Using DNA to Secure High Tech Supply Chains and Protect Against Counterfeiting and Diversion

James Hayward, Ph.D. and Larry McIntosh
Applied DNA Sciences

DNA is a form of forensic evidence trusted by law enforcement and recognized by international courts around the world. This abstract provides an introduction to the utility of botanical DNA taggants to safeguard electronic components in supply chains and to protect against counterfeiting and diversion. A detailed treatment of the science behind Applied DNA Science's botanical DNA technology, its applications to semiconductors and microchips and an overview of DNA analysis by PCR and CE analysis is provided.

Counterfeit Electronics – A Global Threat

The evolution of counterfeiting as a trade nearly parallels the evolution of technology itself. The last two decades have witnessed explosive growth of technology, and the condensation of travel, communication and the massive impact of the internet ensured these new technologies were laterally propagated instantly across the planet. Now counterfeits emerge on the market nearly simultaneously with new product launches, in time for the counterfeits to benefit from the marketing efforts expended by the original. The World Customs Organization estimated that annual global trade in illegitimate goods was roughly $600 billion in 2004, and was expected to double by 2014, representing between 5% to 7% of all world trade (Source: The International Anti-Counterfeiting Coalition). But this is more than a vexing nuisance for brand owners. Counterfeits threaten economies, destroy health and take lives, and destabilize the military.

The Defense Standardization Program Office (DSPO) Journal (Oct/Dec 2009) recognizes the definition of a counterfeit electronic part as "one whose identity or pedigree has been deliberately altered, misrepresented or offered as an authorized product." Early reports of counterfeit electronics emerged from industry. In May of 2006, the New York Times reported a massively coordinated effort of 18 factories in China to copy the entire product line of NEC. Nearly every aspect of the company's brand and product line had been replicated and sold along parallel paths. NEC even found itself honoring the warranties for the fakes.

In June of 2007, the US Department of the Navy suspected that an increasing number of counterfeit electronics was infiltrating the Department of Defense (DOD) supply chain. In collaboration with the Department of Commerce (DOC), a study was initiated to assess the defense industrial supply base and to determine the statistical frequency of counterfeit electronics penetrating DOD. The results of this study, finalized in January, 2010 (US DOC "Defense Industrial Base Assessment: Counterfeit Electronics") showed:

- All elements of the military supply chain have been directly impacted by counterfeit electronics;
- Stricter testing protocols and quality practices are required; and,
- The use of authentication technologies by parts manufacturers, distributors and integrators should be expanded

Current Authentication Solutions are Inadequate

Efforts to secure the authenticity of electronics are first encountered at the primary and secondary packaging. Traditional security platforms to prevent counterfeits are now also part of the counterfeiter's target and consequently within the retinue of counterfeiter's resources. New advances in holograms, optical strips and RFIDs are often available as near-perfect copies within days of their initial launch.

Exacerbating the inadequacy of packaging security solutions, most distributors and integrators store microchips and semiconductors in high-volume bins, capable of matching the demands on their supply. This "bin approach" excludes the packaging to save space and time, so security must be implemented at the product level.

Product inspections offer limited value as a method of authentication. External visual inspections should not be used as a standalone authentication. Physicochemical characterizations are often destructive and rely on a degree of similarity to a bona fide original and the tolerance of the measurements.

Taggants can provide a unique code or fingerprint to authenticate originality. However, as evidentiary tools, the value of a taggant increases as a function of the density of its information content. Mineral taggants, which simply provide parameters of chemical identity and concentration, are only effective as rapid screening tools, often by handheld detectors. Stochastic arrays of fibers or particles are difficult to incorporate in the media used to fabricate microchips and semi-conductors.

Stochastic arrays of Nano particulate ferrite can generate complex "fingerprint" patterns, but care must be exercised to ensure the magnetic field does not interfere with semiconductor function.

Forensic DNA as a High-Content, High-Resolution Taggant to Track Provenance and Ensure Authenticity

Evolved over eons, DNA (deoxyribonucleic acid) provides the blueprint for all of biology. The information content is massive, highly customized by organism, and capable of supercoiling and compaction into infinitesimal space. With a capacity for content that is often compared to computer machine code, DNA is a linear polymer of extraordinary molecular weight that stores its information as a sequence of infinitely variable organic bases. However, unlike binary machine code, DNA's code is quaternary, storing its content as a linear array of four organic options for each bit. With the uncanny variability of DNA (consider the entire variable across organisms and the variation within species), matched by a stringent fidelity, and detection methods that readily identify single molecules of a unique sequence (a detectability that will never be matched by any chemical or physical assay); DNA has become the "Gold Standard of forensics." Challenged by courts around the globe since 1980, there is no better proof of identity, nor is any better proof of identity likely to evolve.

Used by forensic laboratories all around the world, including the FBI, DNA authentication is absolute in character. When used to identify individuals or to establish paternity, the error frequency for false positives is less than one in a trillion.

