Testimony of Gerald Kitchen, Chief Executive, SecureTrading Group Limited
June 6, 2007

Submitted for the Record Concerning
Legislative Hearing on H.R.2046, the "Internet Gambling Regulation and Enforcement Act of 2007"

Held Before the Financial Services Committee
United States House of Representatives
On Friday, June 8, 2007, at 10:00 a.m.

Mr. Chairman and Members of the Financial Services Committee, I am Gerald Kitchen, Chief Executive of SecureTrading Group Ltd, a UK Limited Company which operates a Financial Payments business that specializes in the secure processing and settlement of Internet payments.

I appreciate the opportunity to submit written testimony to you concerning our experiences with the secure processing of Internet payments with respect to high-risk transactions, specifically Internet gambling transactions.

I. INTRODUCTION

First, I would like to provide some information about SecureTrading Group Ltd and Baker Tilly. SecureTrading Group Ltd is a UK Limited Company which has operated a Financial Payments business that specializes in the secure processing and settlement of Internet financial transactions since 1997. SecureTrading Group Ltd is not an online gambling company but rather a payment service provider that, with the support of back office services provided by Baker Tilly ("BT"), processes a wide variety of financial transactions (including legal online gambling transactions) for some of the largest financial institutions in the world.

BT is an independent member of Baker Tilly International, a global network which has 126 member firms in 93 countries with an aggregate worldwide annual fee income of over $2.2 billion, making Baker Tilly International the 8th largest accounting network in the world, by fees.

The card payment processing industry has evolved over many years to put in place a globally cooperative and integrated infrastructure that seeks to optimally and seamlessly mitigate risks and maximise the service experience for cardholders. The participants in this infrastructure include card schemes (VISA and MasterCard), card issuing banks, merchant acquirers, merchants and payment service providers like SecureTrading Group Ltd.

Further to this, the SGBT system provides an oversight and integration role in ensuring compliance and adherence to the various requirements related to risk mitigation and regulation across the payments processing industry.

Working together SecureTrading Group Ltd and BT have developed a transaction system for e-commerce sectors which is specifically designed to provide security, protect against fraud, prevent money laundering, and limit other abuses in areas of e-commerce that are perceived to pose special risks, such as in travel reservations and Internet gambling transactions.[1] In this document I have referred to the system as "the SGBT system".

I am submitting this testimony today to address concerns raised about Internet gambling and to provide information about how many of the same concerns are already being addressed in other nations through the application of specific processes and technology.

II. H.R.2046 AND ITS GOALS

The legislation introduced by Congressman Frank (D-MA) seeks to modernize existing U.S. law by implementing a licensing and enforcement regime for Internet gambling. The licensing and enforcement regime for Internet gambling in the United States will provide appropriate protection against underage gambling, compulsive gambling, money laundering, and fraud for those citizens who choose to gamble online. The bill specifically permits individual states, tribes and sporting leagues to opt out of such an arrangement thus protecting rights that currently exist.

Several concerns have been raised about the activity that might be permitted under the bill. Specifically, concerns have been raised that allowing any legal Internet gambling would invite a number of social harms – such as underage gambling, compulsive gambling, involvement of organized crime, money laundering and fraud.

I would like to address each of these points, but first let me state unequivocally that I do not, nor does SecureTrading Group Ltd, take a position regarding the legality or illegality of gambling or Internet gambling. SecureTrading Group Ltd does, however commend the efforts of Congressman Frank and supports the introduction of H.R.2046 that establishes high standards of consumer protection and security of financial transactions. From the text of the Internet Gambling Regulation and Enforcement Act of 2007 *certain* financial transactions are likely to be permitted. To the extent that this is the case, I respectfully offer to the Committee that there is, today, the technological and process capability in place to permit those *legal* transactions to occur – with protections in place to prohibit underage or compulsive gambling, organized crime, money laundering and fraud. I have spent a career developing such protections, not just for Internet gambling but for *all* financial transactions. I hope this testimony will provide useful information regarding the technology and process landscape and respond to the concerns raised.

[1] Other areas of higher risks of payment fraud, and related abuses include airline travel bookings, adult entertainment, and consumer purchases of digital goods. The SecureTrading Group Ltd's systems and solutions handle a variety of forms of consumer transactions, but as a matter of choice and policy do not include the adult entertainment sector.

