South Carolina Manufacturer's Summit

Mitigating Risk & Maximizing Opportunity: How Manufacturers can Minimize Exposure and Protect Intellectual Property

Patrick Horne

Christy Trimmer

Jamie Gilmer

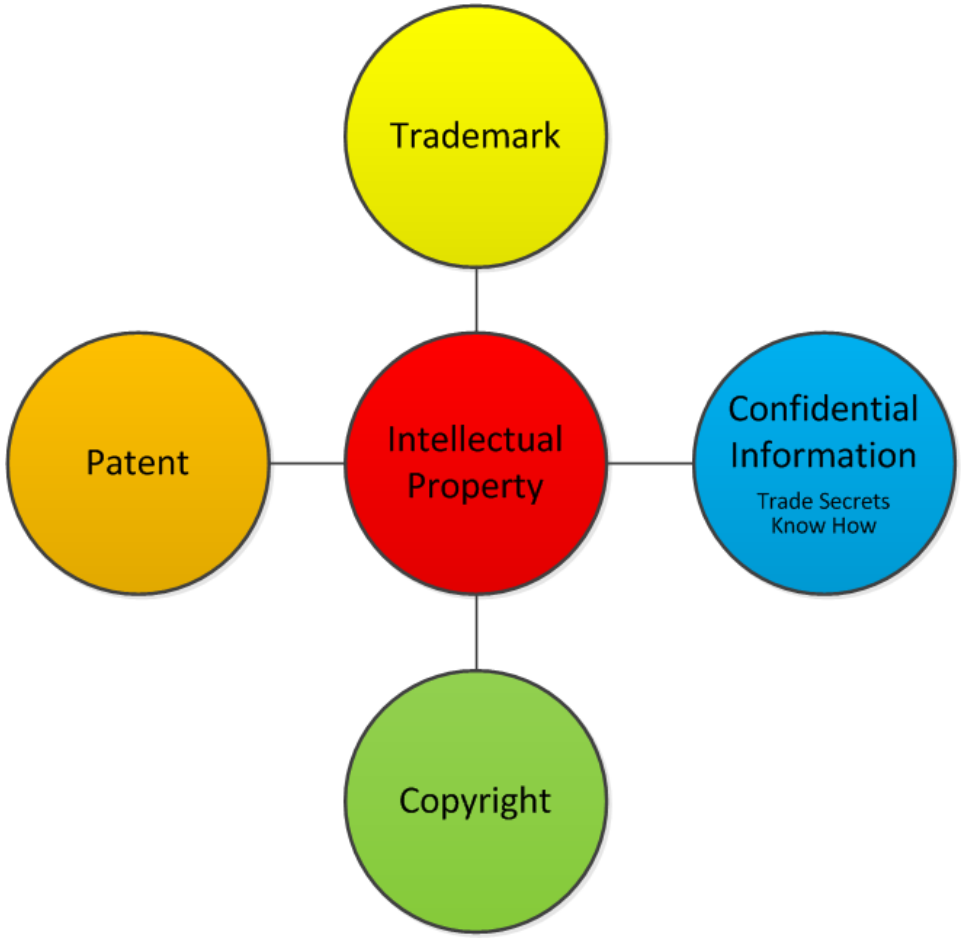
SHUMAKER

Maximize Opportunity

IP and Patents Intro

SHUMAKER

Types of IP


Trademark
Patent
Intellectual Property
Confidential Information
Trade Secrets
Know How
Copyright

Types of IP

- Patent – process, machine, functionality
- Trademark – product name
- Copyright – software, manuals, drawings
- Trade Secrets/Know How – sensor placement, heating times, mold pressures, etc.
- Confidential Information – cost, marketing strategy, customer lists, other information not qualifying as a trade secret. General rule is CI can be anything parties to a contract agree is “confidential information” (with exceptions).

Trade Secrets

- Subset of Confidential Information
- Protected by statute
- A formula, practice, process, design, instrument, pattern, or compilation of information that is:
  - not generally known or reasonably ascertainable;
  - confers economic benefit to the holder (benefit derives not only from the information but from its secrecy); and
  - is subject to reasonable efforts under the circumstances to maintain its secrecy.

Trade Secrets

- A trade secret is the owner's possession of information of a type that can, at the owner's option, be made known to others or withheld from others, i.e., kept secret.

- Trade secret law is not a protection of rights to an idea, but a right to control dissemination of an idea or fact.

Trade Secrets

- Examples:
  - Customer lists;
  - Pricing or margin data;
  - Client date – more than mere “contact information”;
  - Research and development data;
  - Non-public product drawings;
  - Strategic business plans;
  - Sales, marketing, or product manufacturing methodologies;
  - Sales data;
  - Critical self-analysis data.

Types of Patents

- Utility – directed to functional aspects of invention.
- Design – directed to aesthetics of an article.
  - i.e., look and feel.

Patents

- In return for disclosure to the public, the government grants certain rights to the patentee for the term of the patent to allow the patentee to exploit the invention. Scope of rights are defined by the claims.
- The right to exclude others from making, using, selling, offering for sale or importing the claimed invention.
- Utility patent term: 20 years from filing date.
- Design patent term: 15 years from issuance.
- Enforcement is up to the patent holder.
- ***Patent is not a license shielding from infringement of other's patents.***

Patents

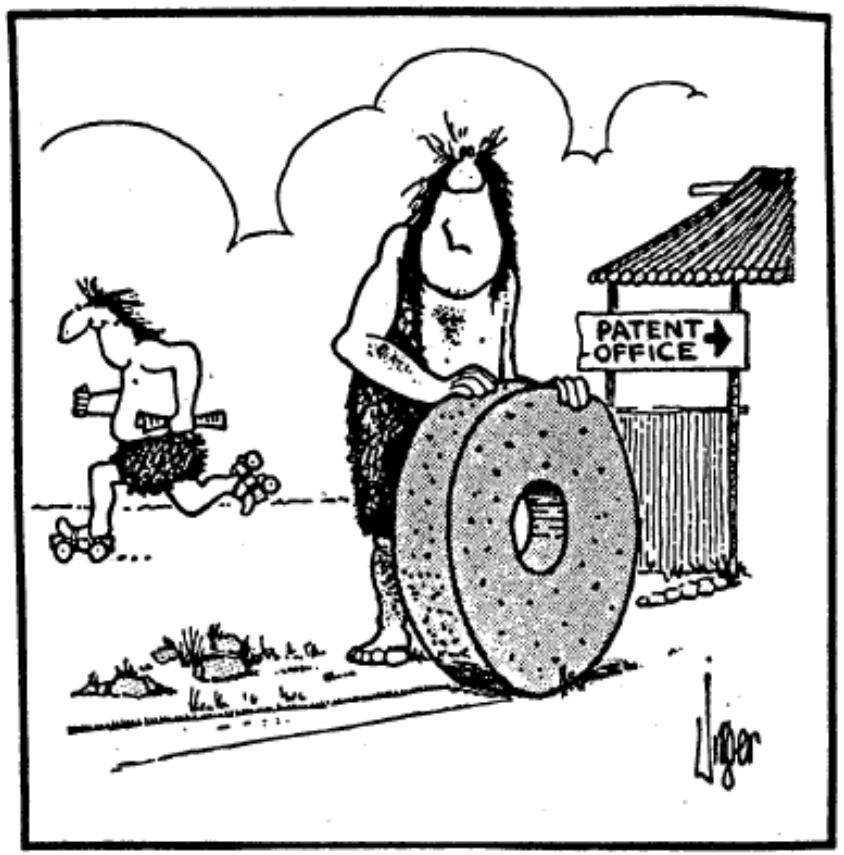
- ***Prevent others from making, selling or using your innovations.***
- ***Demonstrate value to potential investors or buyers.***
- Product differentiation.
- Keep competitors out of markets.
- Gain access to markets impacted by patents of others.
- Basis for strategic alliances.
- Deter others from enforcing their rights against you.
- Source of revenue.

