Testimony of John Lyons
Group Security Advisor
UC Group

House Committee on the Judiciary
Wednesday November 14, 2007

Hearing on Establishing Consistent Enforcement Policies in the Context of Online Wagers

Mr. Chairman and Members of the Committee:

My name is John Lyons. I am Group Security Advisor to the British payments services provider UC Group, where I am responsible to the Board for advising on all matters relating to risk and security and for relations with law enforcement agencies.

I am also Coordinator for the Corporate Executive Programme, an organisation comprising some of the world's largest global enterprises including Intel, HSBC, Diageo and Mitsubishi UFJ – established by FIRST (the Forum of Incident Response & Security Teams to provide advice upon the implementation of global risk strategies). During my time as an employee of the UK government I served as the UK's Crime Reduction Coordinator at the National Hi Tech Crime Unit (NHTCU).

I am pleased to provide the Committee this written testimony to address the issue of online wagering from a security and law enforcement agency perspective relating to the security and integrity of online financial systems.

Summary

The question has been raised whether the prohibition of Internet gambling is necessary to protect consumers from various risks linked to Internet gambling, in particular, the risks of compulsive gambling, underage gambling, money laundering and fraud.

As the Committee considers whether the current U.S. regime of prohibition is being effectively enforced, it should also consider the fact that there exist technological solutions today which could be adopted to bring a very high degree of safe and secure practice/s to online financial transactions, including those relating to Internet gambling. Such solutions will protect not only the consumers but

also the integrity of the financial infrastructure that they are using to facilitate Internet gambling transactions today.

Implementation of such solutions is not only possible in connection with regulating Internet gambling, but is necessary in the broader context of the online payments system. Indeed, if we fail to act promptly to strengthen our ability to secure online financial systems, we face the prospect of organised crime and terrorism gaining more and more funding from innocent consumers - whilst banks and credit card schemes positioned in the middle, act as unwitting facilitators.

Internet Gambling Regulation Promotes Internet Security

There is a pressing need to respond proactively before customer confidence is diminished irretrievably, the integrity of the financial systems is challenged and before governments, legislators and regulators are forced to react to mitigate the potential damage by bringing the online financial industry into line. This threat pertains to all sectors utilizing online financial transactions and not just to the Internet gambling industry. Many informed sources and experts in this arena take the view that we are presently losing the battle in the online space to organised criminal and terrorist groups (sometimes referred to as 'non-state actors') and to hostile foreign governments. Ironically, the very steps needed to create a secure regime that protects consumers in the area of Internet gambling are needed in any case to protect the Internet overall from this array of threats.

The basic principles of actions that need to be taken to protect the payments system generally, and to provide for consumer protections in the area of Internet gambling, are by now well documented. They include:

Authentication and Identity Management – proving beyond reasonable doubt that the person conducting the transaction is who they purport to be.

Authorization – proving that the identified person is the authorized user of the credit / debit card or other financial instrument being used in the transaction.

Age Verification – a second layer of security and process sitting behind the items mentioned above, and which may require

persons to verify their date of birth before access can be granted to goods and / or services online.

User Location – certain services offered online may require that a user's location is identified. In some cases this might merely mean by country, but in other cases the service may require location verification to county / state level or better[1]. Often, the various obstacles which can be placed in the way of technically verifying location data cause concern to many. However, the online merchant, operator and financial services company, can, based on the level of transactional risk involved and the nature of the service, decide to decline the transaction in cases where the location cannot satisfactorily be confirmed (for whatever reason).

Data Sharing on Criminal Activity – every company in the online financial transaction chain holds data relating to criminal activity and attempted activity. Sharing this data throughout the financial 'supply chain' would provide increased levels of assurance in authorizing online transactions whilst providing a significant weapon in the fight against online fraud. In addition, the ability to provide industry reporting of such criminal activity to government and to law enforcement and security agencies would significantly enhance their ability to prevent and investigate online crime.

Two Factor Authentication – The operators involved in certain high risk categories of online transaction, such as travel, gambling, electrical goods and international transactions, could provide their online customers with a second tier authentication token to provide increased levels of assurance and security. Distributed in a secure way to users, this would provide a high degree of certainty of identity, authority and age. Indeed, one might ask why the issuing banks which provide credit and debit cards for use online, do not offer this service now.

Regulation and Enforcement

Currently, law enforcement agencies benefit from the open interaction they have with financial services companies and

[1] Currently Internet Service Providers (ISPs) are very often able to provide this service retrospectively in response to authorised requests from law enforcement and security agencies. However, real time analysis is what is needed and ISPs should be invited to provide solutions for commercial use.

payment providers who provide services to a broad range of e-commerce merchants. A flow of information and intelligence exists from many of these companies, which provides law enforcement with a greater understanding of the nature of new criminal modus operandi in online transactions. In cases where law enforcement agencies choose to investigate online criminality, having the ability as law enforcement officers to sit down and meet with all regulated Internet gambling companies and their payment service providers, banks and credit card companies provide an enormous boost to the ability to fight e-crime.

An Example of Regulation and Enforcement Working

Whilst serving as the UK's Crime Reduction Coordinator at the National Hi Tech Crime Unit (NHTCU), now a part of the UK's Serious Organised Crime Agency (SOCA), I had responsibility, inter alia, for ensuring that law enforcement, the financial industry and online businesses worked closely together in the fight against e-crime. During the period 2003 to 2004, organised crime groups based in Russia, were orchestrating sophisticated Distributed Denial of Service (DDOS) attacks against Internet gambling companies. These attacks, using netbots – thousands of compromised PCs with broadband connections around the world – brought down many Internet gambling companies. In essence, they were taken off the Internet and rendered unable to function.