III. THE SGBT SERVICE FOR HIGH RISK E-COMMERCE SECTORS

Many of the risks that have been articulated relating to online gambling potentially apply to Internet financial transactions more broadly. For example, these transactions involve risks not present in face-to-face business because the card holder and the merchant are not normally together when the transaction occurs. Without safeguards in place, the lack of face-to-face communication has the potential to increase the risk of fraud in any Internet payment by comparison to its counterpart in the physical world. Some e-commerce sectors, such as gambling and entertainment, raise additional public interest concerns that further enhance the need for making these payments both secure and capable of preventing fraud and other abuses. The degree of risk is greatly reduced by reliance upon the stringent controls and oversight of the existing financial institutions.

The SGBT system provides payment and related financial services to Internet merchants to protect both the merchants and the consumers who purchase goods and services from these merchants. In the payment card transaction chain, it operates between the merchant and the acquiring bank and performs the functions of an online payment service provider. The SGBT system carries out the full Internet payment process for the merchant, using SecureTrading's software. However, unlike traditional online payment processors, the SGBT system adds a significant number of security features to ensure that the consumers, merchants and banks are protected from fraud.

The SGBT system works as follows:

- First, SecureTrading Group Ltd sets up a "rolling reserve" escrow account for each merchant in which a percentage of the merchant's revenue is kept for six months. This is done to ensure that chargebacks or refund requests from disputed transactions can be settled against the escrow account. Valid requests for chargebacks and refund requests relating to disputed transactions are accepted as a matter of course. Such claims automatically result in a full repayment to the principal card holder. Depending on the chargeback record of a merchant the "rolling reserve" can be decreased over time. It is therefore in the interest of the merchant to take all possible steps to avoid unauthorised use of payment cards. This aspect of the SGBT system has been highly successful in dramatically reducing the level of chargebacks typically experienced by internet merchants. Our industry comparisons show that merchants utilising the SGBT processing systems are experiencing lower levels of chargebacks than industry norms.[2]

[2] Internet merchants can be the victim of attacks by professional payment card fraud rings, which may cause occasional peaks in the number of chargebacks. For the purposes of this paper this was not regarded as part of "normal transaction traffic."

- The SGBT system monitors the occurrence of suspicious chargebacks and refunds on a payment card (in particular those linked to possible unauthorised use). Should suspicious activity such as excessive levels of chargebacks or refunds occur, SecureTrading Group Ltd immediately stops accepting further transactions from that payment card.[3]
- The SGBT system does not "aggregate" e-commerce transactions, putting them together into a single pool of funds that is then moved through the payments system. Transactions are kept in separate accounts for each merchant and, as needed, for each URL[4]. This ensures funds are retained at a merchant level to ensure all cardholder claims for chargebacks and refund requests are honoured in a timely manner.
- The SGBT system monitors and compares IP address,[5] country of card holder and country of issuing bank as further protection against fraud and ensuring regulatory compliance at a location level.
- The SGBT system constantly monitors the frequency and value of transactions per payment card. The SGBT system ensures that a sudden increase in frequency of use or value of transactions on a payment card is immediately investigated.
- The SGBT system uses secure software which allows it to trace back every single transaction down to the second. In other words, the SGBT system creates an audit trail for every transaction.
- The SGBT system makes continuous use of the services of BT, which extracts all transactions on a daily basis and manages the "rolling reserve."
- All funds are received into bank accounts controlled exclusively by BT. All trading and reserve accounts are reconciled on a daily basis by BT.
- BT calculates all relevant deductions, being the transaction based costs. The same methodology would be used to calculate any taxation to be deducted. These funds are then identified separately from Merchant funds, before paying over to the relevant authorities or recipient 3rd parties.
- BT notifies Merchants daily of the transactions processed by the SGBT system.
- BT retains a full audit trail of all transactions it processes, detailing all information received by BT and the eventual trail through to payment to the relevant parties.
- All of the SGBT system data (including all transaction records) are stored safely on state-of-the-art high security servers both by SecureTrading Group Ltd and by BT.[6]

---

[3] Chargebacks or refunds can be objectively justifiable in e-commerce. For instance, it is possible that a consumer inadvertently "clicks twice." In such cases, the money spent inadvertently will be returned but there is no objective reason to refuse to transact with this consumer in the future.

[4] A "URL" is a web link ("URL" stands for Uniform Resource Locator).

