperation and partnerships with the Law Enforcement, regulatory, and intelligence communities, FinCEN's network approach encourages cost-effective and efficient measures to combat illicit financial activity both domestically and abroad.

As formal financial systems become more transparent, criminal entities have resorted to alternative and increasingly complex means of laundering illicit proceeds. These entities often seek to exploit vulnerabilities in the United States financial system, such as money services businesses (MSBs) that fail to comply with registration and other requirements of the Bank Secrecy Act (BSA) and its implementing regulations.

Certain MSBs must register with the Financial Crimes Enforcement Network under the BSA. In addition, MSBs are subject to anti-money laundering program, reporting, and recordkeeping requirements of the BSA. Registration of MSBs helps ensure that these businesses operate within the formal financial system, and are subject to examination by the Internal Revenue Service and state government agencies.

Identification of unregistered MSBs is a critical component of FinCEN's effort to safeguard the financial system from the abuses of financial crime. MSBs that fail to comply with registration and other requirements of the BSA are vulnerable to exploitation by entities seeking to engage in terrorist financing, money laundering, and other illicit activity. Activities of MSBs operating in violation of BSA registration requirements may not be detected and examined for compliance with anti-money laundering program, reporting, and recordkeeping requirements of the BSA. To combat such threats, FinCEN conducts sophisticated analysis to proactively identify entities operating as unregistered MSBs.

(b)(5)
(b)(7)



Department of the Treasury Financial Crimes Enforcement Network

Proactive Analysis: Emerging High-Risk Financial Trend Identification

Business Objective

Improve the ability of FinCEN analysts to proactively identify emerging high-risk financial trends.

Background and Description

In its effort to safeguard the financial system from the abuses of financial crime, the Financial Crimes Enforcement Network (FinCEN) works to detect and deter terrorist financing, money laundering, and other illicit activity. To combat these threats, FinCEN administers the Bank Secrecy Act (BSA). The BSA requires financial institutions to maintain appropriate records and to file reports that are used in criminal, tax, and regulatory investigations. BSA filings aid Law Enforcement agencies in the investigation of suspected criminal activity such as terrorist financing, money laundering, narcotics trafficking, and income tax evasion.

The Secretary of the Treasury has delegated overall authority for the enforcement of, and compliance with, the BSA to the Director of FinCEN. The Secretary has delegated BSA examination authority to federal regulators. To assist regulatory agencies with the examination of financial institutions, FinCEN conducts sophisticated analysis of the BSA to proactively identify emerging high-risk products, services, locations, and types of customers that may be exploited by entities engaged in illicit financial activities.

(S)(5)
(6)(7)

[REDACTED]

Stakeholders/Beneficiaries

[REDACTED]

(b)(6) [REDACTED]

450 West 33rd Street
New York, NY 10001
tele 212.612.9205

(b)(6) [REDACTED]@theclearinghouse.org



April 10, 2009

The Honorable Max Baucus
Chairman
Committee on Finance
United States Senate
219 Dirksen Senate Office Building
Washington, DC 20510-6200

Re: Proposed Information Reporting Regarding
Certain Transfers to Offshore Accounts

Dear Senator Baucus:

The Senate Finance Committee is currently considering a draft bill (the "Bill") intended to improve tax reporting compliance with respect to offshore accounts. Section 2 of the Bill would add a new section 6045C to the Internal Revenue Code, which would require any financial institution directly or indirectly transferring more than \$10,000 (individually or as an aggregate of "related" transactions) at the direction, on behalf, or for the benefit of a U.S. customer (other than any publicly traded company) to a financial account outside of the U.S. to file a return identifying the U.S. customer, the bank holding the offshore account, the offshore account's "type" and number, and the amount transferred. The purpose of the provision is to provide the Internal Revenue Service ("IRS") with information to help it identify U.S. persons who may be using offshore accounts to evade taxes. While we are sympathetic with this purpose, we are writing to express our concerns about this provision.