Parts of a Patent

- **Cover Page** –
  - Inventors, Assignee, Dates, Related Apps, Fields of Search, References Cited, Abstract and Representative Drawing
- **Figures/Drawings**
- **Cross Reference to Related Application(s)** –
  Priority/Benefit Claims
- **Background/Summary**
- **Brief Description of the Drawings**
- **Detailed Description** –
  - Supports the Claims by Written Description, Enablement, Best Mode
- **CLAIMS** –
  - Heart of the Patent
  - Define the Meets and Bounds of the Invention

Standard for Patentability

- ***Patent eligible subject matter.***
- Novel.
- ***Non-obvious.***
- Useful.



Standard for Patentability

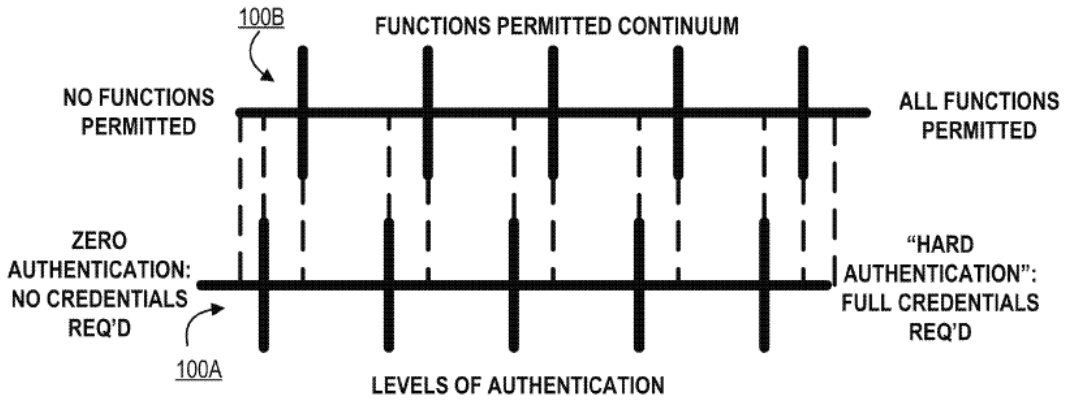
- First test – Is invention directed ***patent-eligible subject matter***?
  - Is it a process, machine, manufacture, or composition of matter.
  - Things occurring in nature, mental processes, algorithms, and ***abstract ideas*** are not patent subject matter.
  - Algorithm itself not patentable but software embodying the algorithm may be patentable, provided it is ***not merely an abstract idea***. It ***must be significantly more than any abstract idea*** embodied by the software.
  - Loan product itself not patentable but software implementing the loan product may be patentable.
  - ***This is where we spend most of our time with fintech patents.***

Standard for Patentability

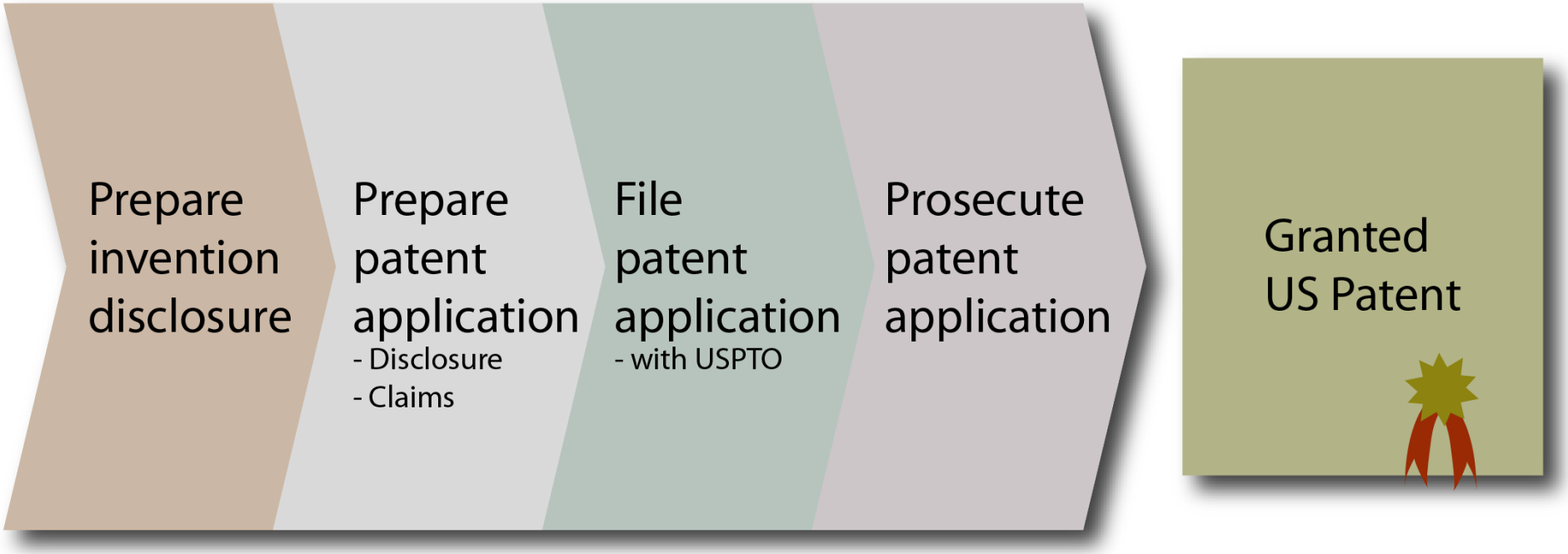
- Second test – Is it new and non-obvious.
- Anticipation – is the invention wholly described in the prior art.
- Obviousness – is there a combination of references that would make the invention obvious to one skilled in the art.
- You can't patent the authentication of an application user but you may be able to patent a authentication method.