[5] "IP address" stands for Internet Protocol address. Every computer connected to the Internet is assigned a unique number known as an Internet Protocol (IP) address. Since these numbers are usually assigned in country-based blocks, an IP address can often be used to identify the geographic location from which a computer is connecting to the Internet.

[6] All card data is encrypted and managed in accordance with the requirements of the Payment Card Industry Data Security Standard (PCI DSS)

- To protect against the risk of money laundering, SecureTrading Group Ltd high risk e-commerce clients are contractually obliged to:
    - Fully disclose the identity of company directors and beneficial shareholders and report any changes.
    - Take all reasonable steps to verify the identity of a consumer (e.g. by collecting a copy of a drivers licence or passport or by using online identification services such as Verid or URU).

  SGBT ensures adherence to this by undertaking regular audits of these processes. When a merchant is found in breach of its contractual obligations in this regard, the merchant's "rolling reserve" escrow account is increased in case of future claims. Should this practice continue, processing services will be terminated.
- In the specific case of Internet gambling merchants, SecureTrading Group Ltd limits the payment of winnings to the card holder (by a bank draft check in the card holder's name or through a transfer to his bank account), and screens names of payees against applicable sanctions lists. As a result, no money is at risk of being paid to individuals or organisations listed on the lists of persons, groups and entities subject to financial sanctions published by the European Union (EU)[7] and the "Specially Designated Nationals list" published by U.S. Department of the Treasury.[8] SGBT ensures adherence by undertaking regular audits of these processes.
- In the specific case of Internet gambling merchants, SecureTrading Group Ltd only deals with merchants who are licensed under applicable local laws and who are in good financial and legal standing, based on banking and legal references.
- Likewise, if a merchant fails to cure any breach of the contractual anti-money laundering obligations or is determined to no longer be in good legal standing, or financially sound, SecureTrading Group Ltd will terminate all services to that merchant.

The SGBT system has been extensively reviewed by several major United Kingdom based clearing banks, including Barclays, Lloyds and Royal Bank of Scotland, as well as European banks and legal practices including Herbert Smith LLP and Alston & Bird LLP.

Thus, the SGBT system has already in place systems that effectively counter fraud and money laundering pertaining to Internet gambling, as well as other forms of potentially higher-risk online consumer transactions. The same sets of processes can be used to combat underage gambling and compulsive gambling, by defining criteria that require age verification or which impose limits on the basis of required personal identifications, to enforce such limitations as may be imposed by any jurisdiction's particular regulatory regime. I address this process further in my testimony below.

---

7 Available at http://europa.eu.int/comm/external_relations/cfsp/sanctions/list/consol-list.htm

8 Available at http://www.ustreas.gov/offices/enforcement/ofac/sdn/

IV. SPECIFIC CONCERNS ROUTINELY RAISED BY INTERNET GAMBLING

As previously stated, there are generally five main areas of public interest concern with respect to Internet gambling transactions – underage gambling, compulsive gambling, involvement of organized crime, money laundering and fraud. These areas of public concern are not unique to the United States – they are concerns faced by a multitude of jurisdictions. Many jurisdictions, including the United Kingdom, have legalized Internet gambling. They have not done so by turning a blind eye to these concerns. Rather they have instituted a regulatory regime whose purpose is to ensure that technology and processes are employed to protect consumers and financial institutions. As other nations have found, these risks can be countered and contained, if those institutions operating Internet gambling payment gateways choose to adopt, or are required to adopt, technological systems and processes specifically designed to address each of these problems, systems and processes such as those provided by the SGBT system. The strength of this system is complemented by the strength of the controls and vigilant oversight of the financial institutions.

- **The role of the operator.**

An important consideration is that all consumers wishing to participate in this activity need to establish a player account with a licensed operator. During the registration process the player's identity must be verified. Stringent "Know Your Customer" (KYC) requirements need to be satisfied to confirm the identity, age and residence of the player. When a registered player logs on to participate in the activity their identity is again verified using a unique identifier generated during the registration process. Additionally, the location of the participant is also checked. Only one account is permitted per player and no payments are made without full verification of the identity of the player.

There is also an onus on the operator to comply with best practices as they relate to responsible gambling measures. These practices include setting player bet limits (individual bet and capped cumulative loss), permitting a player to exclude them self from participating in play, whether at that site or on a broader industry level, and providing players with access to information about their activity.