SigNature DNA markers cannot be copied or reverse engineered and have already been independently validated through a two-year vetted process conducted by the DoE and the Idaho National Laboratory. This technology has been selected as the sole security platform in a program funded by the European Regional Development Fund (a fund allocated by the European Union) and Yorkshire Forward. DNA applications will include the protection against counterfeiting and diversion of UK manufactured textiles from "fiber to fabric." Additionally, these markers have been tremendously successful with law enforcement agencies across Europe resulting in criminal convictions and jail time.

APDN's Intellectual Properties (patents and trade secrets) provide the mechanisms for protecting DNA in harsh chemical and physical environments (see Table below), the insertion of DNA into plastics, films, adhesives, inks, metal surfaces, and protects the methods used to enable DNA to function as a commercial authentication tool.

Table: DNA MARKERS' STABILITY
Applied DNA Sciences, Inc.

Test	Test Specifics	Results
UV Energy	Equivalent to more than 350 years of UV energy accumulation in Denver	Stable
X-ray	4 times the X-ray exposure by scanning machine in an airport	Stable
y-Ray	30 key (kilo-Gray) radiation exposure by y-ray sterilization machine	Stable
thermal	Exposed to pH of 1 to 14 overnight	Stable
Thermal	up to 250 degrees Celsius	Stable

Botanical SigNature DNA:

- is an environmentally friendly, "green" technology derived from botanical DNA,
- is used as a taggant at extremely low concentrations,
- will not alter the quality of any carrier (such as ink, coatings, adhesives, plastics or commercial products) will not require major changes in manufacturing process,
- persists, in physicochemical extremes such as harsh outdoor environs and high temperatures,
- is chemically compatible in a wide range of security inks (overt and covert), varnishes, adhesives and substrates,
- can be layered with other security measures, including barcodes, holograms, RFIDs, etc.
- is detectable in the field, and finally,
- can be forensically authenticated when analyzed in the laboratory.

Key Attributes of SigNature DNA
Applied DNA has proved that its botanical DNA technology provides the following advantages over existing competitive security options.

- ***Resistant to reverse engineering or replication.*** The botanical SigNature DNA platform is virtually impossible to copy. Proprietary methods yield DNA taggants so complex that they are statistically impossible to duplicate. In addition, the DNA segment used in the taggants needs to be replicated billions of times in order for detection and identification to take place, a process that can only be achieved by applying matching strands of DNA. Thus, the sequence of the relevant DNA in a specific taggant must be known in order to manufacture the primer needed for the detection process. The inability of counterfeiters to duplicate SigNature DNA taggants has been proven in the marketplace. A European media manufacturer's production of 600 million optical digital video discs (DVDs) in China included 12 anti-counterfeiting security platforms. Within nine months of the launch of the DVDs, 11 of those 12 anti-counterfeiting platforms were replicated in the market place, with SigNature DNA being the only exception. Moreover, SigNature DNA taggants on those DVDs remain effective to date, three years after launch.

- ***Secure.*** Applied DNA maintains its records of DNA sequences on a secure server. Sequences are encrypted, available to individuals on only a partial basis.

- ***Low Cost and High Accuracy.*** SigNature DNA taggants are relatively inexpensive when compared to other anti-counterfeiting devices, such as RFIDs, integrated circuit chips, and holograms. The costs associated with the production of DNA taggants are not significant since the amount of DNA required for each taggant is small, and the cloning of the DNA segments is performed inside microorganisms such as yeast or bacteria, which are highly productive and inexpensive to grow. In addition, incorporating SigNature DNA into products does not require major changes to the manufacturing process or logistic chain. The relatively low cost of SigNature DNA does not affect its reliability. The probability of mistakenly identifying a SigNature DNA taggant is less than one in a trillion, making it virtually impossible to wrongly identify something marked with SigNature DNA.

- ***Easily Integrated with Other Anti-Counterfeit Technologies.*** SigNature DNA taggants can be embedded into RFID devices, labels, serial numbers, holograms, and other marking systems using inks, threads, and other media. The Company believes that combined with other traditional methods, the SigNature DNA solution provides a significant deterrent against counterfeiting, product diversion, piracy, fraud, and identity theft.

