

# Szrek2 Solutions



REDEFINING

ELECTRONIC DRAW SECURITY

# Executive Summary

Electronic draw machines are being used by lotteries to optimize the draw process and reduce costs, while opening up the opportunity for new games. Their use, however, has been challenged by recent events involving draw fraud and faults. This is because the security requirements, auditable processes, and certification standards developed by lotteries, gaming authorities and certification agencies - despite their obvious benefits - do not fully protect lotteries against draw system vulnerabilities. These include hardware failures, software defects, and insider fraud - all which are difficult to spot because incorrect or fraudulent numbers may look just like randomly generated outcomes!

The answer to these problems is to shift from traditional preventive security methods to **the ultimate solution - draw nonrepudiation**: proof of the draw outcomes and their origin. With this solution, the draw generation process can be fully transparent through:

- (1) **systemic proof of draw integrity** of the random outcomes and the process that generated them,
  - (2) verification **of the proof on an independent system** by third parties such as auditors or outside entities,
  - (3) detection of faults or fraud **immediately when they occur** and at any later time when needed, and
  - (4) **legal protection** to prove in the court of law that draws were (not) interfered with and were (not) resulting from faulty systems.

Maintaining the status quo is not an option: most draw machines currently in use have limited security features and lack sufficient mechanisms for detecting problems. These traditional systems do not support nonrepudiation of the draw results, leaving them vulnerable to faults and fraud. Now, when the industry is realizing the potential repercussions of draw problems, it is crucial for each lottery to carefully consider the benefits that nonrepudiation offers, as many early adopters have already done.

The full white paper provides information about recent faults and fraud that occurred in the US, opinions from lottery executives about the negative impacts these events could have for the industry, and a non-technical guide to the kind of vulnerabilities that electronic draw systems face, along with a suggested solution.

# Contents

Introduction	4
Section 01: Defining the Case for Nonrepudiation and Draw Integrity	7
Section 02: Vulnerabilities of RNG Systems	12
Section 03: Fraud Perception Amongst Lottery Leaders (Research Focus)	21
Section 04: Critical Elements for RNG Security	25
Section 05: The Szrek RNG Solution - Detecting Faults and Fraud	28
Section 06: Trusted Product Suite	33
Conclusion	39



# Introduction

**S**ecurity in the lottery industry is essential. Players must trust that lotteries provide secure games every step of the way. This is even more important for electronic draws as players do not see the process inherent to the selection of numbers. Electronic draw machines (sometimes called Automated Draw Machines/ADMs, digital draw systems, and Random Number Generators/RNGs) are integral to the lottery industry for many reasons, including that they help streamline the draw process with consequent cost-savings, and they are an important vehicle for launching new games and seizing new markets. Lotteries, Gaming Authorities, and Certification Agencies have defined certification standards for the generation of random numbers, security requirements for protecting electronic draw machines, and auditable processes to ensure draw procedures are correctly implemented.

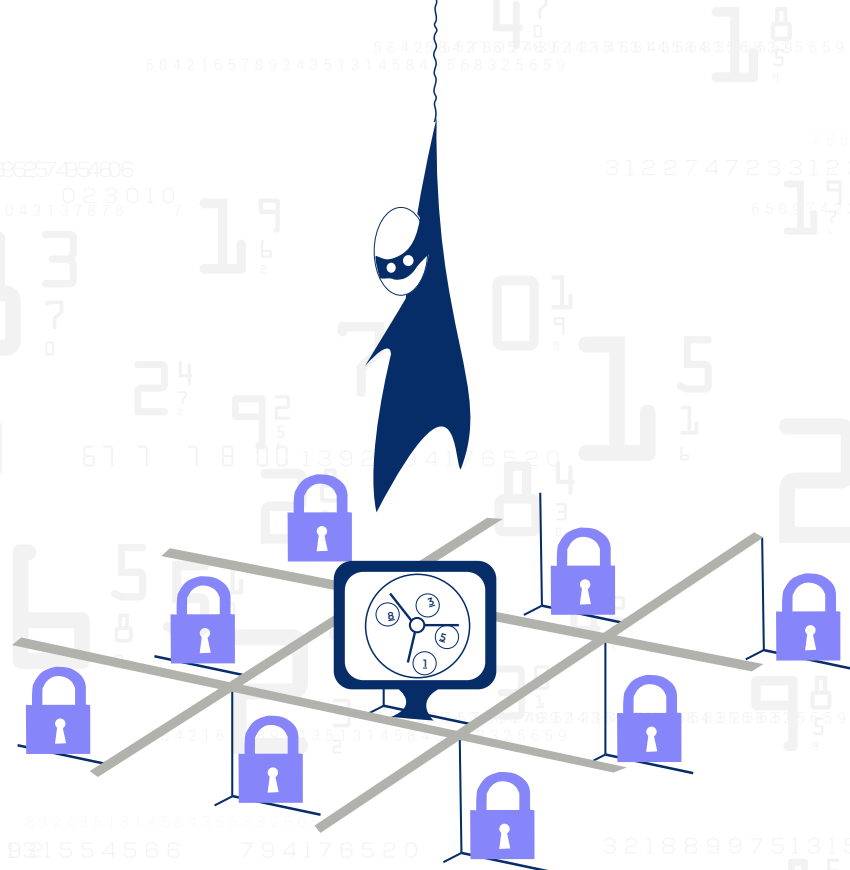
The certification and security standards support a strong rapport between consumers and lotteries. These measures, however, do not fully protect electronic draw machines against hardware defects, software failures, or insider fraud. Many cases of errors or fraud have taken place in the US within the last decade despite the best practices that have been defined and numerous certifications of electronic draw machines by independent labs. The industry keeps being confronted with situations of faulty random numbers due to improper machine setup, hardware malfunctions, software glitches, and fraud. At the core of the problem is the fact that one cannot protect electronic draw machines using only preventive methods, even if these are gold standard. System errors, hardware and software malfunctions, human mistakes, and cases of fraud are inevitable and they generally will not be visible because faulty or fraudulent outcomes may look like randomly generated outcomes! The problem persists because the process for generating random numbers is not transparent.





Section  
**01**

Defining the Case for  
Nonrepudiation and  
Draw Integrity



Traditional RNG  
Vulnerable

## Is there such a thing as a fault or fraud proof lottery draw system?

We believe that equally important to prevention of potential faults and fraud is detection of all draw problems, with irrefutable proof that can hold up in a court of law. Transparency and audit of all aspects of the draw provide proof of the origin and integrity of the generated random numbers.

Most electronic draw systems on the market use the traditional method of random number generation that does not offer full draw transparency. A traditional RNG is secured by restricting access to the electronic draw machine, while protecting it from known threats (see [Vulnerabilities of RNG Systems](#) for more details). The weakness of traditional draw methods is that they rely highly on processes and people, with limited visibility into the system itself: unexpected problems such as a hardware or software errors may not be exposed. Similarly, a concealed break-in into the system may well go unnoticed. Relying on processes, the draw team, lottery, and all other stakeholders need to make a leap of faith – trust that there are no hardware, software, or integrity issues. Sometimes a gross problem will be exposed but other times, the parties assume that there are no problems because they cannot prove otherwise. (See Chains of custody for a pictorial representation.)