Standard for Patentability

- Anticipation - Has the new authentication method been disclosed before?
- Obvious – Is the authentication method obvious based on similar known authentication methods?
  - Don’t overthink obviousness.
  - Legal question (where we spend a lot time).



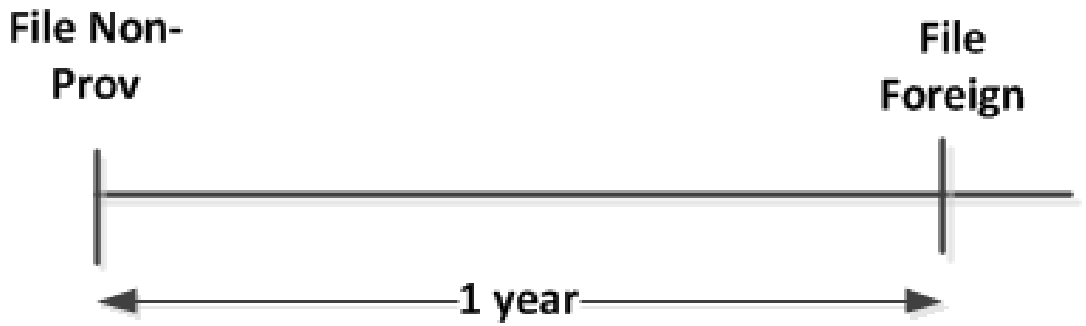
When to file application

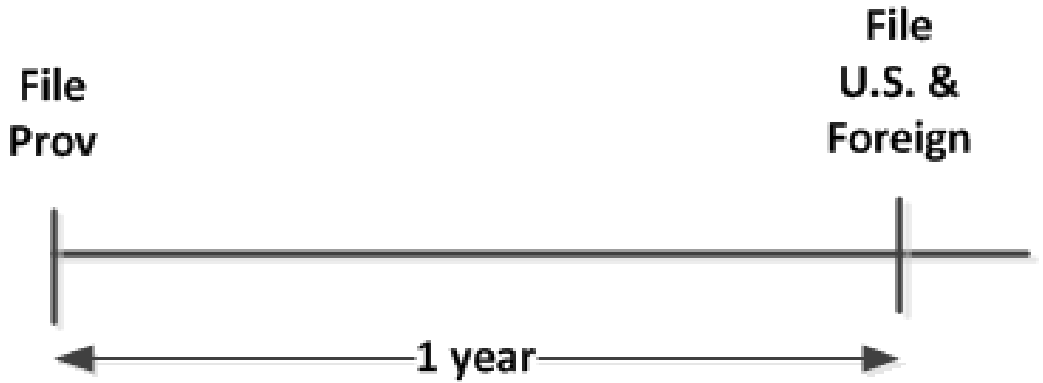


When to file application

- It’s all about timing.
- 1 year grace period – U.S., Canada, Mexico.
- Absolute novelty – EPO, Japan, China, etc.
- Public Disclosure or Use?
  - Disclosure under confidentiality agreement is not public disclosure.
  - Trade conference is public disclosure.
  - Disclosure for funding – gray area – don’t risk it.
  - Using invention for commercial purpose is public use.
    - Experimentation is an exception.

Maintaining Foreign Rights





Patent Rights

- Claims, claims, claims – the claims define the metes and bounds of the patentee's rights – not the description.
- Restrict others from making, using, offering for sale, selling, and importing into the U.S.
- Rights are generally confined to the border.

Minimizing Risk

Trademarks

Trademark Clearance Searching

- The best way to minimize the risk of trademark problems now or in the future is to make sure that a mark is available for use.
- The first step is knowing what a trademark usage is – When should you search? When are you exposed to potential infringement?
- The next step is to identify the scope of your intended use of the mark, in terms of:
  - the goods/services,
  - the strength of the mark, and
  - the geographic scope.

What is a Trademark?

NIKE®

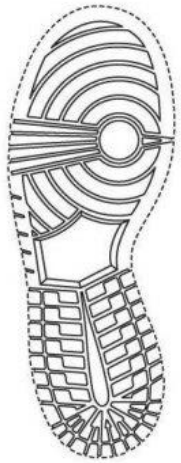
Word Mark
(House Mark)

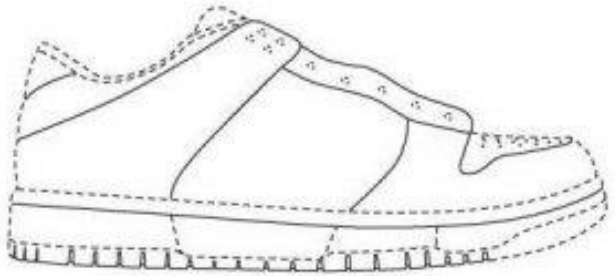
Air Force 1
Word Mark for
product

Design Mark
(logo)

JUST DO IT.