- **Technology and processes exist to restrict customers by location**

The SBGT system allows for the exclusion of customers based on their location in the event that a jurisdiction chooses to opt out.

The individual's location can be identified using IP Geolocation technology. This involves matching the customer's IP address to a specific state and in some cases a specific city or town. This technology is provided by a number of 3rd parties including Quova. The accuracy of the Quova system has been independently verified by PricewaterhouseCoopers as 99.9% accurate on a country level and 95% accurate on a state level.

This accuracy can be further enhanced by considering IP location together with both the registration information provided by the customer, the address to which a payment card is registered and the location of the bank that has issued the payment card.

- **Technology and processes exist to address the risk of underage gambling.**

The SGBT system incorporates a number of barriers to prevent abuse by underage persons. The first barrier is at the merchant's website, which must have appropriate age verification mechanisms in place to qualify for services from SecureTrading Group Ltd. The next barrier is provided by the card issuance rules in place for financial institutions. Finally, underage persons are denied winnings because the SGBT system only permits payment of winnings to the registered account and card holder.

A key part of addressing the underage gambling risk is the KYC checks undertaken at the point of consumer registration with the merchant.

KYC requires that the organisation know whom it is in fact dealing with. In order to satisfy this requirement, the customer is asked for a range of information, including Name, Address, Date of Birth, Telephone Number and information not easily available such as Social Security or Passport Number. This information is then compared to multiple databases to confirm the accuracy and validity. If the customer fails this validation they are unable to open an account. These services are today provided across many industries. Service providers include Experian, Aristotle and GB Group.

Additional KYC checks performed include checking that the registered address of the telephone number matches the details supplied, and that the customer is in fact able to answer the telephone and confirm these details.

Credit card companies typically do not issue credit cards to minors. Nevertheless, minors may validly have access to debit or sponsored cards. In these cases, the Issuer will be aware of the cardholder's age and is able to decline the transactions flagged as internet gambling at the time of authorization.

An additional control ensuring use by the legitimate cardholder is provided by the financial institutions and the card schemes through a requirement, at an increasing number of sites, to enter a password before completing an online transaction (Verified by Visa and MasterCard Secure Code systems).

A final impediment to underage usage goes to the heart of the system designed by SGBT: The underage consumer cannot receive any winnings, as they are not the authorized owner of the card.

SecureTrading Group Ltd acknowledges that enforcement and compliance with regulations cannot be perfect and requires continuous improvement and enhancement. While SecureTrading Group Ltd is confident that the rules in place are sufficiently rigorous to prevent underage consumers accessing the system, should an investigation prove that an underage consumer has circumvented the rigorous controls in place, the principal card holder will be refunded.

- **Technology and processes exist to address the risk of compulsive gambling.**

The issue of compulsive gambling remains a significant challenge. The solutions are complex and require all participants in this industry to work together in a cooperative way with a combination of education, technology and oversight (parental and / or government). The approach required to effectively combat this requires transparency and involvement from various stakeholders.

The SGBT system offers a number of opportunities to address compulsive gambling on the Internet that are as good as, if not better than, those available for bricks and mortar gambling.

First, payment card holders can be offered the possibility to restrict their ability to gamble on the Internet by way of applying to be excluded via a self-exclusion program. Land-based casinos in the United States already maintain self-exclusion programs but the effect of such a program is normally limited to one casino. When self-exclusion from Internet gambling is put into effect via the payments system, it becomes impossible for the person concerned to participate in *any* gambling on the Internet that uses traditional card payments through the payment processor. Furthermore, individuals may fix limits on the amounts they can spend on Internet gambling. Increasing such limits is typically subject to cooling off periods after which the individual would need to reconfirm that he or she effectively wants to increase the spending limit. The ideal solution is for a global self-exclusion database to be established and access made available to all financial transaction processors and licensed operators, providing for a broader blocking capability.

Second, the SGBT system can prohibit individuals from registering more than one payment card to pay for Internet gambling transactions. This would prevent individuals from running up excessive debts by using multiple cards. Similarly players are restricted to only the one account with a licensed operator.

Third, it is relatively simple for the SGBT system to detect an unusual increase in an individual's spending on Internet gambling. This makes it possible to monitor compulsive gambling much more closely than in the case of traditional forms of gambling where the casinos, lotteries and racetracks normally do not know the identity, or the spending pattern, of most of their customers.