In contrast, Szrek offers a solution with nonrepudiation in which electronic draw machine creates unmodifiable data, a Draw Signature, that is independently verified by a second system. This second system, Trusted Audit, detects problems that could otherwise go

If there is a problem that occurs in any part of the draw process and the steps leading up to the draw, the Szrek RNG will detect it. For example, if any of the parties that had contact with the RNG introduced fraudulent software or if there is a change to any data in the computing environment, this will be immediately detected.



Anti-fraud RNG  
Tamperproof

unnoticed. With this model – through nonrepudiation - **Szrek's RNG solution detects 100% of draw faults and fraud.** (See [The Szrek RNG Solution](#) for more detail on the RNG process.) This model is also able to address any customer or stakeholder concerns about a specific draw or all draws. For example, if a rare random event occurs, like a draw of similar or identical numbers on proximate days, the numbers can be checked for integrity. Repetition of identical numbers does happen ([Weiss, 2010](#)), and may even be more likely than we think ([Hand, 2014](#)). It may however cause concern from stakeholders and should be addressed.

There are many cases of draw faults and fraud that could have been avoided and detected if the Szrek RNG systems providing nonrepudiation had been used. These include, recent events like the Tipton fraud case and the Arizona draw game flaw which have left lottery executives' confidence at an all-time low. In a recent scandal (see [Khan, 2017 and Clayworth, 2017](#)), an insider was able to obtain large winnings over several years in multiple states. He was only caught after he collected more than \$2 million in rigged games and carelessly tried to claim a lottery ticket worth over \$14 million. Had the Szrek RNG technology been used, the problem would have been detected the first time a rigged game was played before the winning numbers were announced – when the independent verification failed to confirm the draw numbers. It would have been clear that someone had interfered with the drawing, and the draw would be invalidated. This would have allowed lotteries to catch the perpetrator right away, not permitting for the fraud to continue for several years.





### Traditional RNG - vulnerable

These systems rely on a chain of custody - reliance on the RNG provider, on the certification authority, on the computer's physical security, on the draw procedures, on the personnel, etc. If any point in the chain breaks down, security is compromised but the loss in security may not be visible-making such systems vulnerable to insider fraud and fault

In Arizona, there were two separate recent incidents of draw machine malfunctions, with the same numbers generated for consecutive draws in games played from end-September to October and then again in November ([Coppola, 2017](#); [Marsh, 2017](#)). If the Szrek RNG technology were used, the problem would have been detected **before** the first incorrect draw took place. This would have allowed the lottery to switch to another electronic draw machine, avoid an incorrect draw, and address the problem immediately, instead of unknowingly continuing to use a faulty machine (twice!). The lottery would also have the Draw Signature - the irrefutable proof of integrity that would protect it against any liability cases. As it was, without draw transparency, it required multiple failures for the problem to be noticed. This, in turn, casts needless doubt on the integrity of the lottery and the industry as a whole.

The nonrepudiation of RNGs and draw transparency should be made a requirement for electronic draw machines. Any lack of transparency in any part of the draw opens the industry to vulnerabilities that could easily be avoided, such as these recent events. **Regulators and lottery executives are in a position to protect consumers and build trust by demanding nonrepudiation, verifiable proof of draw outcomes, required for transparency in the draw process.**



### Tamperproof RNG - anti-fraud

The Szrek RNG system has fraud detection in addition to preventive security. Cryptographic hardware and algorithms are used to create proof of integrity (nonrepudiation of draws). The integrity of every draw is verifiable anytime on an independent system. If any link in the chain of custody is broken, it is detected.

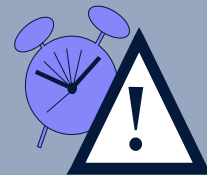




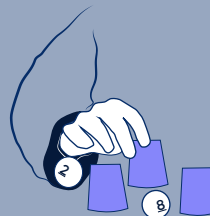
## Section 02

# Vulnerabilities of RNG Systems

Draw time substitution



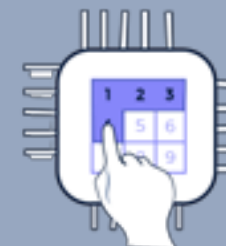
Substitution of numbers drawn



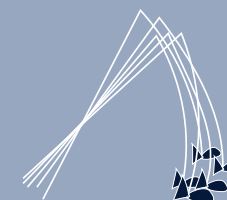
Hardware deterioration



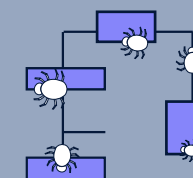
Inadequate RNG design and implementation



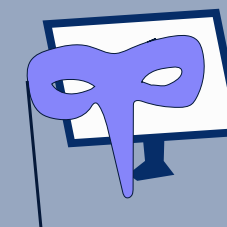
Phishing



Software substitution



Hardware substitution



Traditional RNG security is built around protective security. This type of security has been consistently increasing in most lotteries and RNG vendors have updated their protective security measures. Such measures include background checks of all personnel, the use of only verified vendors, the creation of a secure environment with restricted access, the development of security procedures, role separation for the draw staff, digital signing of draw reports, certification, and code review, etc. In addition, in

some locations – including in most US states – RNG machines are designed to be on an isolated system that is not connected to a gaming system. However, even when the RNG is isolated it can be vulnerable to insider attacks, and insider attacks make up the large majority of security breaches across most industries ([Kroll, 2015](#)). We refer to traditional RNGs as RNGs that have protective security, as described above, and limited detection capabilities. We note that not all traditional RNGs are alike, and there may be additional security measures used to enhance security. However, unless the RNG system offers all-encompassing fault and fraud detection ensured by nonrepudiation, the RNG system will be vulnerable to obscure faults and insider fraud that can go undetected. The following are known vulnerabilities of the RNG system that we have identified:

# Vulnerabilities of RNG Systems



**01 Software substitution:** Fraudulent software is substituted on the certified RNG for a specific draw or draws. We are currently aware of two such methods of attack, (i) a hidden code or a dynamic link library (dll) can be installed on the RNG system at the time when the original code is installed or at a later time, and may be triggered by a specific date or event, (ii) a self-destructive root-kit can be installed on the RNG system at the time of original installation or afterwards, e.g. during system maintenance. In all cases, such software may be very difficult or even impossible to detect because it can be hidden, encrypted, self-destructive, and because it may only run at a specific time. Methods such as certification

may not detect such hidden code because it runs only at certain times or is dependent on other conditional factors related to number generation. Pre and post-testing of draws will not detect the hidden code because such tests focus on analyzing statistical distributions. Verification of program checksums may fail because a different program may be running than the checksummed one or because a verification tool may be corrupt. Scanning of the system may not identify such falsified code - it is very difficult to find something suspicious in a vast amount of code unless looking for a specific code or type of attack. Verification tests cannot find hidden code because they can only test for known problems and cannot predetermine all potential vectors of attack.