Slogan/catch phrase

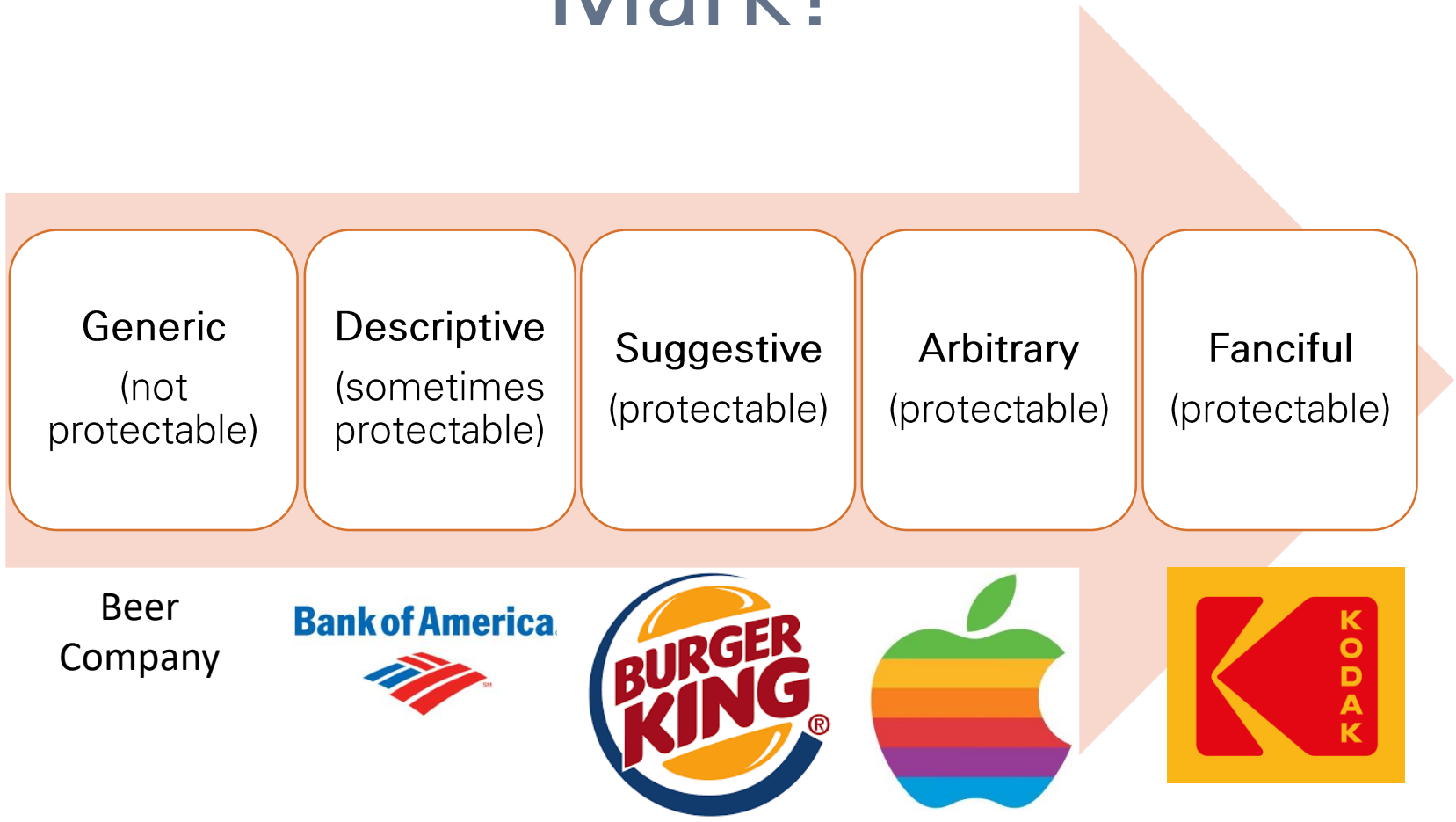




Trade Dress

Scope of Protection: Goods and/or Services

Scope of Protection: How Strong is the Mark?



Maximize Opportunity

Trademarks

Register Your Marks

- In the US, a federal trademark registration provides exclusive nationwide rights
- Provides legal assurances, but also gives you a property right to prevent others from using your mark.
- Three types of federal applications in US: (1) use-based; (2) intent-to-use; and (3) application based on foreign application/registration.
- Consider whether you should register in any foreign countries.
- Consider state registrations as well.
- NOTE: trademark registration is NOT the same as business registration or purchasing a domain.

Use Your Marks and Notice Your Rights

TM

SM

Police/Enforce your Marks

- Trademark rights are premised on exclusive use.
- Trademark owners have a duty to police their marks.
- This does not mean addressing every possible minor infraction, but showing that you are diligent about enforcing against any potential threat of consumer confusion.
- Make sure you are protecting all of your marks – again, this goes back to knowing what you own, and keeping good records regarding your trademark assets.

Minimizing Risk

Patents

Minimizing the Risk of Invalidity, Enforceability, and Design-Arounds

- Establish clear patent procedures
  - Get patent assignments at the outset of the application
  - Use standard forms to capture ideas
  - Be sure to cross-cite references
  - Monitor deadlines
  - Utilize NDAs
  - Do IP training during onboarding
- Perform or have a third party conduct a patent search
- Draft strong dependent claims
- Describe alternate embodiments
- Capture a diverse range of solutions
- File continuations
- Use "picket fence applications" for defensive purposes and "omnibus applications" to capture several related ideas in a single application

Duty of Disclosure

- Failure to disclose relevant information to the United States Patent and Trademark Office (USPTO) can result in a patent becoming invalid and unenforceable.
- Everyone involved in the filing and prosecution of a US patent application has a duty to disclose to the USPTO all information which is relevant in assessing the patentability of the invention which is the subject of the patent application. This applies not only to the inventor(s) but also to anyone else who is involved with the patent application, for example, patent owners and patent attorneys.
- Information is considered to be "relevant" if the US examiner is likely to need to take it into account when examining the application. That is, if it may arguably render any claim unpatentable. If there is any doubt about relevance, it is advisable to disclose the information.

But everybody else is doing it…

- Patent Infringement:
  - Selling, importing, using, or making a product covered by a patent without the patent owner's permission
- Patent Infringement Types:
  - Direct infringement – infringing a patent, even without knowledge of the patent
  - Indirect infringement – infringer did not directly infringe, but helped to infringe on the patent
  - Induced infringement - inducing or persuading someone to infringe a patent
  - Contributory infringement – someone provides a part or a product to help someone else infringe a patent
  - Willful infringement – purposely infringing a patent – will cost you triple!

Myths About Patent Infringement

- We don't need to worry about our competitors' patents because we have our own patents on our products
- We can't be sued for patent infringement because the technical components of our products are made by our suppliers
- We are a government contractor, so we don't need to worry about whether we infringe any patents
- We cannot infringe a patent because we did not copy anyone else's products
- We are using old technology, so we don't have to worry about patent infringement
- Our products are industry standard or standard essential technology so we don't have to worry about patent infringement
- We filed an international patent application, so we will have

Patent Infringement on Amazon

Amazon Utility Patent Neutral Evaluation Procedure (UPNEP) is fast, cheap, and easy for owners of US utility patents or their exclusive licensees

- Timing:
  - Patent Owner has 14 days to submit initial arguments
  - Seller has 14 days to respond
  - Patent Owner has 7 days to reply
  - Decision will be announced within 14 days of the reply date
- Cost:
  - Evaluation is $4,000 from Patent Owner **and** Seller and covers the Evaluator's expenses – no money goes to Amazon
  - Cost is paid by the participant(s) losing the evaluation in the event an evaluation actually occurs
- Process:
  - A neutral evaluator reviews a patent infringement claim and will make a "yes/no decision" about whether the patent covers the product listings.
  - Reasons why an evaluator would say no:
    - Product does not infringe
    - A court has found the patent invalid or unenforceable
    - The accused products were on sale more than one year before the earliest effective filing date of the patent
  - If an evaluator concludes that the accused product is covered by a patent, Amazon will remove the products from Amazon.
  - If a seller does not participate, Amazon will remove the accused products
  - Evaluation is limited to one claim
  - No discovery
  - Only three defenses will be considered by the Evaluator:
    - Non-infringement based on failure to meet one or more claim limitations
    - Invalidity and/or unenforceability by providing a finding by a court of competent jurisdiction or by the USPTO or ITC (Evaluator will not determine validity, must have a court order)
    - On sale one year or more before the asserted patent's earliest effective filing date (any credible evidence that the Evaluator can independently observe such as a sale date on Amazon or Wayback Machine) – affidavits, declarations, or mere arguments will not be accepted