Industry Deployment of DNA Markers

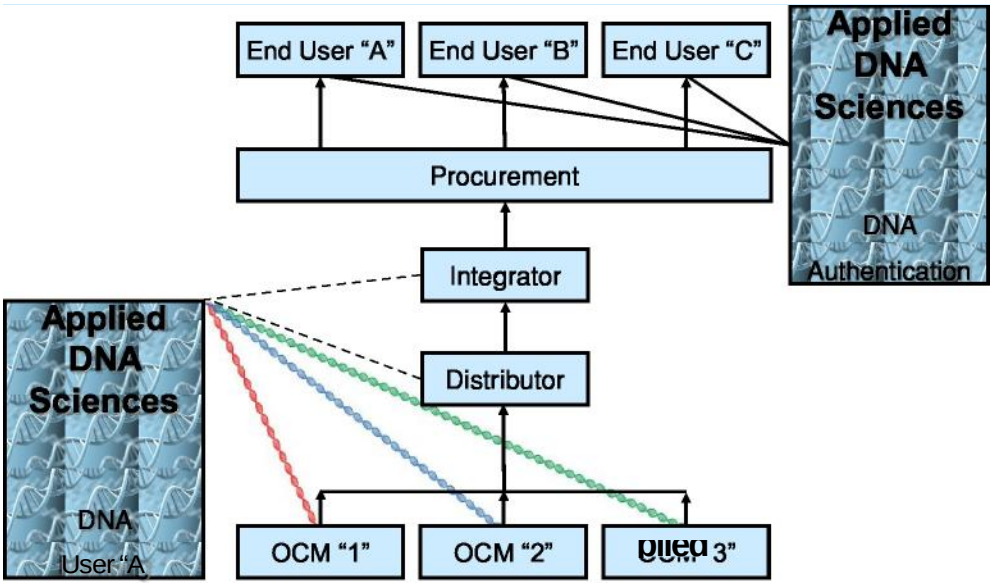
- ***Broad Applicability.*** Applied DNA's ability to integrate taggants in a variety of ways allows SigNature DNA technology to be embedded into almost any consumer product or item. SigNature DNA taggants do not alter the quality of the product and are stable and long-lasting. In addition, as SigNature DNA technology is safe to consume, it can be used in pharmaceutical drug tablets and capsules although it will require FDA approval.

- ***Scalable.*** DNA taggants can be produced in essentially infinite variety. Individual taggants of defined sequence can be manufactured in large scale. For example, in a single batch APDN recently marked 250,000 kgs of raw cotton fibers before ginning. DNA-tagged, individual fibers could be traced throughout the manufacturing process to the completion of retail garments and apparel.

Tagging Cash, the Ultimate Arbiter of Secure Logistics
Since January 2008, Applied DNA has been working with Loomis UK, a cash-handling company that moves over £150 billion in cash annually. APDN has developed taggants in fixatives (the DNA remains in a fixed location) or in transferrable (the DNA may be transferred by iterative contact) formats. In July 2009, Applied DNA announced that it successfully authenticated stolen bank notes, or cash and valuables in transit (CViT), and other recovered evidence received from the UK Police, which is used to assist in the prosecution of the alleged criminals. The SigNature DNA markers present in the recovered evidence resisted removal even after vigorous washing and were also detected on personal items such as clothing and mobile phones belonging to the suspects in the investigations. To support this initiative, Applied DNA opened its first DNA Authentication Laboratory in Yorkshire, England.

UK Police departments have retained Applied DNA Sciences to assist in forensic authentication and the provision of expert witness statements. By June of 2010, over thirty-five criminal investigations in the UK have used SigNature DNA taggants on recovered, stolen currency with a 100% success rate in linking submissions to dye stained stolen CViT. To date, more than thirteen of these cases have progressed to conviction with cumulative sentences in excess of 100 years. All told, APDN's customers enjoyed a 49% reduction in losses as a result of CViT offenses year-to-year while the UK industry as a whole saw a decrease in losses of only 34%. Showing public support, the UK Police have nominated Applied DNA for the 2010 Sheriffs Award and the Guardian Public Service Award. Additionally, police departments throughout Europe have begun using SigNature DNA in covert operations. In March of 2010, the head of the Swedish National Police issued a statement that it plans to use APDN's DNA taggants throughout its operations.

As shown in the flow chart below, the Procurement entity within the electronics industry typically services a range of End Users and would engage Applied DNA Sciences in the DNA marking process. Applied DNA would work with trusted supply chain participants, including, but not limited to, the Integrator, Distributor and Original Component Manufacturers (OCMs) and create unique DNA markers to be embedded into the microchip. Statistical confidence levels are established to determine authentication parameters. Lab analysis is then performed, typically in a non-destructive manner, at any point along the logistics chain. The analysis would absolutely distinguish between genuine and counterfeit components and unequivocal Forensic ID would be declared. The result would be authentic components in the end users' product with counterfeit components segregated and supported with forensic proof should legal action be deemed appropriate.



Using DNA to Secure High Tech Supply Chains

APEX EXPO™ IPC

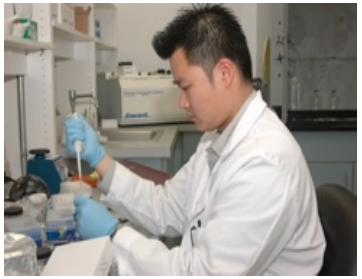
CONFERENCE & EXHIBITION April 12-14, 2011
MEETINGS & EDUCATION April 10-14, 2011
Mandalay Bay Resort & Convention Center, Las Vegas

applieddnasciences™
the ultimate reality check

About Applied DNA Sciences

Our DNA Authentication Labs and DNA Manufacturing facilities are located on the campus of Stony Brook University with access to the Cold Spring Harbor Laboratory. We also have DNA laboratories in Yorkshire, England with affiliations to University of Leeds. Our forensic Analytical Laboratories are staffed with Ph.D. scientists and technical teams.

