Age Verification for Online Gaming

Query Method Versus Multi-factor Authentication

This document contains information that represents the present view of CardLogix Corporation and the issues discussed at the time of publication. Because CardLogix must respond to changing market conditions, it should not be interpreted as a commitment on the part of CardLogix, and CardLogix cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. CARDLOGIX MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. Other product or company names mentioned herein may be the trademarks of their respective owners.

CardLogix Corp. 16 Hughes, Irvine, CA 92618, USA

www.cardlogix.com Phone +1 949 380 1312 Fax +1 949 380 1428

CardLogix

Index

Overview 2
1. The Current Situation 2
2. Multi-factor Authentication 2
3. Stakeholder Issues & Industry Challenges 3
4. The Need for Secure Credentials - Challenges of Both Approaches 4
5. Conclusion 5
6. About CardLogix 5
7. Glossary 6

Overview

Online gaming has become prevalent throughout the world, and is now undergoing review for legalization in markets worldwide. As inevitable as this trend seems, basic concerns from legislators still remain about how to control this activity in an increasingly diverse and complex digital world. One of the primary concerns is underage gaming. Some governments have green-lighted online play, with just a credit card and some routine checks of public databases.

To date, there has been no means to absolutely confirm that an online player is old enough to legally play. This "good enough" approach has alarmed many, from multiple governments to interest groups attempting to protect children. Studies show that underage players are three times more likely to develop problematic playing than adults. For governments considering legalizing online gaming, the prevention of underage play has become a major issue hindering progress. According to FairPlayUSA, U.S. gamers play illegally on 1700 sites based in other countries.

This brief discusses the need for a more secure approach to online age verification. Technology is now available to addresses the complexity of digital identity, online transactions, and tech-savvy players. Instead of gathering and storing tangential data that can be easily discovered or misused, this technology depends on the most compelling and undeniable of human identifiers to succeed—the face and fingerprint.

1. The Current Situation

Online transactions are commonplace today in retail, banking, healthcare, and business. Many methods have been employed to authenticate the identity of the consumer and the transaction. Most processes are built on trust that the connection is secure and the client PC is protected from attacks, such as viruses and Trojan horses.

One type of attack to online identity is "phishing". To prevent phishing attacks, some banks present a picture as a reminder to the user that they are signing in to the correct site. This low tech approach is only marginally effective against phishing attacks.

A common protection against underage access relies solely on the user's input that he or she is of legal age to proceed. This trust based method is often used to gain entry to websites containing adult content. This process obviously will not pass any legislative scrutiny.

The *Query Method* is considered by some groups as the next level of sophistication in determining an identity to protect a transaction or logon. This typically uses a one-time vetting of a person in order to work. When someone applies for online access, personal identifiers such as social security and driver license numbers are compared against semi-public records, such as utility bills. These various data points, including other qualifiers such as IP address, are applied tangentially to produce an approximation of identity, including age and expected location. If the data query algorithm indicates that the person falls within an acceptable range for verification, access is granted. If the data falls outside of the acceptable range, additional questions are asked. Some of these questions may remain as occasional security prompts to the consumer (e.g., "What is your mother's maiden name?"). Typically this process results in the user choosing an online name and password. Unless there is a change to the data set, or the user name and/or password needs replacement, the online user's identity is never again challenged.

2. Multi-factor Authentication

For a truly secure internet logon, a superior method of identification has been successfully applied around the world—*Multi-factor Authentication*. This method uses the advanced credentialing technology of very secure smart cards and biometrics to create an irrefutable identity that can be used across all digital boundaries.

For online gaming, Multi-factor Authentication securely stores a person's biometric identity credentials within an encrypted smart player chip card. The biometric can have many different modalities: face, fingerprint, voice, or iris. The use of one or more of these modalities, in combination with an authenticated card, across any network, establishes the initial vector of player identity and age. When properly executed, the user's biometrics are only stored in the trusted silicon on the card. This lowers the security exposure for the issuer and ensures total privacy for the cardholder.