For example, in the insider fraud case mentioned earlier, a developer of the RNG system (Eddie Tipton) embedded a fraudulent software allowing him to manipulate draw outcomes. Tipton later became the Information Security Director for the Multi-State Lottery Association and his fraudulent software was only detected after many years. The fraudulent RNG was used for draws in at least 6 games played across 5 states. Tipton was caught due to the suspicious way in which he claimed a high prize and only during later investigations was the fraudulent software discovered when the type of attack was largely characterized (Clayworth, 2017; Khan, 2017). Tipton's attack was not very sophisticated; however, it was very effective against a traditional RNG system whose protections are preventive in nature. In an RNG system with conclusive integrity problems' detection, the fraud would have never succeeded, let alone continue for many years. RNG systems providing nonrepudiation of the draw numbers and verification of proof of integrity will ensure transparency for all parts of the draw: these systems will not allow attackers to implant or hide their fraudulent software.



**02 Hardware deterioration:** RNG Hardware may deteriorate over time, causing the RNG to malfunction and potentially lose its randomness property. Faulty hardware may still generate numbers without providing an external indication of hardware deterioration. Such a malfunction can also be fraudulently instigated by an attacker who substitutes RNG hardware to obtain predictable winning outcomes.


The recent Arizona cases (Coppola, 2017; Marsh, 2017) are still being investigated, so the exact cause is not yet known, but it appears that the draw of identical numbers was caused by a system malfunction due to hardware deterioration. A similar problem occurred in Kansas in December of 2005, when the numbers 5-0-9 were selected on three consecutive days (Lottery glitch draws same Pick 3 numbers, 2005).

This type of problem is avoided by RNG systems that verify the integrity of the RNG seed during the draw. The Szrek system verifies hardware before proceeding with a draw. Should the verification fail due to a faulty HSM, the TD360 system automatically switches to use another Hardware Security Module (HSM). If both fail, the machine will not generate draw results and the Lottery is alerted to use a different draw machine or to correct the problem. Please note that signature verification is not a hardware status check but a hardware functionality verification. (See The Szrek RNG Solution for more information on the HSM.)




**Draw time substitution** after the results are generated

The timestamp for offline draws can be altered, meaning draw results can be known before they are published.




**Substitution of numbers** drawn after the results are generated

An insider can substitute the winning numbers and this can go unnoticed if the RNG system does not provide verification methods and the results are not consistently verified.



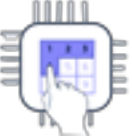
**Phishing** attempting multiple RNG generations to obtain desired outcomes

Traditional RNGs allow for multiple generations and it may be impossible to know how many have occurred.




**Hardware deterioration** results in hardware not performing RNG functions safely or properly

Traditional RNGs may not have specific hardware verification tests in place.




**Defensive software design** detection of software and hardware errors and malfunctions

Software designed to check for errors, detect hardware issues and malfunctions



**Hardware substitution** alternative hardware that produces predictable results

Such substitution may go unnoticed unless there is a way to identify the hardware used for each draw predictable results.

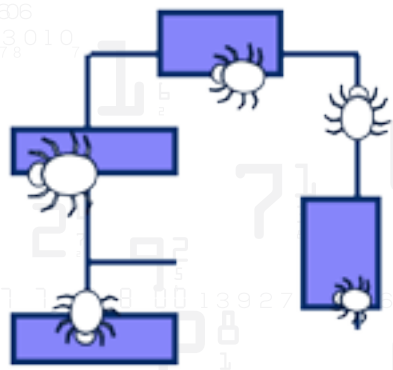


**Software substitution** during initial delivery, during maintenance, or USB later.

Certification, pre-post testing, verification of program checksums, system scans, verification tests, and post-mortem testing may not find the hidden code.

Figure: RNG System Vulnerabilities





**03 Hardware substitution:** RNG hardware can be substituted with a fraudulent hardware to obtain predictable winning outcomes for a specific draw. Unless there is a way to identify which hardware was used, the substitution of hardware can go unnoticed. This is a very similar case to 2, except that in this case hardware is substituted by an attacker.

This type of problem is detected by RNG systems that use background cycling, that verify the integrity of the RNG seed during the draw, or that provide nonrepudiation and proof of integrity.



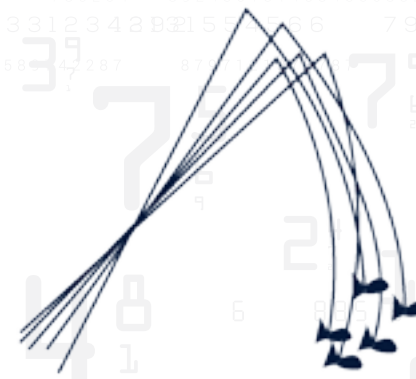
**04 Substitution of numbers drawn:** It may be that the numbers are simply replaced with other numbers if the RNG system does not provide verification methods. Herb Delehanty, consultant, refers to this as the “Low tech paper shuffle” in which the draw results are on a sheet

of paper which is simply replaced. This constitutes one example of substitution. Another example would be printing of the wrong data, possibly intentionally via a wifi connected printer. Delehanty (2017) argues that this is the easiest scam ever to implement and he suggests video and audio monitoring to help avoid this. Video and audio monitoring will help but problems may be missed. A solution that detects what happens inside the system – one that provides proof of integrity – is the gold standard.



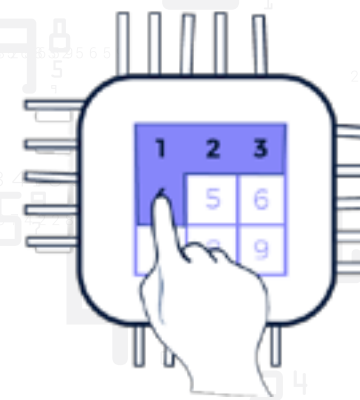
**05 Draw time substitution:** In an offline or isolated system, the system time cannot be continuously verified. This means that the time of a draw could be altered after the draw results are known by an insider.

To detect time related fraud, draw nonrepudiation must include proof of the draw time. Verification of draw integrity will then confirm the actual draw time. Manipulation of draw time is protected by the HSM’s Real Time Clock. (See [The Szrek RNG Solution](#) for more information on the HSM.) The Szrek RNG includes draw time in the Draw Signature which ensures detection of time related errors or attacks.



**06 Phishing:** A traditional RNG, and in particular an offline system, may allow for multiple generations of draw results. This would allow an insider to continue phishing or searching for combinations until a desired draw result is found. This desired draw result could then be published as the proper draw outcome.

Draw nonrepudiation must account for every random number generated. When draw integrity is independently verified, non-verified draws are detected providing proof of phishing.