STONY BROOK



CSH Cold Spring Harbor Laboratory

UNIVERSITY OF LEEDS

The Problem

Counterfeits and sub standard parts
Infiltrate the Supply Chain

The Objective

Risk Mitigation
Brand Protection

The Solution

DNA

Impact on Global Business

- U.S. Chamber of Commerce estimate finds that the global market for counterfeit electronics may be as large as $10 billion.

- It is estimated that there could be in excess of 10,000 brokering and non-franchised distribution operations working around the world.

- *“If devices are procured from a questionable source, the risk is high. Without traceability, a device must be subjected to the fullest extent of all legitimate, supplier-approved testing, especially in mission-critical situations.”*

Counterfeiting; 3 Scenarios

- **Manufacturing shortfall/product shortages**

Counterfeiting operations identify where they can sell their fake wares when there are device shortages caused by insufficient manufacturing output of a certain semiconductor.

- **High value products**

Counterfeiting operations identify where they can sell devices that cost them little to source but can be sold at the high market price of the genuine devices

- **Obsolete and discontinued device**

Counterfeiting operations find ways of delivering “products” that have been discontinued the original manufacturers.

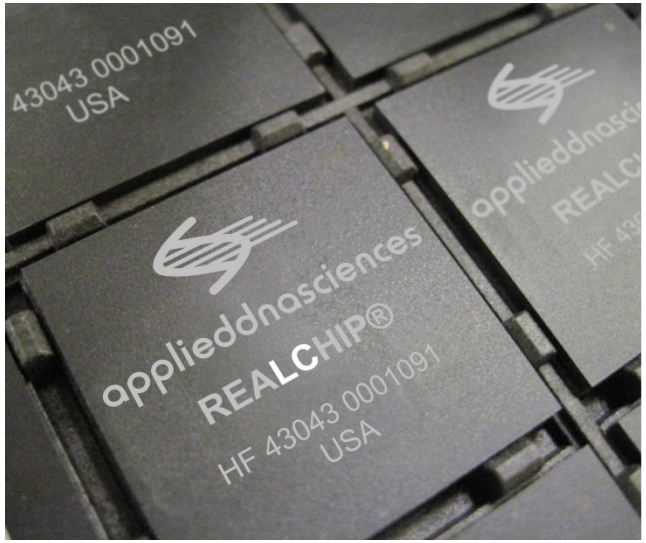
  - In each of these cases the devices delivered are unlikely to operate as genuine parts and very often, by the time the user has identified there is a problem, the source of the device has vanished or is untraceable

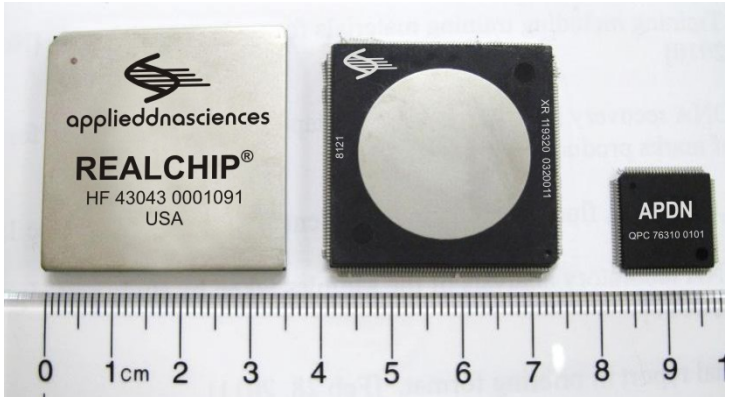
DNA is the "Gold Standard" of Forensic Evidence

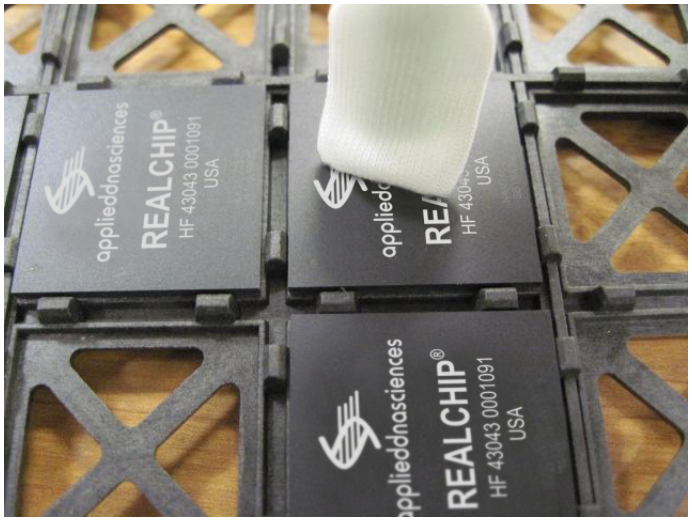
DNA is a form of Forensic Evidence trusted by Police and recognized by Courts globally.

No other form of evidence has withstood such scrutiny.

Protecting the Supply Chain at the Source! The DNA Marking of Microchips..







Can You Tell the Difference?