[REDACTED]

The Clearing House Association L.L.C. ("The Clearing House") is an association of leading commercial banks that frequently represents the views of its members¹ on issues of importance to the banking industry and to the public interest as a whole. Through its affiliate, The Clearing House Payments Company L.L.C., The Clearing House operates funds-transfer, automated clearing house ("ACH"), and check-clearing systems; as a result, The Clearing House has specific expertise in the kinds of systems that would be directly affected by the information gathering that would be needed to file the reports contemplated by section 2 of the Bill. The Clearing House and its member banks support the Bill's purposes, but believe that section 2, as drafted, would create a reporting system that would, at the very least, be extraordinarily difficult to comply with and may, in fact, be impossible to implement.

Below, we first explain the most difficult issues we see with implementing and complying with the proposed reporting requirements; we then address some of the undefined terms used in the proposal and explain the issues raised thereby.

The Bill's reporting requirements are in some ways reminiscent of a proposed reporting scheme that Congress directed the Treasury Department to study several years ago,² which would have required banks to send to the Treasury Department copies of all cross-border funds-transfer payment orders they sent or received. In this respect, it was much simpler and less burdensome than the requirements contemplated by section 2 of the Bill. Even so, Treasury found that while the proposed system might be feasible at some time in the future, putting the proposed system in place would require the expenditure of considerable resources in time, money, and intellectual effort by the government and the banking industry.³ The proposal has not been put into effect.

The reporting scheme contemplated in section 2 of the Bill would be far more complex and burdensome than the earlier proposal: that proposal would merely have required banks to identify all funds transfers they sent to, or received from, a financial institution located outside the U.S. and send copies of the transfer payment orders to Treasury, while the current

¹ The members of The Clearing House are ABN AMRO Bank N.V.; Bank of America, N.A.; The Bank of New York Mellon; Citibank, N.A.; Deutsche Bank Trust Company Americas; HSBC Bank USA, N.A.; JPMorgan Chase Bank, N.A.; UBS AG; U.S. Bank N.A.; and Wells Fargo Bank, N.A.

² See Intelligence Reform and Terrorism Prevention Act of 2004 § 6302, Pub. L. No. 108-458, 118 Stat. 3638, 3748-50 (Dec. 17, 2004), codified at 31 U.S.C. § 5318(n).

³ See Financial Crimes Enforcement Network, U.S. Department of the Treasury, *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System Under the Bank Secrecy Act* (Oct. 2006), available at http://www.fincen.gov/news_room/rp/files/cross_border.html.

proposal would entail the much more complex task of identifying a defined subset of a much larger universe of cross-border transactions, storing and collating information from those transactions, and reporting the results, along with additional information, to the IRS and one or more other parties. Even if we assume that the ambiguities in the Bill can be satisfactorily resolved and the U.S. customers and foreign financial accounts can be properly identified, the complexities of implementing and complying with the proposed system would dwarf anything previously contemplated. Enactment of section 2 would require financial institutions to design, build, and test complex systems to gather information in a common database from a variety of sources in different divisions of their organizations where the data are currently collected and processed; store considerable information that is not currently maintained; and combine the data to compile the required tax reports. It is not possible to estimate with any precision the time and resources that would be required for these financial institutions to complete all of these tasks. It is clear, however, that compliance would not be possible for several years (at a minimum) and that a bank of any reasonable size would have to devote substantial resources to the project.

Given this reality, we strongly urge the Committee to work with the banking industry to develop an alternative method of policing taxpayers' compliance with the requirement that they report their foreign accounts to the IRS. One avenue that could prove promising would be to improve protocols for exchanging information with foreign governments. We would be happy to work with the Committee to explore this and other alternatives to the reporting requirement of section 2 of the Bill, and suggest a meeting between representatives of The Clearing House and its member banks and Committee staff at an early date to begin this process.

Issues—Undefined Terms.