Patent Infringement Defenses

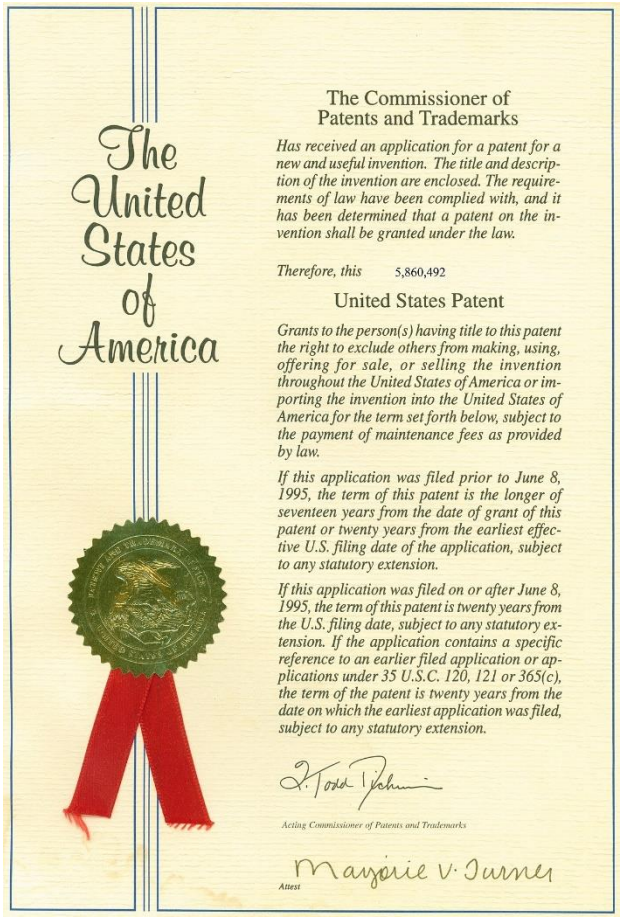
- The patent holder was dishonest on the application
- The patent holder included wrong or misleading information on the patent
- A person used the patented item or idea for illegal activity
- The patent violates antitrust and other competition laws
- It did not meet novelty and non-obvious requirements
- A formal non-infringement and/or invalidity opinion can be used to help avoid willful infringement and treble damages

Maximize Opportunity

Patents

5 Reasons You Need a Patent

- Patents increase profits
- Patents increase company valuation
- Patents obliterate the competition
- Patents attract investors
- Patents are cheap compared to how much money they will make you



The United States of America

The Commissioner of Patents and Trademarks

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this 5,860,492

United States Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America for the term set forth below, subject to the payment of maintenance fees as provided by law.

If this application was filed prior to June 8, 1995, the term of this patent is the longer of seventeen years from the date of grant of this patent or twenty years from the earliest effective U.S. filing date of the application, subject to any statutory extension.

If this application was filed on or after June 8, 1995, the term of this patent is twenty years from the U.S. filing date, subject to any statutory extension. If the application contains a specific reference to an earlier filed application or applications under 35 U.S.C. 120, 121 or 365(c), the term of the patent is twenty years from the date on which the earliest application was filed, subject to any statutory extension.

Acting Commissioner of Patents and Trademarks

Attest

SHUMAKER

Small Entity Status

- If small entity status is asserted in a patent application or patent, the official fees (including the filing fees, issue fee, and maintenance fees) are reduced by 50%.
  - Micro entity status provides 75% reduction in official fees – must be a small entity, no more than 5 earlier filed applications, a gross income that does not exceed 3x the US median household
- The payment of small entity status fees when not entitled to do so may make the patent application or patent invalid or unenforceable.
- The rules which determine whether or not a particular entity is a "small entity" are very complex. However, in general, the following are "small entities":
  1. An individual (e.g. an inventor, an individual to whom an inventor has transferred some rights in the invention);
  2. A small business concern, as defined by complex rules which depend upon, for example, the type of business, the number of employees and/or its annual receipts. In many cases, this includes a business which employs fewer than 500 employees and which is not part of a "group" of companies which employs more than 500 employees in total. A "group" of companies includes any parent company, subsidiary, any subsidiary of a parent company, etc.;
  3. A non-profit organization, as defined by complex rules (e.g. certain universities, foundations, charities etc.).

Virtual Patent Marking

- The Leahy-Smith America Invents Act (AIA), signed into law on September 16, 2011, was designed to establish a more efficient and streamlined patent system to improve patent quality and limit unnecessary litigation costs. The AIA made many changes to United States patent law, including an amendment to 35 U.S.C. § 287(a), the so-called "marking" statute. **The purpose of marking an article is to provide constructive notice to the public that the article is patented.** Failure to appropriately mark an article can preclude the recovery of damages for infringement until effective notice is given. In the AIA, Congress intended to modernize and update the statute. The AIA provides patentees with the option of using "virtual marking," *i.e.*, affixing onto the article or its packaging the word **"patent"** or the abbreviation **"pat."** followed by an **Internet address**.

Virtual Patent Marking Examples

Patents / Brevets: www.kimberly-clark.com/patents

PAT. OR PENDING
YETI.COM/PATENTS

SHUMAKER

Minimize Risk

Cybersecurity and Data Breach

SHUMAKER

What is Cybersecurity?

- Cybersecurity are the measures an organization takes to protect their information technology infrastructure (computers and computer systems) from unauthorized access, attack, and vulnerabilities.
- Cybersecurity is proactive not reactive.

Why is Cybersecurity Important?

- Data has value
- People and organizations generate an enormous amount of data.
- Generating, collecting and storing data has risk
  - Contractual obligations (i.e. indemnification)
  - Federal law
  - State Law
  - Global privacy laws (e.g., GDRP, APEC)

Data Breach

- A data breach is the action that most often triggers an obligation or legal duty under a contract or statute.
- Generally, a data breach is defined as unauthorized access to and acquisition of data that compromises the security or confidentiality of such data.

Incident Response / Data Breach Plan

- Every organization should have an Incident and Data Breach Response Plan
  - Response Team
  - Have counsel pre-selected
  - Work with counsel for a plan on the forensic investigator you're going to bring in.
  - Insurance Coverage
  - Public Relations Team
  - Call Center
  - Legal obligations
    - Law enforcement
    - Notification to Data breach victims
    - Contractual obligations

South Carolina Cybersecurity Law

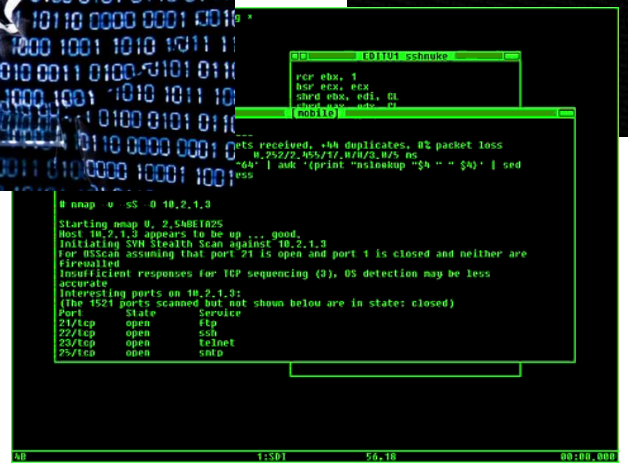
- Section 39-1-90 of the South Carolina Code of Laws
- Applies to individuals, businesses, governmental entities, and other entities that own, license, or maintain personal information. Certain entities may be exempted from particular or all provisions of the law.
- Personal Information is first name (or FI) and last name in combination with SS#, Driver's License #, account #, CC/DB#, etc.
- Must notify individuals in the most expedient time possible and without unreasonable delay.
- If more than 1,000 persons are notified, the entity must also notify the South Carolina Department of Consumer Affairs, Consumer Protection Division without unreasonable delay of the timing, distribution, and content of the notice.
- Violations may result in civil penalties, including damages, injunctions, and attorneys' fees. Violators can be subject to administrative fines from the Department of Consumer Affairs of up to $1,000 for each resident whose information was accessible based on the breach.