Real

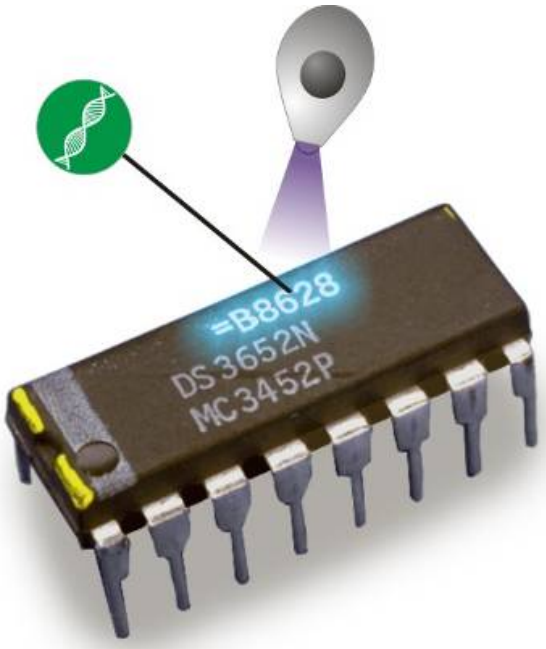
Fake

We Can!

DNA offers absolute authentication. Parts can be **“branded” at the molecular level** using the gold standard for forensic evidence most preferred by global courts.

Microchip Marking Opportunities DNA-UV Adducts

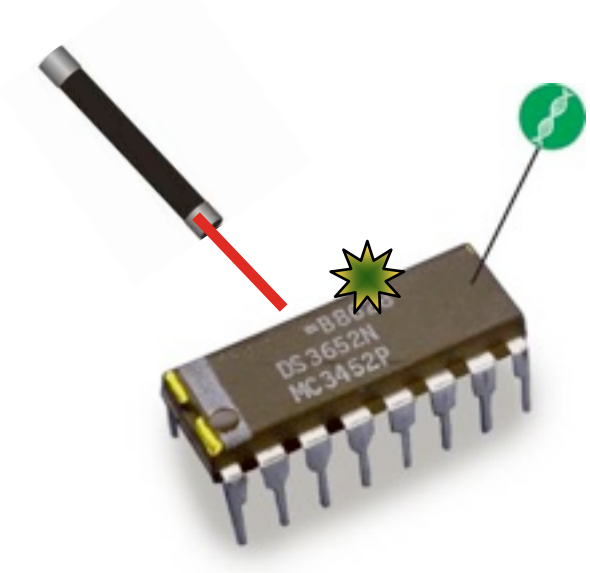
- Ink-jet Inks, Flexographic Inks, Silk Screening Inks, Thermal transfer resins, Laser toner
- Dielectric coatings
- Varnish or Top-coat
- Ink-jet label sprayed onto MC
- Plasma deposited DNA
- Secure label placed MC or PCB



Microchip marked with DNA/Fluorescing ink

Microchip Marking Opportunities DNA-IR Adducts

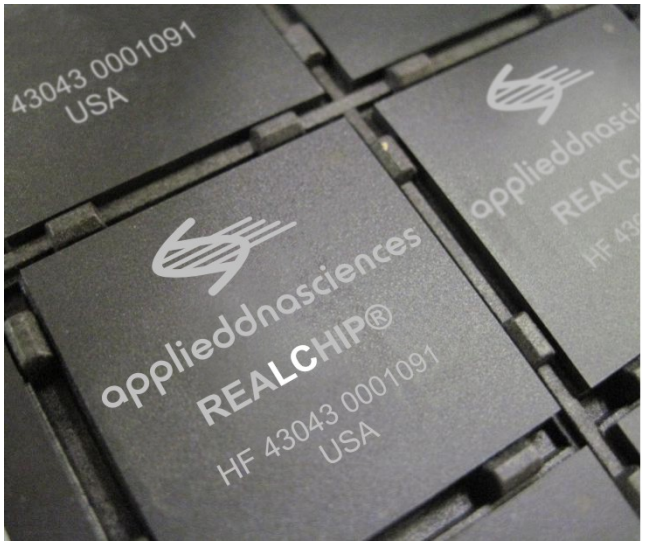
- Can be detected with hand-held fob or by eye following IR laser irradiation (10 mwatts yield visible light emission)