Much (but not all) of the difficulty associated with section 2 of the Bill is the result of its use of undefined terms—words that could, depending on how they are interpreted, make it impossible for the banks to build any system that would allow them to comply with the reporting requirements. This section of our letter will review these issues.

(1) *Transferring* is used as a verb, so it is not clear what kinds of transactions would be covered. We assume that it would cover funds transfers, but it could also be intended

to cover checks, ACH, and other kinds of transactions capable of transferring funds across borders, as well as transfers of securities and other financial instruments.

If the intention is to include not just funds transfers (see item 3, below), then the reporting institutions would be faced with collecting data from different platforms (funds transfer, securities, check, ACH, debit card, credit card, etc.) that are not currently connected and marrying them to the tax reporting platform, an extraordinarily difficult task that would likely take years to complete even in the best economic circumstances.

(2) *Directly or Indirectly.* Cross-border funds transfers usually involve a series of banks linked by funds-transfer systems or interbank correspondent accounts. Large U.S. banks often act as intermediary banks in cross-border funds transfers. Intermediary banks do not have any direct relationship with the originator or beneficiary of a funds transfer and therefore have little or no knowledge of who these parties are or why they are transferring funds, and, except for certain specific circumstances that would not be useful in gathering the information that the Bill contemplates, there is no commercial or regulatory reason for them to have such information. Intermediary banks would likely not be able to obtain such information without making specific requests to the senders of each of the millions of payment orders they handle each year, but many non-U.S. originator's banks may be unable to provide the requested information because of local laws regarding the privacy of customer information or similar limits on information sharing.

Thus, if the phrase "directly or indirectly" is intended to capture intermediary banks, it will risk overloading the IRS with duplicate reports regarding the same transaction.

(3) *Financial account.* The term is not defined in the Bill. It is used in the Report of Foreign Bank and Financial Accounts ("FBAR," IRS Form D-90.23), where it is defined to include "any bank, securities, securities derivative or other financial instrument accounts . . . [including] any savings, demand, checking, deposit, time deposit, or any other account (including debit card and prepaid credit card accounts) maintained with a financial institution . . ." As noted in item 1, this would require reporting institutions to collect information across many platforms that they currently have no way to collect. We submit that the adverse effects of such an exercise would outweigh the incremental enforcement benefits that would flow from it.

In addition, the nature of a funds transfer is that it almost always involves a transfer to an account of the beneficiary at a bank. A large U.S. bank is likely to handle tens of millions of funds transfers each year,⁴ a large proportion of which involve a cross-border component and require no human intervention for processing. Information on individual transactions is not currently retained in a form that can be aggregated for purposes for tax reporting, so reporting institutions would have to expend significant resources to create the systems that would allow them to do so. This would be especially true for intermediary banks, who, as noted, would have only limited information on the originators, beneficiaries, and the offshore nature of the payment orders they receive.

(4) *Related transactions.* The Bill does not define this term, and it is not clear what is intended. It could be interpreted to mean all transactions with the same originator, the same beneficiary, where both the originator and beneficiary are the same person, or to refer to myriad other combinations. Analysis of this issue would be especially difficult when the originator of a funds transfer is a broker or money manager acting on behalf of another person.

The Committee may have had in mind the Bank Secrecy Act provision prohibiting the "structuring" of cash deposits to avoid the threshold for filing Currency Transaction Reports. Over the years, banks have established procedures to detect structuring. But cash deposits and funds transfers are very different operations, and the amount of information normally available to a bank (especially an intermediary bank) in a funds transfer would not usually be sufficient for it to determine if offshore account "structuring" is taking place.

Without a specific, narrow definition of what it means for transactions to be related, we do not believe that it would be possible for banks to determine with any confidence that two or more transactions are, in fact, related.