APPENDIX -
CYBERSECURITY AND DATA BREACH DETAILS

Contents

- Introduction to Cybersecurity & Data Breach
- Proactive Measures For Combating & Mitigating the Impact of a Data Breach
- Cyber insurance and coverage issues
- Data Breach Incident Response
  - Attorney-client privilege issues
- SEC Cybersecurity Risk and Incident Disclosure Guidance
- Effectively Working with outside vendors on cybersecurity

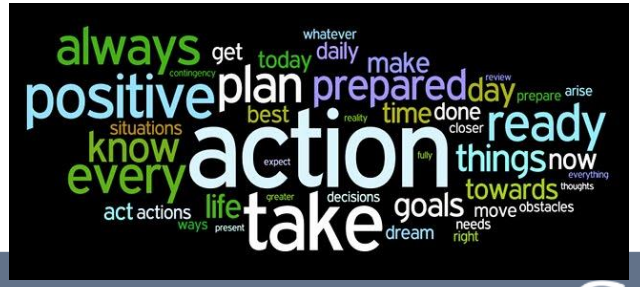
What comes to mind when we hear the term “Cybersecurity”



SHUMAKER

What is Cybersecurity?

- Cybersecurity are the measures an organization takes to protect their information technology infrastructure (computers and computer systems) from unauthorized access, attack, and vulnerabilities.
- Cybersecurity is proactive not reactive.



SHUMAKER

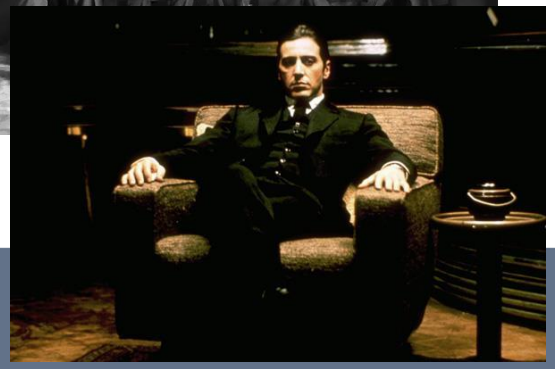
Why is Cybersecurity important?

- Cyber Warfare poses a real world threat
  - Stuxnet
  - Aurora
  - RSA
  - Equifax

Criminal Organizations and Cyber Attacks

- Crime organizations have evolved.
- Fraud generates greater revenue for organized crime organizations than trafficking narcotics.

Source: Meikle, Mike, FaaS: Fraud as a Service, InfosecIsland, Apr. 14,2010



Fraud-As-A-Service

- Underground marketplace where fraud services and goods can be purchased.
  - Malware and exploit kits
  - Distributed Denial of Service attack services
  - Account takeover services (social media, web-based email)
  - Fake documents (i.e. fake driver's licenses, social security cards, passports, etc.)
  - Zero-day Exploits

Why is Cybersecurity Important (continued)?

- Data has value
- People and organizations generate an enormous amount of data.
- Generating, collecting and storing data has risk
  - Contractual obligations (i.e. indemnification)
  - Federal law
  - State Law
  - Global privacy laws (e.g., GDRP, APEC)

Data Breach

- A data breach is the action that most often triggers an obligation or legal duty under a contract or statute.
- Generally, a data breach is defined as unauthorized access to and acquisition of data that compromises the security or confidentiality of such data.

Evolution of Data Breach

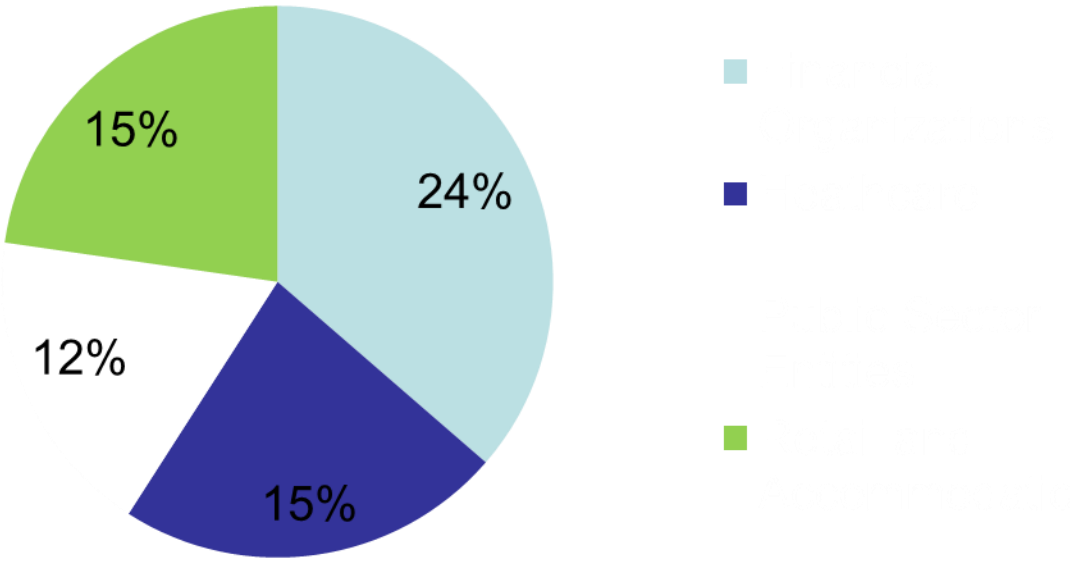
- According to the Privacy Rights Clearinghouse, there have been 7,970 data breaches made public since 2005, involving 10,082,888,054 records.
    - 2005 = 136 breaches, involving 55,101,241 records
    - 2006 = 482 breaches, involving 68,580,711 records
    - 2007 = 454 breaches, involving 141,547,907 records
    - 2008 = 354 records, involving 130,777,900 records
    - 2010 = 800 breaches , involving 140,920,891 records
    - 2016 = 815 breaches, involving 4,810,437,809 records
    - 2017 = 612 breaches, involving 1,925,957,652 records