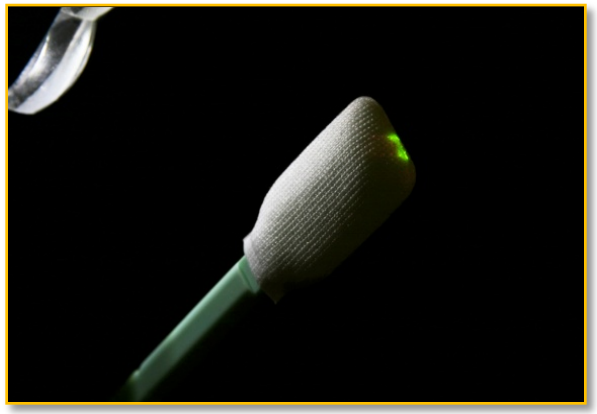


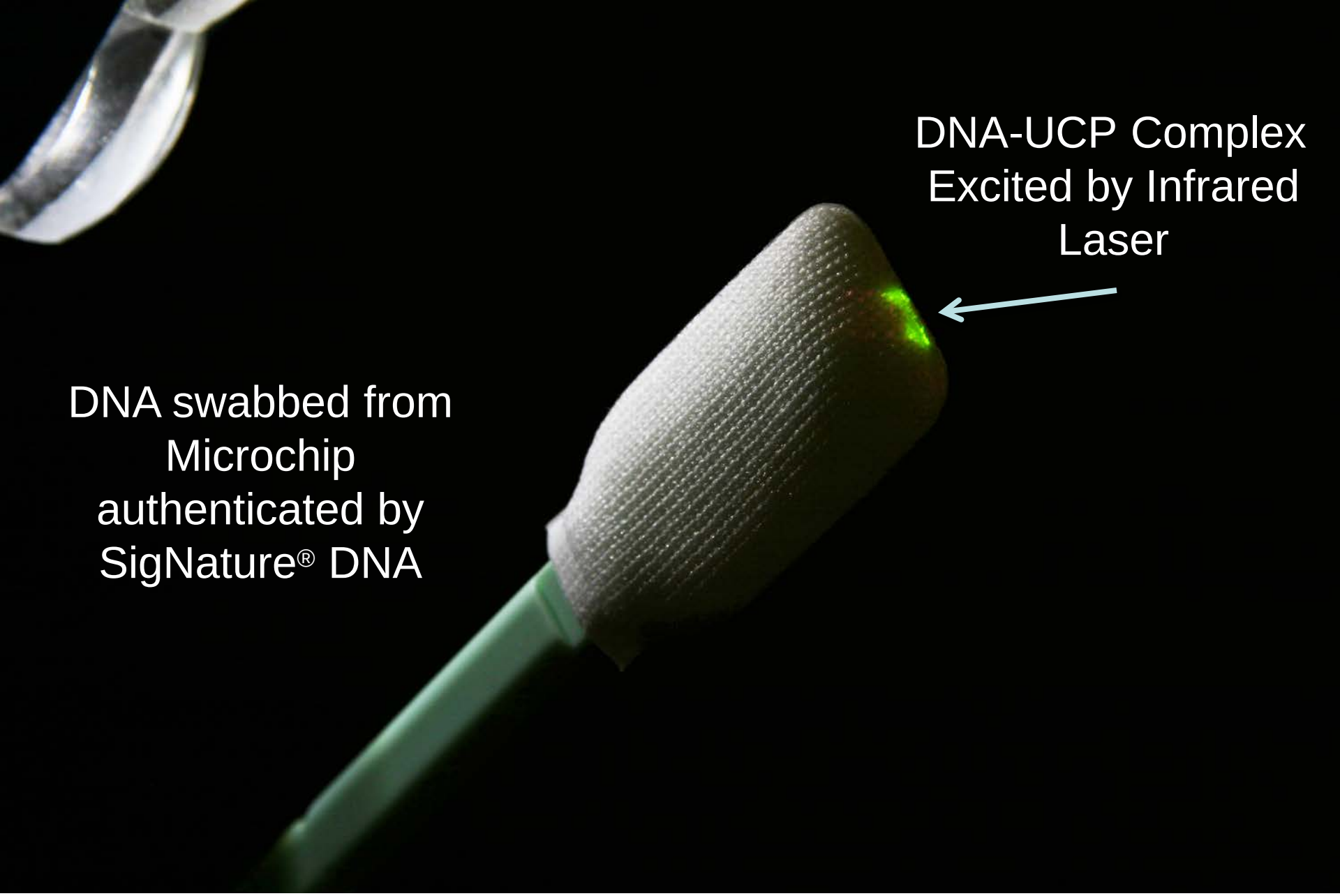
- Varnish or Top-coat
- Metal coatings
- Tertiary Carriers, Cartons or Sealed bins

Swabbing Technique used to Recover DNA from Chip's surface

Figure 3 and 3a– OCM swab sampling technique (depicted in photo on the left), was used to gently lift DNA from printed surface of the microchip. The swab's tip (depicted above) glows brilliant green (under IR laser light) instantly indicating the presence of APDN DNA in sample.






DNA-UCP Complex Excited by Infrared Laser
DNA swabbed from Microchip authenticated by SigNature® DNA

DNA PROTECTED, Tamper evident Fluorescent Label

Figure 1a – DNA PROTECTED Label
Label (under UV (under normal light)