Fourth, as mentioned above the customer's identity is verified using 3rd party KYC systems. Once the information has been validated, it can be checked against various databases of compulsive gambling. In the event that a customer is found to be present in these databases, the registration can be rejected or the customer investigated.

- **Technology and processes exist to address the risk of abuse of Internet gambling by organized crime.**

It is envisaged that the licensing process under FinCEN (Financial Crimes Enforcement Network) would require that licence applicants satisfy the same stringent due diligence and suitability requirements as with land-based gambling licensing processes. These relate particularly to criminal record checks. Additionally, the SGBT system maintains an audit trail of all transactions conducted using the SGBT system. Prior to paying any winnings, the SGBT system can be used to screen the payee against the EU's lists of persons, groups and entities subject to financial sanctions and the United States' list of "Specially Designated Nationals." Additionally, the SGBT processes involve screening the beneficial shareholders of the Internet gambling companies that use its services on a best endeavours basis. These checks could be extended to various information resources including OFAC and the Sanction lists.

Using technology and processes such as those provided by the SGBT system, makes Internet gambling a much less attractive vehicle for organized crime than the anonymous, cash-intensive world of traditional gambling with casinos, lotteries and racetracks or other high turnover cash businesses or businesses lacking transparency in their financial systems. Internet gambling transactions processed by the SGBT system can be tracked by authorized regulators and law enforcement in connection with their criminal investigations. As a part of this process, SecureTrading Group Ltd has instigated links with the United Kingdom Serious Organised Crime Agency (SOCA).

- **Technology and processes exist to address the risk of abuse for money laundering.**

It is envisaged that FinCEN would not permit licensed operators to accept cash deposits into player accounts. Similarly, SecureTrading Group Ltd does not accept cash payments from consumers or Internet gambling businesses. All transactions are recorded with all parties having satisfied stringent KYC checks. All parties are clearly identified. As a result, the SGBT system virtually eliminates the attractiveness of using Internet gambling transactions for money laundering. As the U.S. General Accounting Office has reported:

> "Banking and gaming[9] regulatory officials did not view Internet gambling as being particularly susceptible to money laundering, especially when credit cards, which create a transaction record and are subject to relatively low transaction limits, were used for payment. Likewise, credit card and gaming industry officials did not believe Internet gambling posed any particular risks in terms of money laundering. (…)

[9] The term "gaming" used by the GAO in its report is retained here. The term "gaming" is generally used in the UK to refer to what in the U.S. is ordinarily referred to as "gambling." In deference to this U.S. forum, my testimony uses the term "gambling" throughout.

> "In general, gaming industry officials did not believe that Internet gambling was any more or less susceptible to money laundering than other electronic commerce businesses and noted that the financial industry – which is responsible for the payments system – is better suited to monitoring for related suspicious activity in the area than the gaming industry itself."[10]

The United Kingdom, which spent considerable time and effort studying the feasibility of regulating Internet gambling with a regulatory framework subsequently included in their Gambling Act 2005, takes the view that "there appears to be a paucity of proof" that money laundering through Internet gambling sites is "a significant problem" and that "[i]t is safe to say that gambling transactions completed online can be more secure than cash business conducted in traditional gambling outlets."[11] Compliance with anti-money laundering guidelines and license conditions, use of controls within the financial industry and the adaptation of best practices utilizing technology will ensure the threat of money laundering via Internet gambling is greatly reduced, if not removed.

- **Technology and processes exist to address the risk that Internet gambling operators might defraud consumers.**

An underlying premise of any regulatory regime such as that proposed by Congressman Frank in H.R.2046 is that stringent due diligence and financial viability checks will be satisfied prior to any license being issued. As an extension of this, SecureTrading Group will only provide clearing and settlement solutions to operators who have been licensed under this regime. Notwithstanding this strict licensing regime, SecureTrading Group has technology and processes in place, which will largely mitigate any likely fraud against consumers by operators.

There are two potential avenues for consumers to be defrauded by operators:

Financial - from the perspective of a fraudulent payment card transaction posted by an operator, a consumer has the recourse of charging back the transaction. The "rolling reserve" escrow arrangement in place with Baker Tilly will result in the funds being available to refund the consumer. This virtually eliminates the incentive for merchants working with SecureTrading Group Ltd to defraud their customers. In the sector of Internet gambling, SecureTrading Group Ltd has and will only deal with properly licensed, reputable, and authorized gambling operators.