(5) *At the direction of, on behalf of, or for the benefit of.* The intent here seems to be to cast the widest possible net, but without specific guidance, it is difficult to understand how the reporting institutions would be able to determine which transactions would have to be aggregated. "At the direction of" suggests the focus of the reporting institution should

⁴ The Bank for International Settlements reports that in 2007 the major U.S. funds-transfer systems, CHIPS (operated by The Clearing House) and Fedwire (operated by the Federal Reserve Banks), together handled 221 million transfers and that the U.S. banks that are members of SWIFT (an international funds-transfer system) processed 594 million SWIFT payment orders. See http://www.bis.org/publ/cpss/ctrytbls_07.xls. The cross-border funds-transfer business is highly concentrated, with a few large banks processing a large majority of these transfers.

be on the transfer's originator, but the originator could be a broker, investment manager, or even the bank's own trust department, acting on behalf of its customer. From the point of view of an intermediary bank, "at the direction of" suggests the reporting institution's focus should be its correspondent banking customer, i.e., the originator's bank or another intermediary bank sending the transfer to it. Does the Committee really intend this result? The practical effect (and unintended consequence) is that intermediary banks will need, literally, thousands of employees to make telephone calls to their sending bank customers seeking this information. Even with this effort, they will likely not be able to get the required information for a significant percentage of these transactions, perhaps requiring the banks to reject the payment orders for which they were unable to get the information necessary to make a determination if the transactions were reportable under the Bill.

"On behalf of" suggests the reporting institution's focus should be the person who is the transfer's "true party in interest." But banks may not be in a position to know who that is, especially when the originator is a broker, investment manager, or similar party. Regulations issued by the Treasury Department under the Bank Secrecy Act provide that when a nonbank financial institution initiates a transmittal of funds, it must include information on the customer on behalf of whom it is acting in the transmittal instruction,⁵ but there is no requirement that this information be formatted in a way that it will allow any bank that subsequently handles the transfer to identify that party automatically. Requiring intermediary banks to do this would require reforming the standard formats that are used globally for funds transfers and making changes to market practices to ensure that all parties adhere to standard ways of using those formats. This is a major undertaking that can require years of planning and execution and millions of dollars in data-processing costs.

In the funds-transfer context, "for the benefit of" suggests the reporting institution's focus should be the transfer's named beneficiary. But the phrase is also used to refer to the beneficial owner of the originator's account, for example, the beneficiaries of a trust. As the beneficiary of a funds transfer will be identified only by the name and account number associated with the account to be credited by the beneficiary's bank, the originator's bank and any intermediary banks would not be in any position to know beneficial owner information.

⁵ See 31 C.F.R. § 103.33(g)(1).

April 10, 2009

(6) *Customer Who Is a United States Person.* First, it is not clear whose customer the Bill is referring to. If the reporting bank is intended, the bank (if it is the originator's bank) will likely have information on the sending customer's nationality or jurisdiction of incorporation in its Know Your Customer ("KYC") database, but not in a way that is available to the systems that process its funds transfers or other financial transactions, so additional systems will have to be designed that will allow the funds-transfer systems to access this KYC information so that reports can be generated. In the case of some bank products, such as credit cards and retail banking, information on the customer's nationality may not be available at all. If the intent is to refer to U.S. persons who are customers of offshore financial institutions, this information is unlikely to be available to U.S.-based reporting institutions.

* * * * *

As noted at the outset, these comments are intended to help the Committee appreciate just some of the difficult issues financial institutions would confront in trying to comply with the reporting requirements set out in section 2 of the Bill. We fully support the Bill's goals of preventing U.S. persons from using offshore accounts to avoid taxes, and we would be happy to work with the Committee to develop an alternative means of achieving this goal.

We hope the foregoing has been helpful to you, and that we can meet with the Committee's staff to answer any questions you may have regarding the issues discussed in this letter and to discuss alternatives to the reporting scheme set out in section 2 of the Bill. If you have any questions or would like to discuss this further, please contact [REDACTED]

[REDACTED] at [REDACTED]

→ (b)(6)

Very truly yours,

[REDACTED]

(b)(6)

cc: Ms. Mary Baker, Senate Finance Committee

132
[REDACTED]