**07 Inadequate RNG design and implementation:** There are multiple design and implementation issues that can make a RNG vulnerable including:

(i) the RNG algorithm may not be cryptographically strong – RNG certification by an independent party should include algorithm analysis and verification. There are many examples in which casinos have fallen victim to cheaters who have figured out how to beat the odds ([Allison, 2017](#); [Koerner, 2017](#)). Allison (2017),

founder of the World Game Protection Conference, argues that the lack of security and integrity in RNGs is far too common. The standards that Gaming Labs International (GLI) introduced in September 2016 ([GLI, 2016](#)) help to provide minimum standards for those that decide to comply, including cryptographic strength. The Illinois Gaming Commission is the first gaming board of which we are aware that is requiring adherence to these standards.

(ii) draw system software may not have built-in checks for hardware deterioration or malfunctions. Ideally, systems should perform hardware checks before every draw. When hardware malfunctions occur the device may lose its randomness property as described above (point 2).

(iii) software errors or “bugs” may be present and configuration errors may exist. When draw systems are tested in a mode similar to live systems this may help identify problems. Certification should also be adequate and repeated when RNG software is altered. Suitable testing and certification should have avoided problems in Arizona in 2013 when the RNG did not allow for 8s and 9s to be selected ([Computer glitch Arizona pick 3, 2013](#)), in Tennessee in 2007 when there were no duplicates amongst winning numbers (ex. 1, 2, 2) ([Tennessee Lottery reveals problems with drawings, 2007](#)), and similarly in California in 2005 when there were no duplicates for the Lottery’s Derby ([Vogel, 2005](#)).



## Why RNG with cryptographic integrity verification

To immediately detect fraudulent intrusion to your RNG. Skilled insiders can fix the draw results. You need to detect any fraudulent activity and act on it immediately, to prevent RNG fraud. (*Clayworth, 2017; Pereira, 2016a*)

To verify and demonstrate the integrity of each and every draw.

Circumstantial evidence may be insufficient to detect fraud. And because all results are possible, you may need to prove the legitimacy of questionable draws e.g. identical draws on proximate days. (*Weiss, 2010*)

To avoid using faulty hardware for electronic draws.

Defective hardware can lead to non-random and repetitive draws. (*Pereira, 2016b*)

To guarantee 100% fraud detection and serve as a fraud deterrent.

A person will only commit a crime if they perceive that they have a good chance of success; detection works as a fraud deterrent. (*Becker, 1974*)

To provide admissible proof of fraud in litigation.

Our random numbers are generated using digital signatures, which in many countries constitute legal evidence. (*American Bar Association, 1996*)

We estimate that over the last 13 years (from 2005 to 2017) electronic draw fraud has occurred in games played across 13 states. An additional three have been victims of other problems that have affected the integrity of the winning numbers. If all 50 states used electronic draw systems, this would put the probability of electronic draw problems at 32%. This underestimates the amount of problems, because some states do not take part in electronic draws, and even more importantly we can only report faults or fraud that have been discovered and reported. Mechanical machines also have a history of fraud, with the most famous scandal being in Pennsylvania in 1980 when the daily numbers announcer swapped the original balls with weighted replicas in order to produce controlled outcomes ([1980 Pennsylvania Lottery scandal, 2017](#)).

The problems that have occurred in the most recent years raise a number of questions that we address in the rest of this paper. These include technical questions about how to prevent and/or detect such problems as well as questions about how such problems could affect the lottery industry as a whole. We begin by discussing some of the research we have conducted about fraud perception in the industry.





We are stressing that it is simply not enough to focus on randomness and protective security alone. We have the ability to mathematically prove the authenticity of the random results bringing the overall integrity and transparency of the electronic draw to a new level.



*Walter Szrek, Founding Partner and Chief Technologist*

Section

03

Fraud perception  
amongst lottery leaders  
(Research Focus)

## Study 1: Perceptions of the costs of fraud

At a Public Gaming conference in May 2016, we approached top-level lottery management to obtain their perceptions of fraud in the lottery industry (see Table 1). The survey results suggest that fraud would be damaging to lotteries by reducing their customers, restricting lottery's freedoms to introduce new products, and through imposing large monetary costs on lotteries in the short and medium-run. The average estimates of fraud cost to their lottery provided by lottery leaders was \$283 Million, for the first year, and \$1.31 Billion, for years 2 to 5 after the fraud occurred. The survey did not take into account other potential impact such as increased financial risk of liability through class action, so the numbers may be understated. These numbers are also based on a survey rather than actual costs that were measured, so they are only suggestive, however they highlight that lottery management believe fraud could severely affect their institutions in many ways. To avoid this impact, the best safety and security procedures should be introduced to protect lottery systems and particularly electronic draw systems.

### Lottery Fraud Survey Results

In a survey of 9 lottery directors, 2 former directors, 1 CFO, 1 COO, and 6 other top level management (n=19):

- On average, respondents thought that over half of their customers may stop purchasing lottery tickets or buy fewer tickets if they discovered that lottery fraud had been committed in that state.
- Lottery's legislative and regulatory powers, including the lotteries ability to develop new games, would be impacted by the discovery of lottery fraud - 95% agreed.
- The total short-run costs estimated were, on average, \$283 Million for the first year in which lottery fraud was detected. Total costs include reputational costs, legal fees, political costs, losses in ticket sales, etc.
- The total medium-run costs estimated were, on average, 1.31 Billion for the first 5 years in which lottery fraud was detected. Total costs include reputational costs, legal fees, political costs, losses in ticket sales, etc.

## Study 2: Perceptions of RNG fraud vulnerability and responsibility

We asked respondents to give us their view on the impact of another lottery fraud on the industry, if it occurred. There were 56 respondents in total, 27 of which were from lotteries (including 15 lottery directors), 12 from vendors that sell gaming systems, and 17 from other vendors (consultants, audit, etc.). To test the hypothesis that this impact was independent of the size of the fraud, we asked about RNG fraud involving larger (greater than \$1 million) and smaller (less than \$500) amounts of money. We also asked respondents how much an RNG fraud discovered in one lottery would negatively affect other lotteries. Finally, we asked respondents to identify the different entities that should be held responsible for lottery fraud.