In some cases, these DDOS attacks succeeded in taking hundreds of other businesses off the Internet, because they were connected to the same Internet Service Provider.

Once these attacks had succeeded, the organised crime group, made contact with the Internet gambling companies demanding various payments before the attack would be terminated. This was nothing less than extortion.

In the face of this organised crime onslaught, a number of Internet gambling companies called on the assistance of the NHTCU.

The NHTCU subsequently held a round table meeting with 19 Internet gambling companies represented by their CEOs, Chief Technology Officers and in some cases with their finance chiefs.

The companies were encouraged not to pay up – since by doing so, they would almost certainly have broken money laundering laws

and assisted criminal activity. From the meeting, NHTCU assembled a wealth of evidence and technical data, launched an investigation and subsequently worked for many months with law enforcement officials in Latvia, Lithuania, Belarus and then Russia – where the UK Foreign Secretary of the day discussed with the Russian President, Mr Putin, the need for law enforcement cooperation – which was successfully secured.

By contrast, many unregulated Internet gambling companies in off shore locations were also subjected to DDOS attacks – they simply paid up and continued to do so in the face of further attacks, thus facilitating the success of organized crime.

During the subsequent investigation, which has since come to a successful conclusion, the NHTCU discovered a huge amount of material and evidence to not only assist the DDOS/Extortion investigation, but which also provided evidence that these same organised criminal groups were behind a vast global network of other online criminal activities. These included "phishing" attacks against the USA, Canada, Australia and the UK. It included evidence of massive credit card theft and fraud, the sale of technical exploits and malicious code online to the highest bidders, the control of netbot armies comprising tens of thousands of compromised PCs and servers, the counterfeiting of national identity documents and driving licences, online paedophilia, website defacement – the list was endless, the organisation was superb! The same organised crime groups were involved in many of these activities, and no doubt continue to be so.

Negative Consequences of Prohibition

My point is Mr Chairman, without the ability to reach out, meet, discuss and share information with legitimately regulated companies trading in Internet gambling, law enforcement will find it hugely difficult to bring satisfactory resolutions to investigations. Without regulation of Internet gambling businesses, they will find it enormously difficult to introduce preventative measures to block criminal activities before they succeed.

Without putting in place a robust regulatory regime which introduces the safeguards outlined earlier in my testimony, the entire online sector (not only Internet gambling operations) will continue to be at the mercy of organised criminal groups and will continue to be a source of terrorist funding. In short, if you

regulate an industry and thereby establish security standards, you are able to protect that industry, the consumers who use it, and the infrastructure it uses at the same time. Thus, the regulation of Internet gambling not only has a protective impact on consumers engaging in the gambling activities, but on the Internet itself, just as putting security standards in place for financial institutions and the payments system strengthens a wide array of online protections.

In my opinion, prohibition of Internet gambling in the USA creates a substantial risk of having huge amounts of U.S. persons' currency getting into the hands of criminal groups. Such groups move into unregulated markets, and a prohibition model is in practice just that – a market that is not regulated in practice, because there are no standards that govern it. Operators taking bets from U.S. persons must today operate in the shadows, and that means in the absence of oversight. The result is that unscrupulous alternative payment mechanisms hooked up with unregulated Internet gambling sites off-shore are filling their pockets with untaxed earnings. Located in the shadows, these operators are able to avoid meaningful US enforcement. Publicly traded Internet gambling companies, regulated by internationally recognized regulators, are no longer doing Internet gambling business with the United States. Their hidden counterparts operating where they cannot be seen continue to do so. The passage of the Unlawful Internet Gambling Enforcement Act 2006 thus has had the unintended consequence of helping those over whom the U.S. has the least information, the least oversight and the least capacity to control.

Addressing the Social Problems

Underage gambling, compulsive gambling, involvement of organized crime, money laundering and fraud are areas of public concern and are not unique to the United States but 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. The strength of such a system is

complemented by the strength of the controls and vigilant oversight of the financial institutions.

Operator Enforcement Supplementing Government Enforcement

In a prohibition regime, the government has to do all the enforcement, a task that is in practice impossible to achieve. In a regulatory regime, the operator becomes the primary mechanism by which enforcement is undertaken.

In a regulated regime, 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.

The operator must also 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 For example, the system used by UC Group in Europe 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. The accuracy of one of these systems 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. Such a 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 the operator. The next barrier is provided by the card issuance rules in place for financial institutions.

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 organization 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.

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.

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

Enforcement and compliance with regulations cannot be perfect and requires continuous improvement and enhancement, but this can readily happen in a regulated regime where operators, regulators, and law enforcement work over time to strengthen the integrity of the industry subject to regulation.

This is even true with regard to addressing the risk of compulsive gambling. It is an issue that 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.

A good online 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 and subject to the “human error” of individuals in attempting to physically identify excluded persons. 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, an integrity system prohibits 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 a properly designed Internet gambling 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 can be 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.

All of these kinds of controls make it easier for an enforcement agency, such as the Department of Justice, to protect U.S. consumers, because in such cases, a regulator sets standards, auditors audit them, and a rogue operator can be dealt with as a rogue, an exception to the norm, rather than the norm.

In summary, the most safe and secure way to protect US Citizens who wish to wager online is to regulate the industry, give law enforcement the opportunity to work with US licensed operators and payment service providers and implement the measures outlined earlier in my testimony. I commend to the Judiciary Committee, as an alternative to prohibition, a regulatory structure for dealing with the issue, such as Chairman Frank's HR 2046 initiative, the Internet Gambling Regulation & Enforcement Act 2007, or a similar approach.

I thank the Chairman and Committee Members for the opportunity to submit this testimony.