The Multi-factor Authentication methodology works because:

1. The credential is tied ONLY to the person gaming.
2. Two-factor Authentication is something you have (the card) and something you present (your biometric).
3. The gaming server connection establishes a mutual authentication session directly with the card.
4. The credential is needed for play (card present transaction). This satisfies the payment card industry requirements.
5. An additional encryption layer is provided via a card-based session key.
6. E-signature capability (non-reputable transaction).
7. Communication between the card and PC cannot be sniffed, replayed or attacked via any injected software in the user's machine.
8. Biometrics software matchers can have liveness scans to prevent false person attacks (e.g., like the use of a photo versus the real person in front of the camera). This is achieved through a feature in the software that checks for blinking, or capillary checks on fingerprint readers.
9. Card enrollment/distribution can be used to drive players to land based casinos.
10. Player trust is enhanced by the lack of invasiveness during registration and vetting. Privacy is enhanced due to the biometric being stored only on the card.

3. Stakeholder Issues & Industry Challenges

Government advocacy for online gaming is generating record momentum worldwide, as countries and states struggle economically and seek ways to tax an already booming activity.

In markets where online gaming is not yet legal, banking organizations are barred from handling transactions. As legalization evolves, the many different regulations and laws that take effect are often preliminary or poorly defined. Predictably, banks have been reluctant to support legalization, especially in the U.S. Another concern for the banks is the potential for high value bets and transactions that can be repudiated, or denied, by consumers. These are referred to as "Non-Card Present" transactions, because it cannot be proven that the actual card, and authorized cardholder are present. Banks would be enticed to increase their portfolios in low risk transactions that would come from a non-repudiated card-present transaction.

In many markets and in points of the U.S., there is a general resistance to gaming for moral reasons. The potential of online legalization ignites this argument further. Online gaming detractors argue that the protection of children is a strong reason not to legalize internet gaming. Their argument will rightly follow that the currently proposed legalization with the *Query Method* is not foolproof.

This puts some politicians in an unfortunate position. If they vote for something that could possibly be shown as not infallible, they are at risk; therefore they will stall or not vote for legalization.

Summarizing the Concerns

Stakeholders	Major Concerns
Land-Based Tax Paying Casinos	Loss of Revenue & Brand Extension
Players	Lack of Fair Play & Financial Recourse
Children	Access Restriction
Politicians	Re-Election
Governments	Tax Revenue
Regulators	Methodology To Perform Job
Banks	Non-Repudiation of Transactions
Online Casinos	Over-Regulation

In addition to the markets and stakeholders identified above, there is another potential pool of gamers who have not yet ventured into this arena for a variety of reasons. This anonymous group could possibly represent the largest revenue pool for both casinos and governments. Their concerns are:

- Fear of the lack of fairness and fraud associated with internet activities such as: how do they know they are on the right gaming site with so many phishing attacks on the rise?
- Fear of identity theft from an unregulated online company where they have no recourse
- Suspicion that they are not really playing against other players in a poker room, or that their cards are unfairly exposed to another complicit playing entity
- Possible concern about using yet another name and password that could get lost or stolen by viruses, their children or unhappy spouses. This could put them at financial risk

4. The Need for Secure Credentials - Challenges of Both Approaches

As mentioned earlier, the *Query Method* is currently the one form of authentication being pushed today as a solution for online age verification. This process is used to confirm identity by employing credentials such as a drivers license or account numbers. This data is crosschecked against large pools of information. After a successful crosscheck, the system then derives an answer of age based on probability. The *Query Method* cannot definitively associate a unique human identity to the computer attempting access to online gaming.

The *Multi-factor Authentication* method is the currently required implementation by many governments worldwide for secure internet logon. In the U.S. alone, every employee of all branches of the federal government is issued a smart ID card with the cardholder's biometric data stored on the chip. This is similar to the new e-passports issued around the globe. The strength of the trusted silicon combined with the user's biometric is the accepted approach for a strong credential. It can then be argued for the pending legislation regarding online gaming that this method is already an approved technology for strong identity.