Table 1

### Mean response survey questions

FULL SAMPLE (N=56)

Variable	Mean	Std. Dev.
How bad would another RNG fraud incident be to the lottery industry if the fraud involved a <b>LARGE</b> amount of money (ex.v over \$1million), where 0 is that it would have no effect at all and 10 is that it would be utterly devastating to the industry.	7.77	1.82
How bad would another RNG fraud incident be to the lottery industry if the fraud involved a <b>SMALL</b> amount of money (ex. less than \$500), where 0 is that it would have no effect at all and 10 is that it would be utterly devastating to the industry.	4.84	2.81
How much do you think a fraud incident in one lottery would negatively affect other lotteries, where 0 is that the fraud would only affect the lottery in which the fraud was discovered and 10 is that the fraud would affect all lotteries in the industry?	5.93	2.55
Who is responsible for preventing RNG fraud?		
Lotteries	1.00	0.00
Vendors of Gaming Systems	0.73	0.45
RNG suppliers	0.79	0.41
Certification authority	0.63	0.49
AUDIT/ICS provider	0.48	0.50
Legislature/Govt	0.30	0.46
Regulator	0.41	0.50

Table 2

Respondents expected a RNG fraud of 1 million dollars to be a 7.8 on a scale of 0 (no impact on the industry) to 10 (complete shutdown of the industry), with 84.5% of responses a 7 or above and all but one response above 4. However, when the dollar amount was \$500, the mean response dropped to 4.84. Although, 27% of respondents showed no change in their response when the dollar amount dropped, 23% of respondents showed a drop in 4 points or more. Respondents informally described their answers in terms of how the dollar amount would affect the interest of the story to the press. In terms of how a fraud in one lottery would affect other lotteries, respondents on average thought this would have an effect of 5.93, on a scale where 0 is that the fraud would only affect the lottery in which the fraud was discovered and 10

is that the fraud would affect all lotteries in the industry. Fifty-five percent thought the effect would be between 3 and 6 and 39 % of respondents thought that the effect would be 7 or above. See Table 2 for Respondents always held lotteries responsible for RNG fraud, while the other entities were held responsible by some but not all respondents, Vendors of Gaming Systems (73%), RNG suppliers (79%), Certification authorities (63%), AUDIT/ICS providers (48%), Legislature/Government (30%), and Regulators (41%). Respondents generally had different reactions to this question; some believed in one entity (lotteries) having sole responsibility while others considered RNG fraud to be an issue whose responsibility should be shared across the different entities.

See Pereira (2016a) and Pereira (2016b) for more detail on these studies.



## Section

# 04

## Critical Elements for RNG Security

In an industry that relies on people buying tickets to fulfil a dream, consumer trust is paramount. Problems with incorrect, non-random draw results can undermine that trust. We begin by explaining some **misconceptions** about draw security and then outline important security measures for electronic draw systems that should be adopted by lotteries.

### SECURITY MISCONCEPTIONS

#### MISCONCEPTION 1:

#### **Mechanical drawing machines are more secure.**

Since it is often perceived by the public that electronic draw systems can be easily manipulated, one approach would be to return to mechanical draw machines. However, when the security measures and draw transparency are correctly implemented, an electronic draw system provides better control and protection for the gaming environment than a mechanical system, making the electronic draw system also more secure than a mechanical system. Additionally, electronic draw systems offer more capabilities, such as the support for more types of games, the ability to have more frequent draws, and the capability to manage draw outcomes. Such systems are also much less costly because the draws for all games can be handled by one system, versus a separate machine for each game, and require much less human involvement to manage them. Last, but certainly not the least, electronic draws can yield an undeniable proof of integrity, while mechanical draws cannot.

#### MISCONCEPTION 2:

#### **Electronic draw systems are most secure when they are isolated from other systems or networks and protected using physical measures.**

Isolating draw systems does not protect from insider attacks, as demonstrated by the recently discovered fraud cases. Additionally, committing to stand-alone offline draw systems introduces limitations on draw capabilities, and thus may limit lottery growth. Isolated draw systems require more human effort and thus yield higher operational costs. Humans fulfill the need for completing manual procedures; they are more prone to error than automated ways of communicating data. Properly implemented security measures that include nonrepudiation of draws and verification of the integrity using the independent audit and verification system provide more security than isolated drawing systems.



# NECESSARY RNG SECURITY MEASURES

To provide some guidance, we identify a checklist of critical security measures which help protect the integrity of the RNG.

Elements (1) - (5) improve on traditional methods of assuring integrity and establish best practices provided by third-party vendors. Fraud detection and audit on an independent system - (6) and (7) - rely on nonrepudiation to provide proof of the actual draw numbers, for greatly enhanced security and assurance of integrity.

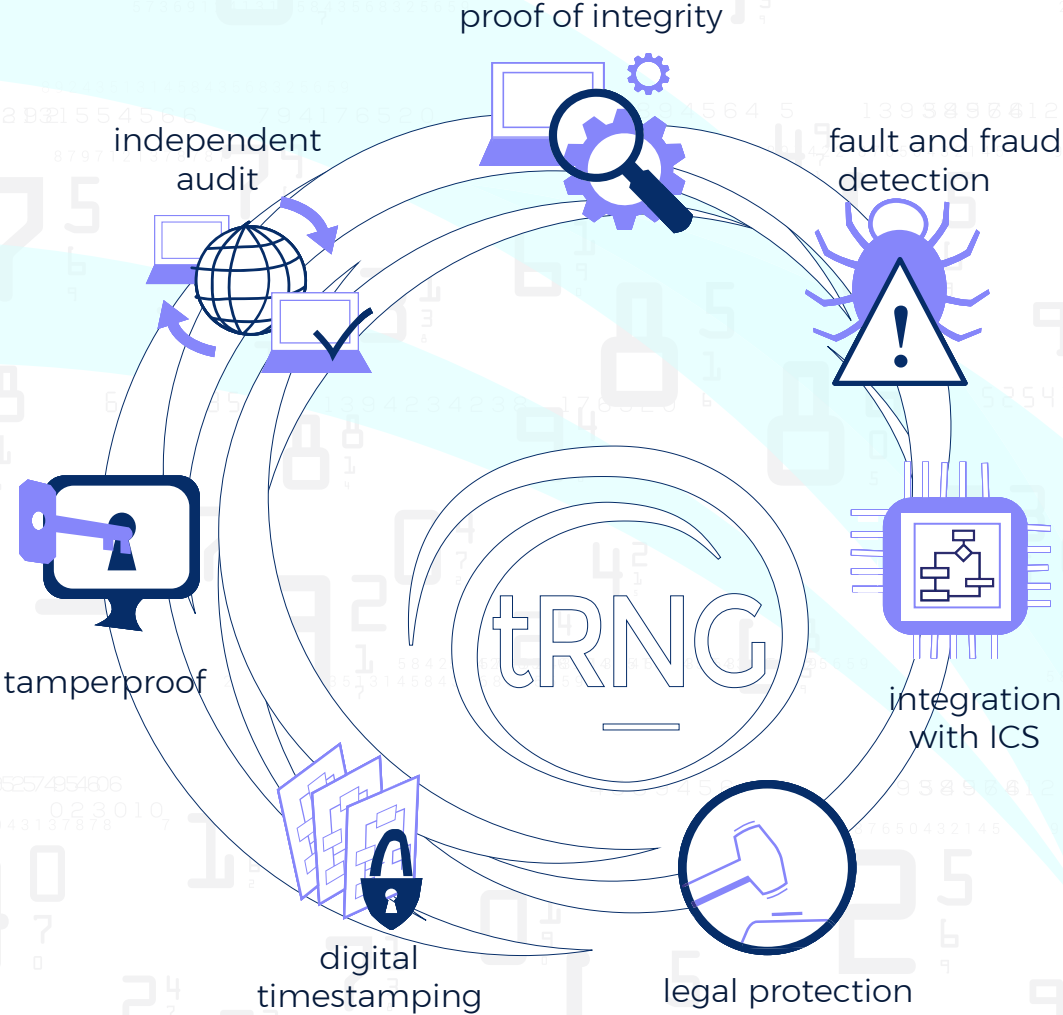
**(1) Independent third party provision:** Draw systems should be provided by an independent third party. To avoid potential conflict of interest, separation of functions is crucial. Hence, (a) lotteries should not develop their own draw systems and (b) lottery gaming systems vendors should not provide their own draw systems.