Costs of a Data Breach

- According to the Ponemon Institute's 2017 Cost of Data Breach Study:
  - Average cost of a data breach to a company in 2017 was $3.62 million or $141 per record that was lost or stolen
  - Data breaches most expensive in the U.S. and Canada
    - Average per capital cost in the U.S. is $225 per capita.
    - Average total organizational cost in the U.S. was $7.35 million.
    - Most vulnerable industries to a data breach – financial, health and services sectors

Victims of Data Breach

- According to Verizon's 2017 Data Breach Report



Sources of and Tactics Used in Data Breaches

- According to Verizon's 2017 Data Breach Investigations Report:
  - 75% of data breaches were carried out by outsiders to the organization.
  - 25% of data breaches involved actors that were internal to the organization
  - 18% were conducted by state-affiliated actors
  - 51% involved organized criminal groups





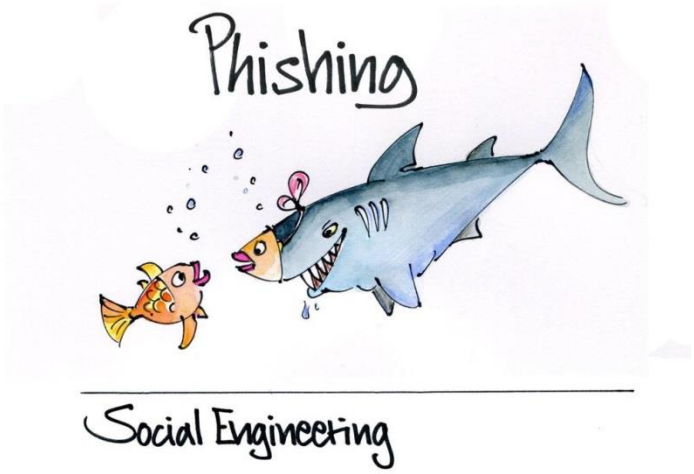
Sources of and Tactics (continued)

- Tactics
  - 62% of data breaches involved hacking
  - 51% involved malware
  - 81% of hacking-related breaches leveraged stolen and/or weak passwords to gain access.
  - 66% of malware was installed via a malicious email attachment
  - 73% were financially motivated
  - 21% of breaches were related to espionage
  - 27% of breaches discovered by third parties

Source: 2017 Verizon Data Breach Report

Who is behind these schemes?

- Hackers/hacktivists
- Phishing Attacks
- Social Engineering
- Ransomware/Malware/ Worms/Viruses
- Internal actors



What can we do to guard against threats to cybersecurity?

- Be Proactive!
- Conduct a Data Inventory
  - How is data generated in the organization?
  - Who generates or collects the data?
  - Why is the data collected?
  - How is the data used?
  - Where is the data stored?
  - How long is the data stored?

- Who has access to the data?
  - All employees?
  - Third party vendors or service providers?
- What types of information does this data contain?
  - Personal information?
  - Medical, financial or legal information?
  - Sensitive business information or intellectual property?
- Is the data backed-up or archived?
- How is the data protected (e.g., encryption, redaction)?
- Where is the data back-up stored?
- How long are back-ups kept?

Proactive Measures

- Inventory policies and procedures
  - Information governance or data retention policies
  - Employee computer and internet usage policies
    - How are employees permitted to generate and store information?
    - Are USB, flash, and DVD-writing drives enabled for employee use?
    - Do employees have off-site access to files and information?
    - Any policy prohibiting employees from using personal email accounts or emailing files to themselves to work from home?
  - Organization policies for customers or the organizational website concerning how the organization handles information

Proactive Measures (continued)

- Technical measures
  - Is your organization utilizing the latest technical measures and best practices to guard against threats?
  - Are server ports adequately closed and protected?
  - Server logs?
  - Is two or three factor authentication required to access information from outside the business?
  - How does the organization address and prioritize software patches and other vulnerabilities?
- Annual Penetration testing?
- Training employees (Social engineer, phishing, etc.)

Cyber Security Risk Insurance Coverage Issues

- Cyber Insurance Coverage Considerations
  - Insure for a wide variety of risk
  - Carriers often have panels of experienced data breach attorneys and forensic investigators
  - Always read the cyber insurance coverage carefully to see if there are any specific requirements on the organization as a prerequisite to the insurer covering an incident.

Incident Response / Data Breach Plan

- My opinion: every organization should have an Incident and Data Breach Response Plan
  - Response Team
  - Have counsel pre-selected
  - Work with counsel for a plan on the forensic investigator you're going to bring in.
  - Insurance Coverage
  - Public Relations Team
  - Call Center
  - Legal obligations
    - Law enforcement
    - Notification to Data breach victims
    - Contractual obligations

Incident Response / Data Breach Plan (continued)

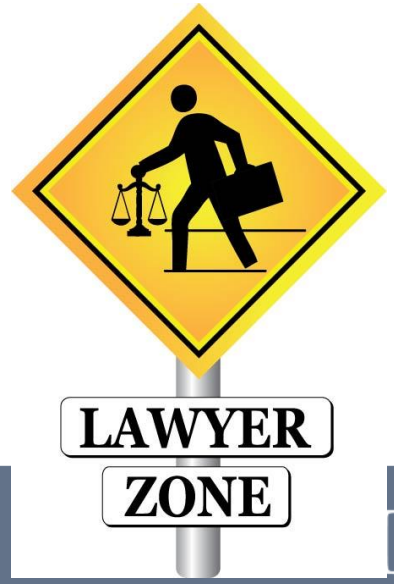
- Once you have a plan in place with defined roles and responsibilities, it is critical that the organization practice its response.
- Conduct drills on different breach scenarios.
  - Compromised email, phone system is down, etc.

A Data Breach Occurs – What Should You Expect?

- Timing
  - Not unusual for it to occur during long weekend or Corporate Holiday
- Tend to be chaotic events with tons of opportunity to make mistakes.
- Don’t forget to notify your insurer!
- Information evolves very quickly
- Discovering the breach is really just the beginning
  - State and Federal law requirements
  - Regulatory inquiries
  - Inquiries from State AG’s
  - Class Action Lawsuits

Attorney Client and Work Product Privileges in Data Breach

- Attorney-client privilege applies to:
  - Client request for legal advice from an attorney
  - Communications between client and the attorney that are necessary for the lawyer to render his or her advice in relation to the matter the attorney was employed or consulted for.
  - The lawyer's legal advice to the client



Attorney Client and Work Product Privileges (continued)

- Work Product Doctrine applies to protect documents prepared in anticipation of litigation by:
  - The client
  - The client's attorney
  - Agents and consultants for the client and attorney
  - Experts retained by the client or the attorney

Attorney Client and Work Product Privileges (continued)

- A requesting party can overcome the work product doctrine protections by showing:
  - Substantial need for the work product materials
  - That the party cannot obtain a substantial equivalent of the materials by any other means without undue hardship.
- Waiver
  - Attorney Client Privileged Communications
    - Disclosure to anyone outside the litigation team or company.
  - Work Product Doctrine
    - Typically, waiver recognized where the disclosure is to an adversary or a third party that may share the work product with an adversary.