---

[10] *See*, United States General Accounting Office, "Internet Gambling. An Overview of the Issues", December 2002, GAO-03-89, p 37 (available at http://www.gao.gov/new.items/d0389.pdf).

[11] *See,* United Kingdom Department for Culture, Media & Sport, "The Future Regulation of Remote Gambling: a DCMS Position Paper", April 2003, para. 69-70 (available at http://www.culture.gov.uk/global/publications/archive_2003/gamb_position_paper.htm).

"Rigged" Games – licensed operators in leading regulatory jurisdictions, both land and Internet based, are required to satisfy the regulator that games offered to consumers are fair and operate honestly. One example of an independent standards authority for the online gaming industry and which oversees fair gaming, player protection and responsible operator conduct, is the non-profit organization eCOGRA (www.ecogra.org) with its Generally Accepted Practices (eGAP). It is a requirement of any leading regulated jurisdiction, land and Internet based, that games and related financial transactions are fair, money is safe and secure, and that those involved in the conduct of gambling operations are suitable persons. It is anticipated that such compliance requirements would be an integral component of a regime envisaged under FinCEN.

V. POLICY ISSUES

As stated above, SecureTrading Group Ltd endorses the regulatory regime proposed under H.R.2046, the Internet Gambling Regulation and Enforcement Act of 2007. The non-discriminatory licensing process coupled with relevant opt out provisions for states, tribes and sporting leagues, promotes a commonsense control structure at the same time providing the government with an opportunity to generate additional revenue. SecureTrading Group Ltd believes the obligations under the bill relating to consumer protection - underage, problem gambling, absence of crime, money laundering and fraud specifically, in the context of the opt out provisions – can readily be combated by the use of technological tools, addressing concerns with online gambling previously discussed.

In the view of SecureTrading Group Ltd the most serious of all the concerns in an unregulated environment is the possibility of organized criminal activity involving online gambling, such as money laundering and fraud. However, as discussed previously, H.R. 2046 proposes a regulatory regime that will address these concerns via stringent due diligence and suitability checks and ongoing monitoring, at the same time providing consumers with the necessary protections.

SecureTrading Group Ltd recognizes that banks and operators of payment cards are already subject to sufficient federal requirements to combat money laundering, and when applicable, to state requirements to combat fraud. But other types of current and developing Internet payment methods being driven underground by prohibition efforts may not be under any existing federal or state obligations to apply these types of protections.

For this reason, SecureTrading Group Ltd supports H.R. 2046 and the use of technologies, processes and regulatory oversight to combat organized crime, money laundering and other fraudulent activities. Technologies and processes do exist today and are being used to accomplish these goals. Furthermore, if Congress requires use of such technologies to protect the public interest, the market will inevitably create further products designed to address these risks for any businesses that wish to handle any such lawful transactions.

VI. CONCLUSION

Regardless of the position that Members of Congress take on the prohibition or legalization of Internet gambling, we can all agree that there are certain "ills" that must be prevented. One would be hard-pressed to find an advocate *for* underage gambling, compulsive gambling, money laundering or fraud. I sincerely hope that this testimony has demonstrated that there are ways to protect against these exact harms and ills that the opponents of Internet gambling regularly cite as reasons to prohibit Internet gambling. SecureTrading Group Ltd has developed and implemented a robust and 'fail-safe' payment system which has withstood the test of time. The system has been found to work successfully by regulators and law enforcement in other countries.

I am confident that SecureTrading Group Ltd and other providers could develop additional approaches that would address whatever regime the United States and, as applicable, individual U.S. states, tribes or sporting leagues may adopt.

Accordingly, if Congress decides to allow *any* Internet gambling transactions to occur, they should do so knowing that technology and processes exist to protect their constituents from falling victim to underage gambling, compulsive gambling, and involvement of organized crime, money laundering and fraud. It exists, it is being utilized, and it is working very effectively.

I remain available to provide further information to the Chairman and other Members of this Committee, as well as to other Members of Congress, regarding the mechanics of our approach to combating fraud, money laundering, underage gambling, compulsive gambling, and organized crime involving online gambling or to review the various approaches undertaken to manage these issues worldwide.

Mr. Chairman, I thank you and the Committee for its time and appreciate the opportunity to submit my remarks for the record.