The Report Committee for Michael David George
Certifies that this is the approved version of the following report:

Identity Trust Framework for iGaming

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor:

____
Suzanne Barber

____
Craig Blaha

Identity Trust Framework for iGaming

by

Michael David George

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in
Identity Management and Security

The University of Texas at Austin
December 2017

Dedication

To Katia, Alek & Natasha. I appreciate all your support, as well as from my family and friends, in my adventure in the master's program and report.

Acknowledgements

I would like to thank my supervisor, Dr. Barber and reader, Dr. Blaha of my master's report committee for their encouragement, insightful comments, and hard questions.

I would like to express my sincere appreciation to Dr. Andre Wilsenach, Executive Director at the UNLV International Center for Gaming Regulation at Las Vegas, Nevada in sharing iGaming industry knowledge.

Abstract

Identity Trust Framework for iGaming

Michael David George, M.S.I.M.S

The University of Texas at Austin, 2017

Supervisor: Suzanne Barber

Abstract

The online gambling community, or the iGaming industry in the United States has individual solutions and a mix of classic processes to manage universal customer identity but it lacks a standard identity management framework in which to enroll new iGaming users, monitor those users and ensure secure transactions, which leaves it open to identity theft and financial fraud.

The iGaming industry offers online poker, sports betting and casino table games. iGaming providers (provider/providers) include companies such as PartyPoker.com, Pokerstars.com, Bovada.com, BetOnline.com among others. An iGaming player (player/players) is anyone who plays to gamble on games through the Internet. This report focuses on the requirements and specification for an Identity Trust Framework to enhance security and privacy in the United States iGaming industry and players.

Table of Contents

List of Figures

Introduction

The Global iGaming industry size, as stated by Statista, is "$45.86 billion growing to $56.05 billion by 2018."[1]. iGaming has seen a rise driven by celebrity players & television broadcasting. Countries that have legalized iGaming include Australia, Belgium, Canada, France, Germany, Gibraltar, Hungary, Ireland, Italy, Liechtenstein, Macau, Malta, New Zealand, Panama, Philippines, Poland, Russia, Scandinavia, Singapore. Spain and Switzerland. In the United Kingdom, the number of active online gambling accounts held "in 2005 was 4.92 million and currently there are approximately over 17.22 million accounts between November 2014 and March 2015."[1]. Argentina, Mexico and a few Asian countries have all started the process of legalizing online gambling.

For the United States, iGaming is in the infancy and evolving. Before 2006, online gambling, which came in prior to iGaming, was significant in the United States. Residents of the United States had a choice of different gaming places on the internet. By 2006, the American government passed a legislation called the Unlawful Internet Gaming Enforcement Act. The act had a profound effect on the online gambling industry, as it created a legal environment that led to many providers pulling out of the American market. US Players had fewer options and playing on offshore sites seemed riskier as the providers where not necessarily in compliance with domestic laws.

In the United States, it is legal to gamble online in Nevada, New Jersey, Delaware and Pennsylvania (November 2017). Another seven states are in the process of legalization (California, Illinois, Massachusetts, Michigan, Mississippi, Washington and New York).

The iGaming industry does not have a consistent framework to manage customer identity in order protect iGaming players and providers from identity theft and financial fraud. Since 2014 "online gambling fraud has increased 60 percent."[2] Compared to other online commerce industries, which includes retail, travel, and online financial services there has been a 25 percent decrease in detectable fraud over the same period.

What are the current challenges for the iGaming industry?

The iGaming industry is confronted with a diverse and complex set of challenges:

- The Identity Trust Framework (ITF): The iGaming industry must provide different levels of assurance and player identification process instead of using a mix of classic unreliable processes (copies of driver's license, passport, etc.). Levels of assurance include a degree of confidence in the processes of authentication. Assurance provides that the entity claiming a particular identity, is the entity to assigned to that identity.
- Enrollment: The iGaming industry must collect and secure PII (Personally Identifiable Information). "PII is information that can trace an individual's identity, either alone or combined with other information linked to a specific individual. Examples are name, address information, telephone numbers, SSN, biometric data (height, weight, eye color, fingerprints, etc.)."[3] This process will assist to simplify and standardize the end-to-end process of the player's account from creation to closing. The Intelligence sharing among the iGaming industry will share common risks and best practices regarding player protection.
- Identity proofing: to disclose and trace an individual's identity and create a player account. The iGaming industry must be capable of vetting PII to confirm iGaming players are who they say they are.
- Identity Management Lifecycle: The iGaming industry must be capable of simplifying and standardizing the end-to-end process of the player's account from creation to closing.
- Intelligence sharing: The iGaming industry must develop mechanisms to share common risks and best practices regarding player protection that occur in iGaming.