Why do these protections matter?

- Legal counsel needs to be the one directing the investigation by the forensic examiner so that it is clear that the purpose of that investigation is for rendering legal advice to the company and preparing the company for reasonably anticipated litigation. *See Genesco, Inc. v. Visa USA, Inc.,* 302 F.R.D. 168 (M.D. Tenn. 2014).
  - Genesco GC hired Stroz Friedberg, a computer security firm, to help investigate a company data breach. In the litigation that followed, Visa sought communications that Genesco had withheld about Stroz's investigation, claiming attorney-client privilege and work product doctrine. Court upheld the privilege and work product doctrine finding the evidence supported that Genesco's GC had retained Stroz in anticipation of litigation.

Why do these protections matter? (continued)

- Consider dual track investigations
  - Ordinary Course
  - One for legal advice and in preparation for litigation.
  - *See* In Re Target (next slide)

In Re Target, 2015 WL 6777384, *1 (D. Minn. Oct. 23, 2015).

- Plaintiffs sought documents withheld by Target on the basis of attorney-client privilege and the work product doctrine.
- Plaintiff's argued privilege designations were improper on the basis that Target would have had to conduct such investigations, regardless of any investigation.
- Target argued that the investigation undertaken by their task force was at the direction of legal counsel, was not an ordinary course of business investigation, and was done for the purpose of educating target's attorneys for purposes of pending and reasonably anticipated litigation.
- The District Court upheld the privilege for the task force's investigation.

Investigation

- Once you have hired a forensic consultant and they have examined the data
- Within a couple weeks we want to be able to answer:
  - How did the breach occur?
  - How long did the breach go on?
  - Is the vulnerability fixed?
  - What information and systems were accessed or compromised?
    - Important for trying to determine the number of people impacted and any contractual obligation.
  - Idea of where the attack originated (i.e. country, within the building, same state, etc.)
  - Number of computers or hackers involved in the action

Relevant Bodies of Law

- Federal Statutory Law Considerations
  - Medical Privacy
    - Health Insurance Portability and Accountability Act (“HIPAA”)
    - Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”)
    - Genetic Information Nondiscrimination Act of 2008 (“GINA”)

Relevant Bodies of Law (continued)

- Federal Statutory Law Considerations
  - Financial Privacy
    - The Fair Credit Reporting Act
    - The Fair and Accurate Credit Transactions Act
      - The Disposal Rule
      - Red Flags Rule
    - Gramm-Leach Bliley Act
      - Privacy Rule
    - Dodd-Frank Wall Street Reform and Consumer Protection Act
    - The Federal Trade Commission Act

Relevant Bodies of Law (continued)

- State Statutory Laws
  - Data Breach Notification Laws – perspective of the resident victim
    - 48 States and 4 U.S. Territories have data breach notification laws (D.C., Guam, Puerto Rico, and Virgin Islands)
    - Alabama (legislation pending) and South Dakota don't have data breach notification laws
  - Other information protection statutes
    - About half of the states have statutes that pertain to protecting social security numbers.
  - Duty to notify law enforcement?

South Carolina Insurance Data Security Act

- Title 38, Chapter 99 of the South Carolina Code of Laws effective 1/1/2019
- Licensees must establish a comprehensive, written information security program. Section 38-99-20.
- Licensees must meet additional requirements if contracting with third-party service providers that maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.
- A licensee notify the Director no later than 72 hours after determining that a cybersecurity event has occurred when certain criteria are met.

States' Laws

- California (Civil Code 1798.28 & 1798.82)
- Connecticut (Sec. 36a-701b)
  - Broad "breach of security" definition
  - Requires "appropriate identity theft prevention services and, if applicable, identity theft migration services."
    - Services must be provided for not less than 12 months
- New York (General Business Laws § 899-aa).
  - Requires notice to affected residents for disclosures of "private information"

Relevant Bodies of Law (continued)

- Regulatory Obligations?
  - Does this breach require reporting or disclosure to a federal agency?
  - SEC Disclosure?
    - SEC Commission recently issued Guidance on Cybersecurity Disclosures for Public Companies.
- Contractual Obligations?
  - Duty to notify service providers?
  - Clients?
  - Lenders?

SEC Guidance on Cybersecurity Risks & Incidents

- Public companies need to inform investors about material cybersecurity risks and incidents in a timely fashion.
- Boards and officers need to be informed about cybersecurity risks and incidents.
- Public companies should have policies and procedures in place to:
  - Guard against directors, officers and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident and
  - Help ensure the company makes timely disclosure of any material nonpublic information.

SEC Guidance on Cybersecurity Risks & Incidents

- Public companies must
  - maintain comprehensive policies and procedures related to cybersecurity risks and incidents.
  - have disclosure controls and procedures to make accurate and timely disclosures of material events, including those concerning cybersecurity.
- Materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information on the business and scope of company operations.

SEC Guidance on Cybersecurity Risks & Incidents

- Guidance not intended to suggest disclosures that could compromise a public company's cybersecurity efforts by providing a roadmap for a potential hacker or detailing specific systems, technical information or equipment.
- Recognizes that some material facts may not be available at time of initial disclosure
  - Companies have a duty to correct and update prior disclosures to ensure they are not misleading or materially inaccurate.
  - Companies should ensure that revisiting disclosures is part of their incident response plans.
- Commission recommends that companies avoid generic cybersecurity disclosures and provide specific information useful to investors.

Working with Vendors on Cybersecurity Issues

- Fully vet your vendors and service providers
  - Vendor questionnaires
    - Information Security Program
    - Incident Response Plan
    - Number of Information Security Professionals
    - Inquiry into whether third parties provide vendor with IT services
    - Does vendor conduct background checks on employees
    - Physical, Environmental, Operational and Communications Security
    - Business continuity Disaster Recovery

Working with Vendors (continued)

- What standards does the vendor adhere to?
  - SOC2 Audit Report?
  - ISO 27001 Certification?
  - Internal and external assessment and auditing?

Contracting with Vendors/Service Providers

- Requirements for data and information security
  - No standard or duty of care in most jurisdictions for protecting data, so define it in the contract.
  - Include mechanism to ensure the service provider is checking and auditing their data security on a regular basis and certifying to you that their security standards are being adhered to.
  - Require immediate notification of a suspected or confirmed data breach.
  - Data security audit rights

Contracting with Service Providers (continued)

- Is your organization subject to the GDPR (goes into effect May 25, 2018)?
  - Wise to include provisions contemplating future GDPR accommodations in the contract; or
  - Go ahead and address the required provisions between controllers and processors for any processing of personal data, international data transfers, etc.