**(2) Protective security:** Security of the RNG must include state-of-the-art protective security which should include: strong password protection, restrictions on access, and read-only use of the RNG program, configurations, and reports. Also, lotteries should set procedures to restrict user access and define role separation, including users from different groups or organizations to perform draw, audit and other functions. Audit logs should be created to allow the review of system activity. Periodical review of these logs should be done.

**(3) Certification:** Independent certification of randomness and code review is necessary. Certification should include verification that RNG is well designed: no patterns of outcomes and that the RNG is cryptographically strong, the knowledge to the RNG software and previously generated random numbers will not allow to predict next outcomes. As we have seen this certification does not protect against a hidden code nor it prevents injection of fraudulent code in the future.

**(4) Verification of checksums:** Another important method requires verification of checksums or hashes of RNG software code, to detect any changes in the software code or configuration since system certification. This verification may be circumvented by a fraudulent software.

**(5) Security certification:** In addition to random number certifications, security certifications can be performed to increase confidence in the draw system. These certifications may include scanning of the draw system delivered to the lottery to detect malicious code and system vulnerabilities. A system snapshot can be taken at the time of delivery and used later for comparison to detect unauthorized changes.



**(6) Fraud-detection:** The RNG includes fraud-detection capabilities: each time a draw occurs, the system creates a *tamperproof* log file corresponding to the draw; if any changes are made to the log file, an independent audit would identify these changes. By building a tamperproof log file, the draw provides non-refutable undeniable proof of draw integrity. To clarify the principle of audit logs and integrity auditing:

- a. If log files are not tamperproof, fraud-detection is not certain.
- b. A tamperproof electronic log file is distinct from activity log and draw reports; computerized attacks may be 'invisible' and they may create fraudulent logs.
- c. Proof of integrity of a draw system should not require sharing of privileged or secret information, as this can involve potential collusion and fraud.
- d. Digitally signing already generated data does not provide undeniable proof, as the data may have already been modified when signed. In fact, draw reports generated in the recently publicized RNG fraud case were digitally signed.

**(7) Audit on an Independent System:** A draw system should provide nonrepudiation and should allow independent verification of draw integrity on a different system. This second system must be independent from the number generation process, so that it can detect any fraud to the potentially manipulated draw system.

- a. The independent system should be able to analyze tamperproof logs (7) to prove the integrity of *each individual draw*, its time and numbers drawn.
- b. Forensic audit methods rely on scanning of hard drives. Audit should **not** rely solely on scanning of draw systems as these procedures are expensive and are not fully reliable: some evidence will not be recoverable through scans. A skilled programmer will not leave traces of attack or make them extremely difficult to find.



Section

05

## The Szrek RNG Solution - Detecting Faults and Fraud

**Szrek's RNG provides nonrepudiation of the draw outcomes, with proof of integrity, which differentiates it from other methods.**

Currently, RNG systems on the market use the traditional method of random number generation and do not offer full draw transparency. In addition, they do not provide draw nonrepudiation, thus problems may exist that cannot be seen externally. The traditional process of random number generation does not create proof of integrity that could be verified on an independent system. By contrast, **Szrek's RNG solution detects 100% of draw faults and fraud**, every time, every step of the way.

**Szrek's patented RNG method detects software and hardware malfunctions, integrity problems and fraud, and provides a fully transparent draw. In addition to the TD360 draw system, Szrek offers its Trusted Audit system, which verifies the integrity of every draw. With Szrek's RNG system, the lottery can be confident in its draw results, and it can also easily verify draws and address any inquiries about draw integrity.**

Even though the random numbers are unpredictable, and all outcomes are possible before the generation, once generated, specific numbers can be proven as the only valid selections. Ultimate draw integrity verification is performed after the draw by Trusted Audit, which enables for full transparency of the draw process. For example, if for lotto 6 of 49 numbers 7, 9, 11, 23, 25, 37 are generated by TD360, Trusted Audit will mathematically verify the numbers and confirm that the numbers are valid, or it will detect and report a discrepancy. Furthermore, integrity verification can be done by a third party, such as internal auditing departments, external auditing entities or even regulators, increasing the transparency of the whole process for the stakeholders.

# How does the Szrek RNG solution work?

## Overview

The Szrek RNG is a software and hardware based solution. The Szrek RNG achieves nonrepudiation by using a Cryptographic Digital Signature as the Seed for the RNG. The RNG seed is generated by a tamperproof hardware device – a Hardware Security Module (HSM) -that is NIST certified. An important property of the digital signature is that it is unpredictable yet it can be verified by a standard algorithm. In Szrek’s solution, this signature is verified with a different set of software on an independent system. This signature verification detects fraud, faults, or any other problems.

## Random Number Generation Process




























The process of generation in its initial step verifies if the RNG hardware device generates a correct RNG seed and proceeds with a draw only if there is no device error; otherwise, it switches to a second device. During a subsequent step, the verified RNG seed, which is in the form of a digital signature, is saved as a Draw Signature. The record is written to a tamper-proof draw Signature File that is transferred to the Trusted Audit system, manually or automatically. Because the draw Signature File cannot be altered or manipulated, it provides reliable information to identify any malfunction of the hardware or software, a configuration error, or any type of fraud and serves as proof of draw integrity.

## Ultimate Draw Integrity Verification

The Trusted Audit system reads the Signature File and for each draw (1) verifies the RNG seed (digital signature) and (2) recreates the draw results. Comparison of the draw results generated on the Audit and RNG systems will detect any kind of problem: an incorrect configuration on the RNG system, CPU or memory errors on the RNG system that would affect RNG outcomes, and any type of integrity issues including manipulation of the draw results, etc.

If there are suspicions of draw problems or a need to check on draw integrity for historical draws, these can be easily verified on the Trusted Audit system by processing Signature Files for these draws. This is in contrast with traditional draw systems, where you cannot be sure if there have been any problems that have gone unnoticed.

## Security and Integrity

	 Traditional RNG	 Anti-fraud RNG
 Reliance on standard algorithms and public information, no privileged secret information	 	
 Remote access and monitoring of draws without compromising security	 	
 Can be integrated with Internal Control Systems	 	
 Defensive software design - detection of software and hardware errors and malfunctions	 	
 Tamper-proof hardware and software		
 Nonrepudiation of draw - proof of integrity can be verified anytime on an independent system		
 100% Fault and Fraud detection, including all insider attacks		

## Result

The draw generation process is transparent and enables verification of the numbers drawn on an independent system that can be performed by independent third parties such as internal auditing departments or outside entities. The verification can take place at the very time of the draw, just after the draw, or at any other later time. If there is any problem with the random number generation process, this problem will always be detected. The Draw Signature existing in the form of a digital signature can also serve as legal protection.