What is an Identity Trust Framework (ITF)?

The Identity Trust Framework (ITF) will provide multiple levels of enforcement mechanisms for parties exchanging identity information. The OIX (Open Identity Exchange) is a membership organization that works to accelerate the adoption of digital identity services based on open standards. The OIX states: "A trust framework is simply a legally enforceable set of specifications, rules, and agreements governing the operation of a specific multi-party system."[4] Further described by OIX President Don Thibeau, "The purpose of a trust framework is to ensure both the functionality and trustworthiness of the identity system. Ensuring that the identity system functions properly is a fundamental goal. Yet, a functional identity system is not necessarily a trustworthy one. The specifications, rules, and agreements that comprise the trust framework must be written to help ensure the level of trustworthiness required by the entities participating in the identity system and the community relying on the services offered by the identity system."[4]

The ITF has operational roles responsible for ensuring common policies and address information sharing. Any provider (or participating entity) can make changes to the ITF. A committee is usually created for all or some of the participants utilizing the identity system for required changes or any regulatory issues. The ITF is efficient and scalable allowing participants and end players to rely on assurances for identities, verification and authentication. The provider issues the credential to a player once the identity, security, and privacy policies are complete. The framework offers a certification program for large multi-party identity systems, that enables a party who accepts a digital identity credential and the relying party. The relying party in this case is any entity which makes a statement about itself, in order to establish access.

Based on the definitions, the iGaming trust framework must:

1) Define the requirements for the proper operation of the iGaming identity system by providing a governance structure that includes technical and operational specifications legally binding on all providers.

iGaming can create a governing agency, such as the New Jersey Casino Control Commission, but a federal entity that houses policymakers, for administering regulations, granting licenses and ruling on disciplinary matters. An iGaming agency could utilize Nevada or New Jersey regulatory board, but include representatives from each state in which iGaming is legal in the United States. The Nevada Gaming Commission is a state governmental agency involved in the regulation of casinos throughout the state, along with the Nevada Gaming Control Board (NGC). The NGC founded in 1959, would provide a deep reference to gaming and best practices. Another seat at the iGaming agency would include the International Gaming Institute (IGI), which provides research and educational programs in the United States and across the globe.

The provider certification process protects the iGaming player's identity while ensuring compliance and security for the iGaming provider. These certifications for providers can be a valid stamp of authentication, representing compliance by the iGaming providers website or a cumulative compliance list.

The assessors and auditors, can validate the certification criteria and iGaming trust framework requirements. The iGaming auditors would conduct quarterly audits for the iGaming provider during the first year, then move to a yearly audit. Existing regulations could be of use from Nevada or New Jersey, as both have a deep history in gambling laws and regulation. The focus is ensuring best practices for identity protection requirements.

The iGaming Identity Trust Framework is to ensure the exchange of identity information. As noted, "it needs to combine objective criteria for measuring parties' capabilities, processes for conducting assessments, and a set of agreements tying participants together."[3] OIX introduces this as the required agreements within the "Principles of Openness". iGaming will benefit from the transparency, accountability, mechanisms and process by each of the participants, as described above. The participants can commit to abide by the Principles of Openness and incorporate them into their agreements. This includes the concept of non-discrimination, to ensure parties avoid exclusive arrangements. In summary, providers must be consistent with laws of their jurisdiction to include open reporting and periodic reports on governance.

The iGaming Identity Trust Framework model specifies that there are three main mechanisms required which include a criterion for measurement, set for certification process and legally binding agreements. The criteria for measurement, would be to assesses the iGaming providers ability to meet the technical, operation and legal parameters. As stated, "the policymakers and identity trust providers will need to include criteria by which potential new participants may be measured."[4] Policymakers and iGaming experts can share the standardized criteria and best practices for participants to understand, apply and become compliant. If possible, the goal would be to ensure meeting criteria not only in the United States, but extended to interact globally.

2) Ensure regulations for the processing of identity information (PII).