We believe that Query Method-based age verification is no longer adequate for any industry, and especially for online gaming. Although fairly accurate, it is not foolproof. Reasons for this include:

- Professional hackers, using viruses, Trojan horses, and phishing attacks, have become highly sophisticated in collecting data, thus increasing the risk of a stolen identity
- Many tech-savvy teens know their parent's passwords and PINs.
- Internet data breaches are continuing to rise steadily across all business sectors, with the identities of customers left clearly unprotected. For medical records alone, the U.S. DHS reports that more than 11 million people have had their personal information exposed in the past two years. Bank of America, Wells Fargo, Citibank, and Staples retail stores have all had major data breaches. Casino operators cannot afford to become victims of a required publicly reported data breach. A breakdown of trust can have a very quick and detrimental effect on business.

- After the initial process, most *Query Method* based systems rely on a chosen user name and password. User names and passwords are highly vulnerable to brute force dictionary attacks. They are easily hacked or sniffed by viruses and Trojan horses, and sometimes are left on a sticky note or passed from person to person. According to analysts at the Giga Group, the cost of password interactions in call centers is typically $25 per phone call and $40 for every call escalated to the next level. The Gartner Group estimates costs for password replacement can be as much as $18 per user per year.

Comparison of Age Verification Approaches

	Query Method	Multi-factor Authentication
Total Cost	Low	Relatively Low
Privacy-Invasiveness	High	Low
Bank Accepted Transaction	Probably not	Yes
Foolproof/Accuracy	Medium	Ultra high
Casino Liability	High	Low
Mutual Authentication	No	Yes
E-Signature Capability	No	Yes
Integration between internet play and Physical Casino with Continued Branding	No	Yes
Impervious to Identity Theft	No	Yes

5. Conclusion

It is estimated that Americans spend approximately $4-6 billion on internet gambling annually, despite the fact that it is not yet legalized. In the U.S. and around the world, states and local jurisdictions are rapidly legalizing this already prevalent activity. Federal governments must solve basic questions of regulation, in particular the protection of minors, before they can proceed with legalization. Politicians and bankers both want to avoid the risk of supporting the wrong technical approach, so inaction is their inevitable behavior.

Multi-factor Authentication, powered by the proven technologies of smart player cards and biometrics, is an established method for irrefutably integrating identity with play. This method can eliminate some of the fears that hinder political action for online gaming and enable the legislative process to move forward. This method also solves many technical and marketing problems associated with online gaming.

6. About CardLogix

CardLogix has delivered smart cards, software, companion products, and integration to Stored Value and Identity applications since 1998. For over ten years, the company has supplied the Gaming and Hospitality Industry with millions of smart cards for Cashless Play, Player Tracking, Guest Room Access, and Loyalty programs. CardLogix solutions address the growing need in many identity applications for increased security and privacy. CardLogix biometric solutions include products for Gaming, Military IDs, National Health, and Law Enforcement.

7. Glossary (from smartcardbasics.com and creditcards.com)

Authentication — To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Biometric — A measurable, physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity, of an individual. Facial images, fingerprints, and iris scans are all examples of biometrics.

Card Present Transactions — Card present transactions are those in which a card is physically present. Merchants are charged different levels of fees by the card transaction processors (such as Visa, MasterCard), depending on the level of fraud risk. Card present transactions (because the card is available for inspection) are considered less risky. Therefore, they carry lower fees than online or phone transactions.

Credential — A card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. A smart card can store multiple digital credentials.

E-Signature (Digital signature) — Digital information used for the purpose of identification of an electronic message or documents. Digital signatures provide a way of authenticating the identity of creators or producers of digital information.

Factor — A physical or informational item that allows authentication of identity. There are three types of factors: Something you know, something you have, or something you are.

Phishing — A cyber attack that directs people to a fraudulent website to collect personal information for identity theft.

SSL (Secure Sockets Layer) — A cryptographic protocol that provides authentication and confidentiality to internet applications.

Trojan Horse — A seemingly useful and innocent program containing additional hidden code, which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Trusted Silicon — Part of a technology called Trusted Platform. Trusted Silicon refers to chips within smart cards that are designed to protect data and secrets. The architecture of the Trusted Silicon chip prevents attacks through many design and cryptographic features. The silicon and platform are supported by many semiconductor and computer manufacturers.