Nonrepudiation of the winning draw outcomes generated by Szrek RNG needs to be distinguished from other methods that do not provide proof of integrity. For example, digitally signing already generated draw numbers does not provide nonrepudiation and is not effective because the numbers drawn could have been defrauded prior to being signed or could have been generated by a malfunctioning system. Similarly, using the digital signature as the RNG seed will provide nonrepudiation only if digital signatures and the signing keys (private keys) are protected by a certified and secure Hardware Security Module.





Section

06

## The Trusted Product Suite

Szrek offers its **Trusted Product Suite™**, which is an integrated platform of secure lottery products powered by tRNG. The suite includes Trusted **Audit**, Trusted **Draw**, Trusted **Play**, Trusted **Ticket**, Trusted **Transaction**, and Trusted **Monitor**.



## tRNG

The RNG platform provides a common infrastructure and tools for the integrated functionality of all Trusted Products. The RNG platform is based on Szrek2Solutions patented technology that ensures the nonrepudiation of random numbers: the irrefutable proof of integrity that can be verified anytime. RNG platform supports a range of systems from simple standalone systems to complex online configurations with backup systems and backup sites. The platform accommodates growth, allows for the seamless introduction of new games and features, and supports the most demanding interactive environments.



## trusted audit™

Trusted Audit provides integrity verification and audit for all Trusted Products. It performs mathematical verification, which detects data corruption or manipulation. Trusted Audit supports manual and fully automated verification. It ensures that all data is verified, in near real time or at the end of business day, so that any discrepancies due to errors or fraud are detected and reported. It can audit over 10,000 random numbers per second. Trusted Audit works independently or it can be integrated with the lottery ICS system.

The patented method allows for auditing the individual random numbers and associated game data. Even though the random numbers are unpredictable, and all outcomes are possible before the generation, once generated it can be proven that specific numbers are the only valid selections.

Along with the random numbers the associated game data is verified by the Trusted Audit system, which for instant win games confirms that a specific prize belongs to a specific player and for draw games verifies that the bets were not changed after the draw.





### trusted draw™

Trusted Draw is a reliable electronic draw system with built in fraud detection. It replaces and/or augments mechanical drawing machines or replaces a traditional RNG with a more secure system. Trusted Draw supports all game types and works stand-alone or connected to a gaming system, providing a high degree of automation. When integrated with Trusted Audit, the draw system offers exceptional security with full proof of integrity/ 100% fraud detection.

Since 2005, Trusted Draw has been certified numerous times for games including traditional lotto, numbers, raffle, raffle from file, and 2nd chance games with variable odds. Various configurations of Trusted Draw systems are provided to support different lotteries' needs. Drawings can be held locally, offline, directly on a draw machine, or remotely, with draw manager and auditor in the same or different locations; online drawings can be invoked directly from the gaming system or manually by the draw manager. A single Trusted Draw system can support many different games and draws for multiple jurisdictions, with ease of adding a new game or game change.

Trusted Draw has many important features that help to streamline the whole draw process, making the draw easy and reducing errors. Multi-media animations can be created from the draw results and immediately shared with television or social media.



### trusted play™

Trusted Play is a reliable high performance RNG for instant and interactive game outcomes with built-in fraud detection. Typical applications include on-line real time betting on the internet and through mobile platforms, interactive TV betting, Video Lottery, casino betting, and on-line lottery. When integrated with trusted audit, the RNG system ensures transparency and functions in a fully automated manner, processing over 2,000 generations per second.

Various Trusted Play generation methods were certified, such as instant win games with depleting or non-depleting pools of outcomes (class 2 and class 3 games), session based games, such as card games, etc. A single Trusted Play system can support many instant and interactive game types as well as multiple jurisdictions. Trusted Play can be deployed in primary and backup data centers, with one or more Trusted Audit systems, and optionally with the Trusted Monitor™ system. There is also a Trusted Play+ system available, which merges Trusted Draw and Trusted Play functionality on a common platform.



### trusted ticket™

Trusted Ticket server secures paper and electronic tickets and provides authentication of lottery tickets in various gaming environments and at different Points of Access (POA), including tickets printed on 3rd party lottery terminals, in-lane cash registers, POS, or electronic tickets on mobile phones. Ticket authenticity is verified independently by trusted audit to endorse prize payment. Trusted Ticket does not require specialized software in POAs.



### trusted monitor™

Trusted Monitor product provides remote real-time monitoring of Trusted Draw, Trusted Play, Trusted Audit, Trusted Transaction, and Trusted Ticket systems for operators and third parties. While all Trusted products run in the protected environment provided by the secure data center, Trusted Monitor offers secure remote browser access from outside this protected environment. Trusted Monitor is a passive monitoring system – the user cannot change anything on any of the Trusted Product Suite Systems. Each Trusted Monitor system can communicate with many Trusted Product Suite Systems and environments.



### trusted transaction™

Trusted Transaction server is offered to secure transactions by digitally time-stamping transactions in real-time. Such a solution is especially useful to secure bets before the (electronic or mechanical) draw. Time-stamping creates a proof of data content that can be verified any time. Digital time-stamping constitutes legal proof of content and guarantees detection of data corruption or manipulation. Some lotteries (e.g. German Lotteries, Israeli Lotteries) require that lottery transactions are digitally time-stamped to prove that they were not modified after the draw. Such digital time-stamping also meets the requirements of MUSL's Rule #2 in the United States. Trusted Transaction would also meet the performance requirements of the biggest lotteries during lotto mania.

## Customers, Partners, and Certifications

Since 2005 our customers have used our products to generate random numbers for their draws and instant games and to prove the integrity of all drawings. Customers from the United States have included IGT, Iowa Lottery, Oregon Lottery, Texas Lottery, Kentucky Lottery, Georgia Lottery, and Rhode Island Lottery, amongst others. Our customers outside the United States have included IGT, Scientific Games Gmbh, Danske Spil S/A, Lottomatica, Sisal S.p.A., Ithuba Holdings (South African National Lottery), Loterie Nationale (Luxembourg Lottery), and ONCE (National Organization of Spanish Blind People), amongst others.

These products have been certified for numerous games on four continents by GLI, Eclipse Testing, TST, SeNet International Corporation, Delehanty & Associates, eCOGRA, Copenhagen University, Sapienza University, Milan University, and FORTE Technology.

We have integrated our products with the following gaming providers: IGT, Scientific Games Gmbh, Novomatic, Gioco Digitale.

Our partners include IGT, Novomatic, Scientific Games Gmbh, Spectra, Spyrus, and Winsystems.