To be successful, iGaming providers and players must be willing to participate in a large-scale network of trust, linking identity service providers. The provider would want to know how accurate the PII is. The capture and identification of strong credentials includes driver's license, state ID or passport or fingerprints. When the identity provider shares player information and PII, a primary concern is to establish trust with other iGaming providers, who do not currently share sensitive information within the United States subject to an existent iGaming intelligence sharing center.

As each state becomes legal for iGaming, the providers can establish a standard way to share identity information and risks throughout the United States. This would ensure compliance, for providers in each state to integrate and address standardized formats for PII. Each provider will need to agree to liability via contracts. In those contracts, the demarcation of rules and laws contained in each framework. Currently, iGaming providers processes vary from provider to provider. The identity solution will register accounts with the iGaming Identity Trust Framework to enroll for access, privileges, and resources within the gaming platforms. The provider is responsible for the player's identity data and validation, which generates a significant risk in handling player's privacy data. The iGaming providers can standardize within the United States, but may or may not standardize across the globe as inconsistent frameworks exist among the United Kingdom, Europe and Australia.

3) Define roles and operational responsibilities of providers and players.

ITFs consist of multiparty agreements among members, which enforce requirements and ensure trust in the acceptance of identity credentials. To create an iGaming ITF, all members adhere to enforcement rules and policies by identity providers. Identity providers are the iGaming companies which will create, maintain, and manage identity information for players. Examples of other trust frameworks include credit card, electronic fund transfer and privacy frameworks. In an Identity Trust Framework (ITF), the set of specifications, rules and legal obligations address a specific element or issue of importance to the transaction by each trust framework.

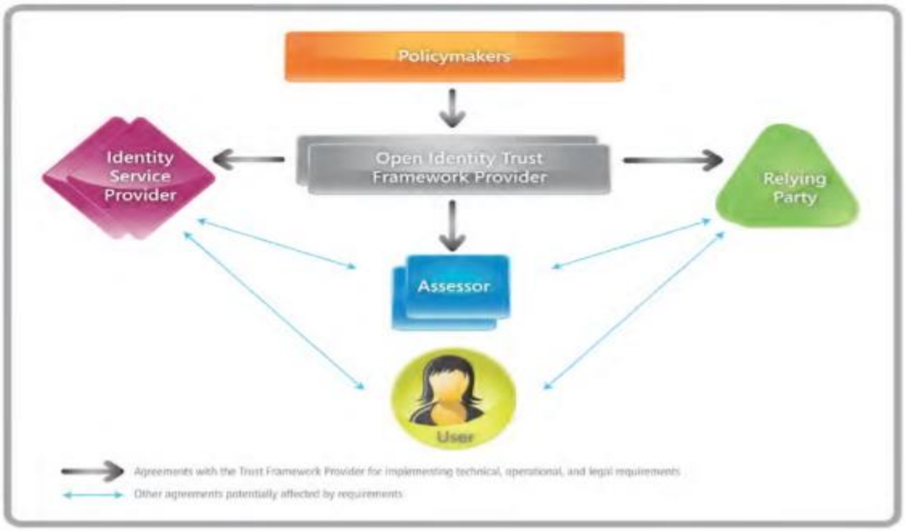

Policymakers
Identity Service Provider
Open Identity Trust Framework Provider
Relying Party
Assessor
User
Agreements with the Trust Framework Provider for implementing technical, operational, and legal requirements
Other agreements potentially affected by requirements

Figure 1: OIX: Participants in an OITF Identity Information shows roles and relationships in terms of agreements, which links the participants.

The iGaming provider will need to ensure inclusion for all iGaming providers to follow trust framework requirements. The identity provider would reduce risk and promotes efficiency "by issuing credentials and confirming aspects of the exchange."4 The provider can hold enforcement mechanisms for parties exchanging identity information and ensure player validation and player attributes are protected and shared. Requirements and mechanisms must support the flow of information among players, identity service providers, and relying parties.

4) Provide adequate assurance regarding the accuracy, integrity, privacy and security of its identity data and processing.

The iGaming Identity Trust Framework providers will ensure the set of certification requirements given by the policymakers. The providers can utilize the certification process which look to validate the capabilities and "vet" the process to have a clear set of requirements for certification. “Typically, providers will include five basic processes which include the assessor may provide evaluations for the trust framework including conditions like competence, independence, absence of conflict of interest”. [4] The identity service provider “may apply for certification from among the options available, such as self-certification, audited certification and third-party certification.”[4] A process for “accepting the assessment results and publishing the final output of the process through certification listing service”[4] by the provider. The process allows for renewing certifications “at regular intervals, with possible auditing of compliance”[4] which require future updates.