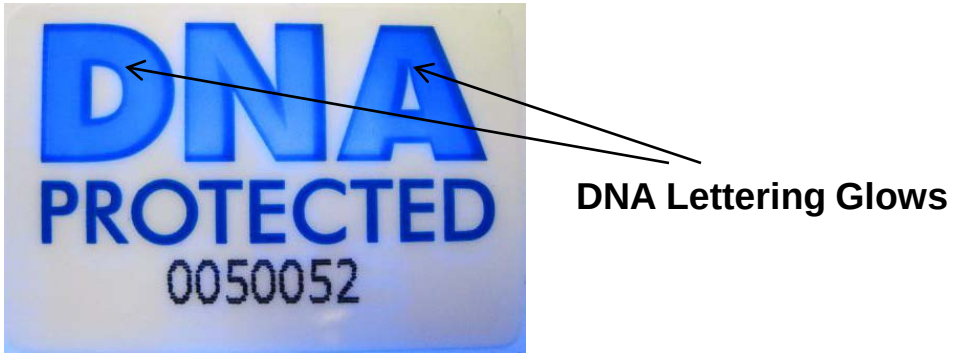


Figure 1b- DNA PROTECTED

Sample Processing:

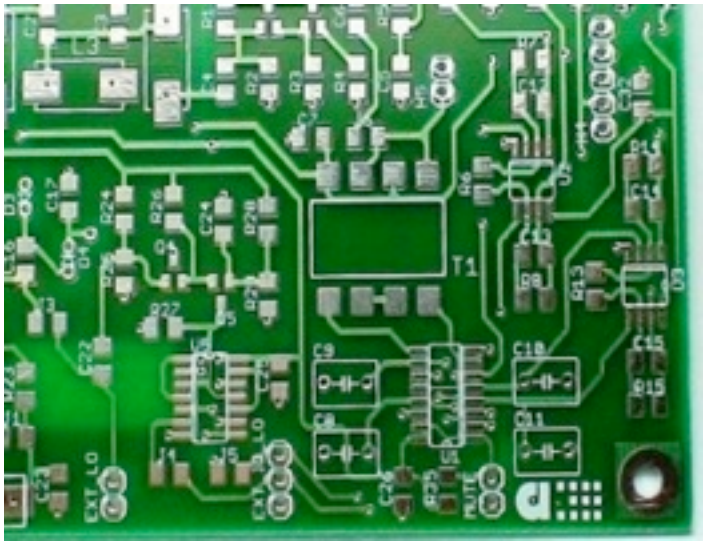
Each sample submitted was forensically evaluated for the Presence of DNA. DNA extraction was performed using a proprietary protocol

Tamper evident **VOID**
will appear upon removing label.

Microchip Marking Opportunities Printed Circuit Boards

- Conformal coatings
– Keep dust, water and conductives out
– Keep DNA-Rapid Reporter in

- Antistatic bags
- Tertiary Carriers, Cartons or Sealed bins



Microchip Marking Opportunities: Labels for Moisture Barrier Bags

- Secure Labels ensure chips can be authenticated without removal

Microchip Marking Opportunities Plastic Packaging

- DNA inserted during plastic molding stage
- Supply agreement with second largest global IMD manufacturer (Tokyo)
- Supply agreement with one of Europe's largest brand-owners

In-Mold Decoration

SigNature DNA is a Proven Technology

- **Productized.** Over a billion commercial products marked.
- **Stable.** Established forensic quality authentication which has been independently validated by Idaho National Labs. Operated by Battelle Energy Alliance and DOE.
- **Reliable.** Negligible false positives.
- **Intellectual property.** Broad scope of intellectual property rights – 38 patents and 7 trademarks. Strong Trade Secrets base.

DNA Secure Content

Linear Code in Molecular Polymer is Similar to Machine Code (but more dense)

Creating a SigNature DNA Marker

Large Botanical DNA is acquired.

DNA is segmented.

Segments are shuffled, reassembled and encrypted to form a unique, secure DNA marker.

DNA: Because it CAN…

- Scientifically verify genuine product and legalize pedigree.
- Enhance logistic security with a forensic evidentiary trail.
- Pinpoint gray market diversion through a combination of covert and overt tagging systems.
- Resist aggressive removal techniques.
- Be combined with rapid detection techniques.
- Adapt to virtually any physicochemical environ.
- Stand to challenge as irrefutable evidence in law courts, worldwide.
- Be readily scaled in creation and authentication.
- Offer a green solution.

And Because it CANNOT…

- Be copied even if samples are removed for sophisticated laboratory re-engineering and or replication purposes.

SigNature DNA Protects 40% of the UK Cash-in-Transit Industry (>40 B$/yr)

1. Loomis Cash Box "Attack"

Following discharge, cash is marked with SigNature® DNA.

2. Recovery of Stained Notes

Stained Evidence recovered by U.K. Police

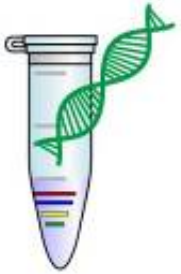
3. Screen for SigNature® DNA

DNA marker detected with UV handheld device.

4. Sample Collection

Stained evidence sent to DNA Lab for analysis.

5. DNA Analysis



DNA is extracted and analyzed.

6. DNA Authentication

An Expert Witness Statement Report is provided to the UK Police and Loomis. Before a Case Goes to Trial, the Police submit the Report to the Crown Prosecution.

DNA-UCP adducts protect the entire custody chain

- 18 months: 22+ convictions; 120+ years of jail time.
- 100% authentication rate; 100% conviction rate.
- Now being adopted across the country of Sweden, and throughout the EU.