## Conclusion

We provide guidelines to identify a secure solution for electronic draws. Currently, there are two complementary ways of addressing the threats of faults and fraud: first, by increasing preventive measures; and, second, through robust proof of the integrity of draws that can be independently audited. Preventive measures can be systematically incorporated into processes and best practices so that the likelihood of mistakes, malfunctions or manipulations is reduced. Their limitation is that they can only address known vulnerabilities and hence are insufficient. Second, through non-repudiation, lotteries can unequivocally demonstrate the validity of each and every draw, can detect faults or fraud when they occur, and can prosecute offenders. Furthermore, by eliminating the benefits of engaging in such crime, this solution will work as a fraud deterrent.

Szrek provides a methodology for RNG that offers nonrepudiation, allowing lotteries to prove the integrity of all electronic draws. This proof can then be provided to all stakeholders whenever required – allowing for a level of security that surpasses other electronic drawing systems and even mechanical drawing machines. The nonrepudiation offered by the Szrek solution has positive externalities for the industry as well, by helping to avoid draw problems such as those involving faults and fraud. **Regulators and lottery executives should address draw fraud and faults by demanding nonrepudiation, the verifiable proof of draw outcomes, thereby protecting consumers and building trust with all stakeholders.**



References:

1980 Pennsylvania Lottery scandal. (2017, July 7). In *Wikipedia*, The Free Encyclopedia. Retrieved from [https://en.wikipedia.org/w/index.php?title=1980\\_Pennsylvania\\_Lottery\\_scandal&oldid=789475149](https://en.wikipedia.org/w/index.php?title=1980_Pennsylvania_Lottery_scandal&oldid=789475149).

Allison, Willy. (2017, January 20). Security and Surveillance: Running the RNG Risk. *Global Gaming Business Magazine*. Retrieved from <https://ggbmagazine.com/article/security-surveillance-running-the-rng-risk/>.

American Bar Association. (1996). Digital Signature Guidelines. *Information Security Committee*, Section of Science & Technology Report. Retrieved from [https://www.americanbar.org/content/dam/aba/events/science\\_technology/2013/dsg\\_tutorial.authcheckdam.pdf](https://www.americanbar.org/content/dam/aba/events/science_technology/2013/dsg_tutorial.authcheckdam.pdf).

Becker, Gary S. (1974). Crime and Punishment: An Economic Approach. *National Bureau of Economic Research*. Working Paper 3625. Retrieved from <http://www.nber.org/chapters/c3625.pdf>.

Clayworth, Jason. (2017, August 22). ‘I certainly regret’ rigging Iowa Lottery, says cheat who gets 25 years. *Des Moines Register*. Retrieved from <https://www.desmoinesregister.com/story/news/investigations/2017/08/22/iowa-lottery-cheat-sentenced-25-years/566642001/>.

Computer glitch leads Arizona Lottery to issue new Pick 3 tickets (2013, August 17). *Azfamily*. Retrieved from <http://www.azfamily.com/story/23160723/arizona-lottery-issuing-some-pick-3-replacement-tickets>.

Coppola, Chris. (2017, October 5). Arizona Lottery glitch produces same numbers in multiple drawings. *Azcentral*. Retrieved from <https://www.azcentral.com/story/news/local/phoenix-breaking/2017/10/05/glitch-spits-out-identical-lottery-numbers-multiple-games-over-multiple-days-arizona/738075001/>.

Delehanty, Herb. (2017, July 27). Random Number Generators. *NASPL Professional Development Seminars*, Oral Presentation, Nashville, TN.

Gaming Laboratories International (2016). GLI-11: Gaming Devices. *Technical Report*. Retrieved from <https://www.gaminglabs.com/pdfs/GLI-11%20Gaming%20Devices%20V3.0.pdf>.

Hand, David. (2014, February 1). Math Explains Likely Long Shots, Miracles and Winning the Lottery. *Scientific American*. Retrieved from <https://www.scientificamerican.com/article/math-explains-likely-long-shots-miracles-and-winning-the-lottery/>.

Khan, Roomy. (2017, August 31). The DNC IT Scandal And The Jackpot Lottery Fraud: When Digital Gatekeepers Become Thieves. *Forbes*. Retrieved from <https://www.forbes.com/sites/roomykhan/2017/08/31/the-dnc-it-scandal-and-the-jackpot-lottery-fraud-when-digital-gatekeepers-become-thieves/#641997204c86>.

Koerner Brendan. (2017, February 6). Russians Engineer a Brilliant Slot Machine Cheat—And Casinos Have No Fix. *Wired*. Retrieved from [https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix/?BCCarticle\\_ID=9227&v=html](https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix/?BCCarticle_ID=9227&v=html).

Kroll. (2015). *Global Fraud Report 2015/2016*, November. Retrieved from <http://www.kroll.com/en-us/intelligence-center/press-releases/the-threat-within-insider-fraud-on-the-rise>.

Lottery glitch draws same Pick 3 numbers three consecutive days. (2005, December 23). *Lawrence Journal-World*. Retrieved from [http://www2.ljworld.com/news/2005/dec/23/lottery\\_glitch\\_draws\\_same\\_pick\\_3\\_numbers\\_three\\_con/](http://www2.ljworld.com/news/2005/dec/23/lottery_glitch_draws_same_pick_3_numbers_three_con/).

Marsh, Adrian. (2017, November 22). Arizona Lottery game glitch produces duplicated results again. *Azcentral*. Retrieved from <https://www.azcentral.com/story/news/local/phoenix/2017/11/22/arizona-lottery-game-glitch-produces-duplicated-results-again/890839001/>.

Pereira, Helena. (2016a.) The Importance of Security and Fraud Detection for Electronic Drawings. *Public Gaming Magazine*, July/August. Retrieved from <http://www.publicgaming.com/PGIJULYAUGUST2016/PublicGamingMagazineJuly-August2016/HTML/#54>.

Pereira, Helena. (2016b.) RNG Integrity: Perceptions of Fraud Risk and Known Vulnerabilities. *Lottery Insider*, Vol. 78, no.5, January. Retrieved from <http://www.lotteryinsider.com/vol78/no5.htm#01>.

Tennessee Lottery reveals problems with Cash 3, Cash 4 drawings (2007). *wmcactionnews5*. Retrieved from [http://www.wmcactionnews5.com/story/6963034/tennessee-lottery-reveals-problems-with-cash-3-cash-4-drawings\),and](http://www.wmcactionnews5.com/story/6963034/tennessee-lottery-reveals-problems-with-cash-3-cash-4-drawings),and).

Vogel, Nancy. (2005, May 13). Glitch Trips Up Lottery’s Derby. *Los Angeles Times*. Retrieved from <http://articles.latimes.com/2005/may/13/local/me-derby13>.

Weiss, Mark. (2010, October 18.) Israel lottery draws same numbers as three weeks before. The *Telegraph*. Retrieved from <http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8070751/Israel-lottery-draws-same-numbers-as-three-weeks-before.html>.

Disclaimer:  
Our analysis of events is strictly based on publicly available information and our knowledge and experience with RNG technology.  
Determining what actually happened in specific cases was not our goal. We, rather, use the events as examples of problems and vulnerabilities of electronic draw systems. We present a solution that protects against RNG risks independent of the source of the problem and that has been used by lotteries since 2005.



Szrek2Solutions