The legal structure ensures requirements and agreements for the iGaming trust framework. The first legal requirement is the policymaker and providers must have a contract to enter into agreements. The overall agreement sets out to ensure the technical, operational and legal requirements by policymakers. The second, consists of identity provider certification agreements which ensures a contract bound between the provider and certified identity service providers. The third is the relying party certification agreements. “These are contracts between the OITF provider and relying parties who have been certified to meet the technical, operational and legal requirements of a trust framework.”[4] The fourth part is the assessor agreements, which are contracts with the providers. The assessors basically evaluate the identity service providers and relying parties with sign off. The last is the Terms of Service (TOS) Agreements, which “is designed to establish the rights and responsibilities for players that they do not already have in TOS agreements with identity service providers and relying parties, the relevant requirements may need to flow down to the TOS agreements that directly involve players as parties."[4] Essentially, there is no single trust framework agreement, the five types of agreements coincide to work to form the legal structure for the iGaming Identity Trust Framework.

If the iGaming industry truly wishes to experience high growth globally, the expectation is to adhere to the new standard for consumer rights regarding their data. iGaming will ensure to put systems and processes in place to comply for European iGaming parties and European players. The General Data Protection Regulation (GDPR), a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions. This will ensure all providers are subject to audit of conformance and may be under each provider's privacy policy. A public facing iGaming privacy policy would contain all these items and represented on each of the iGaming provider's website. OITF providers can state on their public websites how the OITF provides accountability for identity information exchanges.

How does the iGaming Identity Trust Framework meet challenges and reduce risk?

The iGaming Identity Trust Framework is critical for exchanges involving identity information in the iGaming industry, because both players and providers will need to protect themselves from risk. The iGaming ITF will ensure identity requirements are meeting an acceptable format, which is critical to protect personal information. The first concern of iGaming players is PII. The iGaming ITF would support a standard and efficient way to ensure identity proofing while reducing risk that extends to both sides: players and providers. The iGaming providers must identify players to gamble. The player onboarding process is critical, in which to establish and verify the identities as fundamental component for trust and security. A standardization for sign up begins with identity proofing.

Identity Proofing

Identity proofing is critical to the iGaming activity and the transactions required by players to disclose PII. For a player to participate in online game, the first interaction will be to establish a player account, which will include input of various PII.

Identity Proofing "is the process by which a credential service provider collects, validates, and verifies information about a person."[5] The iGaming providers must be able to vet and certify player identities containing PII and additional information about their financial transactions. The identity verification will require a standard format for gathering required proofing information. Each player profile will require a full name, date of birth and home address. The player will need to authenticate to a higher degree of assurance by the iGaming provider.

The iGaming providers must identify customers and link them to specific bank accounts, residential addresses, and other identity proofing details in order to create a player account. An "identity transaction, which involves the collection, storage, processing, communication, and use of information relating to the identity of a person, entity, or device."[3] Usually this consists of a mix of classic processes, such as sharing copies of passports to be able to identify players. This manual exchange of PII is currently in practice, but highly unreliable and random to secure the provider and player.

Currently, there is a lack of advanced and standardized identification techniques to provide multiple levels of assurance in the player identification process. The identity proofing process provides evidence to a credential service provider (CSP) reliably identifying themselves, thereby allowing the CSP to assert identification of a player. These requirements for each of three identity assurance levels. Further, NIST has provided requirements for enrollment and identity proofing, "applicants that wish to gain access to resources at each Identity Assurance Level (IAL). The requirements detail the acceptability, validation, and verification of identity evidence that will be presented by a subscriber to support their claim of identity."[6] This sensitive information is used to build a profile, the iGaming player record. The iGaming providers will want to ensure when creating and enabling a credential, that the players instantly recognized and authenticated before any connection or transactions processed.