Current Hosts for DNA

- Surface treatments, plastics, laminates, varnishes, clear coats, reactive adherents
- Plasma deposition
- Metal surfaces, metal coatings
- Extruded, molded plastics, IMD
- Cyanoacrylates and adhesives
- Wide range of security inks
  - Flexo, offset, gravure, thermal transfer
- Laser toner and inkjet Ink
- Cash degradation ink
- Paper, labels, packaging
- Textile treatments, yarn, fabric
  - Integrated in fibers
  - Direct application onto product
  - Woven labels, insignias

Can You Tell the Difference?

Real

Fake

We Can!

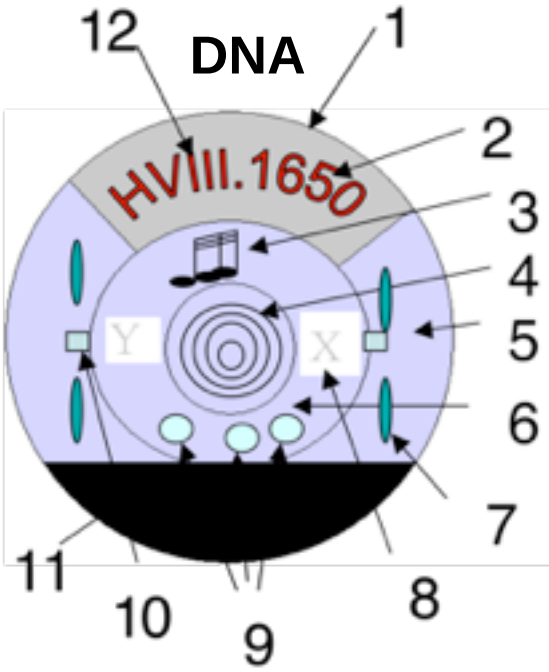
DNA offers absolute authentication. Parts can be **“branded” at the molecular level** using the gold standard for forensic evidence most preferred by global courts.

SigNature DNA Can Protect Electronics and Electrical Components

SigNature DNA can mark virtually any material including metal, in-mold secure printing for electronics, laminates, inks, polycarbonate, plastics, etc.

Millions of EU Optical Disks tell our story…

DNA



1. PET Al sputtered foil release label
2. Fluorescent red ink turns orange with red laser
3. Musical node hologram: shape shift/ change
4. 10 concentric circles. Shapes shift when tilted
5. X,Y microdots visible under 30X magnification
6. Random interference lines
7. 4 microprints of ‘AUDIO VIDEO’
8. Shine red laser 30° from top of X and US ‘culture’ projects on paper 45° below.
9. Three circles encoded with Characters ‘U’ ‘S’ ‘A’
10. Microprint ‘AUDIO VIDEO’
11. Machine readable encrypted codes
12. DNA embedded in #2 fluorescent ink

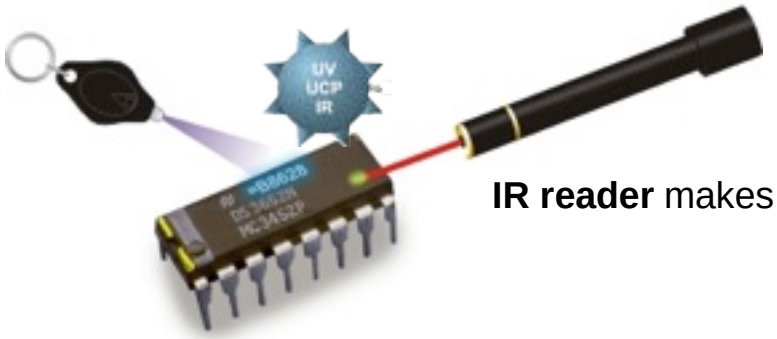
Within 9 months of launch, 11 of the 12 security platforms were copied by counterfeiters. SigNature DNA was the only measure that could not be counterfeited.

DNA combined with Optical Reporters

Rapid Reporters

Patented APDN Linkers to Optical Reporters

You must have the key to unlock the unique Forensic DNA code



IR reader makes DNA mark glow green

UV reader makes DNA mark glow blue

Applied DNA Sciences, Inc.

Dr. James Hayward

25 Health Sciences Drive
Stony Brook, NY 11790
www.adnas.com

The Anti-Counterfeiting Group

Safe Harbor Disclaimer OTCBB: APDN

The statements made by Applied DNA Sciences, Inc. (the Company) may be forward-looking in nature and are made pursuant to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Forward-looking statements describe the Company's future plans, projections, strategies and expectations, and are based on assumptions and involve a number of risks and uncertainties, many of which are beyond the control of Applied DNA Sciences, Inc. Actual results could differ materially from those projected due to changes in interest rates, market competition, changes in the local and national economies, and various other factors. The Company undertakes no obligation to update publicly any forward-looking statements to reflect new information, events or circumstances after the date hereof to reflect the occurrence of unanticipated events.

appliedDNAsciences
the ultimate reality check