Currently, fingerprint recognition via biometrics readers integrate into laptops and smartphones, which may pose an option in identity validation. Fingerprinting or even finger-vein, palm-vein readers, seem to be the most commonly deployed solutions. The advantage to fingerprint recognition technologies, already widely used by banks. Combinations of fingerprints and passcodes can prove to be highly valuable and efficient, which the iGaming industry could leverage. Merchant payments also have facilitated payment transactions utilizing biometrics (customers enroll into the system, put credit into their account using kiosks and credit cards, and pay using their fingers). Other valuable data derived from the Identity Proofing process is verification data in the form of voice recognition, which is a form of biometrics, adopted by banks. Voice biometrics compares the customer's voice to their unique voiceprint on file, signaling the operator verified the identity. Regardless of the biometric utilized, the goal is to have a fast, efficient and effective way to proof an identity for initial enrollment and then ongoing identity validation checkpoints. A rapid enrollment process will capture all identifying content required to establish an iGaming identity.

Unique Identifiers

A credential, as defined by NIST is "an object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber."[6] Once the identity proofing system has gathered the required data, the iGaming providers are able to create "Identifiers" which may include identity information about the subscriber collected in the enrollment process. iGaming should focus on unique identifiers, to ensure an interchange format that is universal. This unique identifier could be comprised of letters, numbers or preferred code used, rather than a player's PII. The universal identifier would serve as key to access both public gaming platform and the iGaming private databases. The identifier should not be secret, such as a name or selected identifier number (and iGaming code). The actual unique identifier would avoid redundancy, and leave space for administrative information or future expansion. This unique identifier use is for stand-alone transactions as well, such as a call to the technical support center just needs a key to access a game, database, or financial transaction to benefit the player and provider.

Enrollment

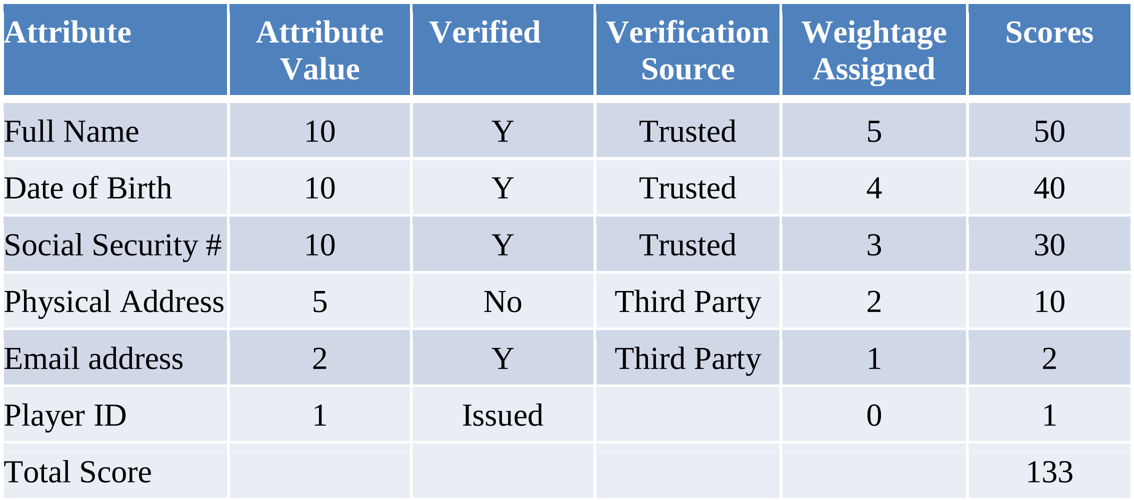
The enrollment process for iGaming platforms and players is also key. Pre-Enrollment requirements include various levels of player identity data such as mobile number, geo-location, IP address and validation via social network sites. "Enrollment is the process through which an applicant applies to become a subscriber of a CSP and the CSP validates the applicant's identity."[3] The enrollment process must avoid long waiting times and complex registration procedures. Enrollment would request strong attributes (first name, last name, employee identification or driver's license). The performance objective would be to validate identity among multiple points to include biographic information, identity documents, compliant facial images, fingerprints, iris and digital signatures.

The enrollment process should be standard, scalable for growth, and provide a seamless user experience. iGaming should not limit attributes associated with identity, a second key requirement of a global identity management service. During the enrollment process, the capturing of identity data and establishing a proven identity record is critical. Individuals should be able to complete the enrollment process online, which would be a secure capture of required biographic information, such as name, address, and social security number, and verify against trusted sources. The amount and type of data captured is dependent on the level of assurance and risk associated with the transaction. Once validation has proven the identity record, it can then be active for future verification of identity to access services, applications or accounts. Once the proofing has verified player's identities, the provider will issue accounts and credentials to the player.

Identity Scorecards

The iGaming providers should look to reduce consumer risk. Identity proofing is currently relying on static data. “When iGaming security is discussed at conferences and referenced by regulators, the most common subjects that come up are Know-Your-Customer (KYC) and geo-location… It is something visible that politicians and other stakeholders can easily see, Gus Fritschie, a CTO and gaming security expert explained.”[4] The “identity history” begins here and is aggregated from public and proprietary data sources to now living in the provider’s system.

The first step can be to attain a risk score for individual identity documents or resources used to create a player account and apply a metric. The scorecard provides a metric and ranks the verified data from the player. The “identified level of trust, that the identity is real, based on the accuracy of the attributes presented.”[6] iGaming will need to initially score a new player, for account creation and later monitoring. If attributes are not verifiable, then categorizing the identity should demonstrate a non-trusted status. If a set number of attributes, can verify a set number (say 5), there would be an output of a collective score, the identity will have just in initial proofing to attain a player account. The below is a sample, to evaluate risk from the level of trust, from an initial static score to gain an account.



Attribute	Attribute Value	Verified	Verification Source	Weightage Assigned	Scores
Full Name	10	Y	Trusted	5	50
Date of Birth	10	Y	Trusted	4	40
Social Security #	10	Y	Trusted	3	30
Physical Address	5	No	Third Party	2	10
Email address	2	Y	Third Party	1	2
Player ID	1	Issued		0	1
Total Score					133

Figure 2: iGaming Player Identity Scorecard

Once the iGaming players have an initial or "static entry score", the verification process can be automated. Each level of trust for a player will have a variation in levels, so the trust scorecard functions as a static base in which to then perform ongoing dynamic identity monitoring. iGaming will need to monitor identity behavior once identity proofing and enrollment has completed and players have access to the game.

"Identity Scores" can add dynamic information from a variety of sources and analyzing patterns from the total identity behavior information. Transactions within the platforms provide iGaming player statistics on volume of games played, which games played, the transactions played per game, cost/bets played and payouts which in turn would result in a risk score. The risk score could lead to examination into the identities track record, and see if there is history of unethical or unwanted behavior.

An "identity risk pool" contains a higher identity threat data (if players exhibit specific activities such as random playing times, location data from player login is not of origin or amounts that are irregular). iGaming providers will need to actively monitor identity behavior (an input) to the transactions and payouts (outputs).

Player ID	Type of Game	Table Cash Rate	Amount of hands played	Weightage Assigned	Total Scores
Falcon1	Poker	$1	22	1	22
Gold4u	Sports bet	$5	15	3	225
Callstation99	blackjack	$10	10	5	500

Figure 3: iGaming Identity Scorecard for player behavior

The goal would be to identify bad behaviors, or gauge the "identity risk" once playing. Creating a scorecard would utilize dynamic metrics based on the iGaming player. This could help analyze results of activities, specifically activities that lead to fraud. The scorecard would help to identify threats by estimating the probability that a customer will display a defined behavior. The identity scorecard would demonstrate "weighted" transactions within iGaming platforms. The identity risk would help indicate the potential of gaining or losing value within the iGaming provider's environment.

An identity scorecard for the iGaming provider could include measurements regarding operations and internal processes. National regulations exist to protect citizens from gambling addiction and illegal or unreliable operators. So, the development of regulations and compliance should require successful existing gambling regulations to be consistent and clear for the United States. A scorecard for providers can be based on the contracts, assessment and ensuring the appropriate measures to protect private data and identity information exchange. The "Principal of Openness", should include an identity scorecard to identify those internal mechanisms to ensure reputable providers.

Weight	Scorecard for Provider	Example A	Example B
5	Legal requirements	Auditability	Breach notification
4	Data Protections	Breach notification	Classification of Data
3	Reporting/Publication	Interoperability	Open Versioning
2	Open Disclosure	Awareness/Training	Incident Management
1	Accountability	Retention/Decommission Identities	Business Continuity/ Disaster Recovery Plan
0			

Figure 4: Sample Identity Scorecard for Providers

The scorecard goal is to help safeguard identity transactions and evaluate routine identity transactions to ensure the iGaming providers generate reports on valuable information in the iGaming trust framework and aid in promoting interoperability. iGaming risk must be a continual measurement and monitoring of active patterns of an identity risk score.

iGaming Intelligence Sharing

iGaming providers will need to unify to help identify and share potentially risky or fraudulent activity. The providers should be inclusive, to protect personal information and avoid breach of data across the iGaming industry. An iGaming Intelligence Center, or iGIC, would enhance sharing of player information within the community. Sharing of security or threats provides value, which is to exchange knowledge among the iGaming companies and federal, state, local or other private-sector levels. Currently, federal agencies do not share intelligence, but audits and information reporting are mandatory per governmental regulations for the iGaming industry.

If the iGaming Industry committed to a iGIC model, it would ensure use of open integration and sharing threat intelligence, but provide iGaming player protection, which is more successful. This unified network will house analysts from a diverse set of agencies, similar to “brick and mortar” casinos that have a “black book” or share information about players (identities and behaviors) caught cheating or conducting fraudulent activities (financial or identity fraud). The iGIC could unify the iGaming providers from each state.

An example of intelligence and use of analytics is the Retail Cyber Intelligence Sharing Center (RCISC), which is a cooperative from over 30 retail companies that work to identify common threats and share best practices. RCISC “builds and sustains valuable programs, partnerships, products and opportunities that enable growth in their trust–based relationships, strategic knowledge and tactical capabilities.”[6] Collaboration and shared knowledge among providers could encourage security and growth in the iGaming industry.

Old models focus on internal identity management and the account holders. The key is to separate these identity systems into spheres, which are usually binary (trust or untrusted). Multiple identity spheres should create further depth of the account holder’s activity and identity in iGaming. For example: the account holder/player could be a high, medium or low profile depending on the transactions values.

This type of intelligence sharing, involves a common connection to intelligence and information, typically through secured networks. Player protection will prevent a player banned from one casino from going to another. The iGaming environment needs to develop a more proactive security posture to monitor risk. Better decisions made by the iGaming community would result in the detection of security threats. iGaming organizations should aggregate or correlate security data, but more importantly analyze collected data from multiple sources to support defensive actions in a collective model. The proactive sharing of specific threats to the iGaming industry will aid all providers in fighting cyber-crimes. The result will be a highly focused iGaming industry that is protecting players and maintaining their trust.

The iGaming industry is less mature, so unified communication about security controls and increased identity protections is critical. An example is sharing a threat that would affect iGaming, such as Teslacrypt. The design was to encrypt game-play data for dozens of video games, prompting the player to pay a ransom in order to decrypt the files. For example, this threat can halt poker sessions at which the player is in. Advanced intelligence and communication updates about threats will aid in combating of fraud.

Previously, most U.S. banks prohibited the use of their cards for the purpose of Internet gambling. Currently, those credit card restrictions no longer exist due to recent legalization in United States of iGaming, which would increase deposit activity and thus possible fraudulent activity. The iGaming transactions involve other forms of payment besides credit card, such as debit card, electronic check, certified check, money order, wire transfer, or even Bitcoin. The iGaming players upload funds to the iGaming providers, make bets or play the games that they offer, and then cash out any winnings. The iGaming players can often fund gambling accounts by credit card or debit card, and cash out winnings directly back to the card. So, the number of electronic money services offered and the accounts and funding will be a large target. If the iGaming providers share threat information, the risk will reduce, as long as the technical standardization prevails.

Additional Technical Alternatives

The creation of a new Identity Trust Framework requires navigating possible inputs and outputs of the identity data exchange. A standard for creating identity data and records, securing the transmission, storage of identity data must be present for future exchanges. Technical requirements should consider product versions, software or application standardization, common protocols, storage standards, and the actual transmission and exchange of identity data. Registrations should be standard technical exchanges with other providers.

iGaming must use a common negotiation protocol to allow providers to control the privacy and security terms, under which they are willing to assert identity and exchange of information. The protocol must support anonymity for protection of personal privacy. Additional technical supplements to help maintain flexibility for iGaming may include automation. Automation would lead efficiency improvements in identity recognition and processes that currently require human supervision. For example, banks can accelerate client onboarding by capturing biometric identity documents (such as face and voice recognition) when starting a client contact. For all subsequent interactions, some or all of biometrics can painlessly authenticate the customer.

A common protocol will help assert and authenticate a player identity. The player attributes are part of the credentials (which are stored in a database entry). A technical standard will aid data exchange or interoperability for providers across the iGaming industry. In the past, various XML text strings led open data interchange. The definition of XML (Extensible Markup Language), is a text-based format used to share data on the World Wide Web and intranets. The requirement for coding this standardization should be a universally held standard or at minimum only two options.

The current standard everyone is moving to enable sharing is JSON, which is becoming the dominant data exchange format. JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write, and for industry machines to parse and generate. With the use of Enterprise Service Buses (ESB's), will process applications, pull an authority and go to active directory and create a player to make rest call to inject or share player identity data into all applications- across all multiple data sources. With ESB's options, the iGaming providers could connect to other providers. The core component, Extract Translation Load (ETL) will send data on receiver's end and use processing and their engines to digest and translate the required data. Having this standard would enable all players to hold one identity for multiple service providers while also grant a more effective way to connect to a regulatory body.

Another technology option would be for the iGIC to implement something similar to blockchain. The blockchain can serve as the public ledger for secure online transactions. A blockchain can decentralize and distribute a digital ledger or database used to record transactions across many computers. The record would allow participants to verify and audit transactions inexpensively and ensure a mass collaboration for authentication. Blockchain technologies go beyond transactions and enable exchange as powerful unifiers of data and information. iGaming providers can expect to enable or exclude people within their own and other iGaming platforms. Blockchain technology could make it possible to share and store PII's to help solve problem gamblers or fictitious identities used to commit fraud.

Machine learning is another technical addition which could utilize voice watch lists, which are matched recordings and comparison analysis to prevent identity and account fraud. Contact centers that utilize machine learning have reduced call times and support with an authentication process that is streamline. This could help reduce financial losses from a hack or customer identity fraud. For crime reduction, watch lists can reduce uncertainty of resolving online disputes backed by the provided ITF for iGaming.

Conclusion

The proposed iGaming Identity Trust Framework will enable refinement for architectures, business processes, governance models, operational policies and practices, and member obligations required for identity systems. In creating the iGaming ITF, reducing costs and promoting efficiency, is critical. For a new iGaming ITF to be successful, authorities in different jurisdictions may require a basic set of requirements or agreements. Lack of global standardization and gaming regulations will provide further hurdles, which the iGaming industry can be proactive and facilitate a shared framework. Gambling providers have the challenge of each jurisdiction differing in their demands and how to allow iGaming to use technology to meet regulatory requirements. The iGaming ITF will allow scalability and integration across the globe. In analyzing the components of ITF, identity proofing and enrollment will help provide a foundation for the iGaming identities and ensure protection and integrity for PII and data.

Identity Scores and Identity Provider Scorecards can reduce risk and provide transparent metrics. An identity rating could help the risk impact on multiple levels of identity transactions, with the overall goal of risk avoidance. Audits for risk and security controls will synchronize and integrate systems. Information sharing must align across all internal iGaming activities and across providers. The collaboration through an inter-connection, such as the iGaming Intelligence Center, would reduce threats, enhance risk reduction and promote maturity in the iGaming industry. This report offers key ingredients for a successful iGaming Identity Trust Framework to include a standardized and efficient enrollment, identity proofing, unique identifiers, identity scorecards and intelligence sharing among framework stakeholders. Technology, policy and regulations advances must be embraced to realize a successful future for the iGaming industry.

References

1 "Size of the online gambling market from 2009 to 2018 (in billion U.S. dollars)". www.statista.com. Statista. Retrieved 6 September 2016.

2 "Global Identity Verification Service Reports Online Gambling Fraud Spikes to All-Time High Between Black Friday and Cyber Monday". www.americascardroom.com. By Bob Garcia. December 1, 2017

3 IRS Website: Definition of PII:
https://www.irs.gov/irm/part10/irm_10-005-001.html

4 OIX: The Open Identity Trust Framework (OITF) Model, publication March 2010. Managing editor: Mary Rundle. Co-Authors: Eve Maler, Anthony Nadalin, Dummond Reed, Mary Rundle and Don Thibeau

5 Developing Trust Frameworks to Support Identity Federations, NISTR 8149. By David Temoshok and Christine Abruzzi. Deloitte & Touche. October 2016

6 RCISC: The Retail Cyber Intelligence Sharing Center (R-CISC) is the cybersecurity resource for the retail industry. https://r-cisc.org/

7 Thomas, I., & Meinel, C. (2011). An Attribute Assurance Framework to Define and Match Trust in Identity Attributes. 2011 IEEE International Conference on Web Services 580-587. doi:10.1109/ICWS.2011.80