INTELLECTUAL PROPERTY SECURITY USING QKD: AN END TO THE EVISCERATION OF AMERICAN INTELLECTUAL PROPERTY

WAYNE PLOURDE*

ABSTRACT

This article discusses a need for added cybersecurity tools, which protect U.S. Intellectual Property ("IP"). Currently, the U.S. Government employs several disparate strategies at various agencies to combat the theft of IP. These strategies include increased Export Controls; reviews of foreign controlling interests that threaten U.S. interests at the Committee of Foreign Investment in the U.S. ("CFIUS"); stringent review of foreign Visa applications; and implementing sophisticated encryption protocols. This article focuses on the latter, implementing sophisticated encryption protocols. Starting with a Brief History of Data Theft over the centuries, including examples of Nations' response to prevent data theft and examples of successful Trade Secret/IP theft, the espionage backdrop over the centuries is presented. Entering the 21st Century, the U.S. is in a defensive position amid foreign cyber-economic campaigns, which are focused on conversion of U.S. IP. Traditionally, Secrecy Orders were designed to ensure IP in patent applications remained hidden from inquisitive foreign governments. However, from an economic perspective, the crucial need to ensure patent applications are kept secret is currently not adequately addressed by a Secrecy Order because databases may still be breached.

* 2024 graduate of the Intellectual Property LLM program at the George Washington University School of Law and CIPO at Janus-patents, https://tinyurl.com/Janus-Patents.

Because the movement of data is not addressed by current cyber security protocols, a new quantum security tool is presented. This quantum tool has a protocol that prevents the movement of data and therefore offers unparalleled cybersecurity because it prevents any electronic transfer (e.g. movement) of data. This tool could be deployed as an added layer of security to existing protocols because this tool stops movement of data; traditional protocols detect and prevent unauthorized entry into a database.

Developing a quantum infrastructure requires several U.S. agencies work together, and requires a commitment of tax dollars, to ensure implementation. Because competing nations have prioritized campaigns to dismantle U.S. technology, those campaigns could catapult their economies ahead of the U.S. economy, by orders of magnitude, in only a couple decades. Thus, implementing an extra layer of security using a new quantum tool has potential to end cyber espionage. Economically, this would safeguard our reputation as the source of the world's top technologies.

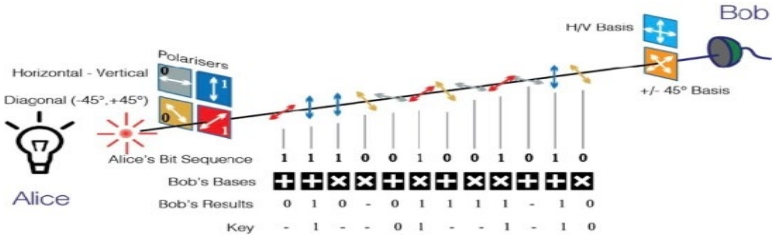
PREFACE

Intellectual Property ("IP") is in the limelight as law enforcement grapples with stopping its' theft, which is often an invisible crime. Policymakers are also diligently formulating 21st Century strategies, including Export Controls, more stringent Visa review, and other controls to safeguard the United States' status as a leader in research and a source of superior technologies. The concept of Quantum Key Distribution ("QKD") offers a way of distributing and sharing secret keys that are necessary for cryptological protocols. The protocol ensures information remains secret between the communicating parties.[1] Inventions may be kept secret until the disclosing party choses to disclose their invention to the world via a patent application. However, the disclosing party could also request *non-publication* of their patent application. A non-publication request is a deliberate strategy to keep an application secret and free from inquisitive eyes until it is granted. Notwithstanding a grant by the USPTO, when a Chief Officer of a defense agency notifies the government that publication of an invention, by the granting of its' patent, would be detrimental to national security, a Secrecy Order will be issued by the Commissioner for Patents at the USPTO.[2] This article explores a new tool, QKD, which ensures privacy of patents by restricting *data movement*. QKD is avant-garde because it focuses on any data movement to or from a secure fortress instead of just restricting entry into a data fortress. QKD may be integrated with plans such as the Zero Trust Architecture.

---

[1] *Quantum Key Distribution (QKD)*, QUANTUM FLAGSHIP, https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd [https://perma.cc/N9HQ-MJDH] (last visited Feb. 21, 2024) [hereinafter QUANTUM FLAGSHIP].

[2] Secrecy Order, 37 C.F.R. § 5.2(a) (2020).



An illustration of how QKD generates a Key.[3]

I. INTRODUCTION

> "Artificial intelligence is the future . . . .it comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world."[4]

[3] QUANTUM FLAGSHIP, *supra* note 1 ("[T]ypically, information is encoded on single photons, as shown in the photo. Alice can choose to encode these in a "bit sequence" using one of two states, like vertical (V) or horizontal (H) polarization, and she also can choose to encode in two different states; here, two combinations of these states labeled +45° and -45°. Bob then chooses to measure in one of the two, what we call bases – either he measures H,V, or he measures +45°, -45°. If he measures in a base that is different from the one Alice used to prepare, then his answer will be random and discarded, but if they chose the same one, then they will have perfectly correlated results; Alice sends H and Bob detects H, and these are kept. This last step requires Alice and Bob to communicate about which base was used but reveals no information about the result, which now becomes the secret key.").

[4] Major Johnathan J. Rudy, *"OK Google" Play the National Anthem: Arms Control and Eminent Domain to Maintain America's Technological Advantage*, 12 CASE W. RES. J.L. TECH. & INTERNET 1, 2 (2021); *Whoever leads in AI will rule the world': Putin to Russian children on Knowledge Day*, RT, https://www.rt.com/news/401731-ai-rule-world-putin/ [https://perma.cc/HVT3-8CBK] (Sep. 1, 2017).

A. Background

Less than 60 years ago the U.S. Federal government played a much greater role in technological development.[5] Because the Federal government abdicated the role of technological development to Silicon Valley,[6] the incentives have changed from viewing opportunity through the lens of national security to viewing opportunity through the lens of profit.[7] Hence, strategies to extract Intellectual Property from the sanctuary of secrecy orders, non-publication requests, or private databases will thrive in the 21st Century.

Usually, when IP was generated by the U.S. government, if an invention was determined to be detrimental to our national security, then a Chief Officer of the IP-generating defense agency requested a Secrecy Order from the U.S. Government. Secrecy Orders ensured inventions would be secret.[8] However, when for-profit entities generate new tech that attracts foreign interest, some of their business decisions, when viewed through the opportunistic lens of profit, may not focus on requesting a Secrecy Order. For instance, this could be because some profit-seeking entities are financially positioned with less cybersecurity resources. In such a scenario, a company policy mandating Secrecy Orders for sensitive tech will not be prioritized. Thus, novel security protocols should be utilized to ensure sensitive IP is always secured. This article discusses QKD as a possible solution.

---

[5] Rudy, *supra* note 4, at 18; Robert Meltz, *Takings Law Today: A Primer for the Perplexed*, 34 ECOLOGY L.Q. 307, 311 (2007).
[6] Kelo v. City of New London, Conn., 545 U.S. 469, 482 (2005).
[7] Scott Rosenburg, *Tech giants are the new gatekeepers*, AXIOS (Feb. 1, 2019), https://www.axios.com/2019/02/01/tech-giants-new-gatekeepers-1548976974 [https://web.archive.org/web/20230601171510/https://www.axios.com/2019/02/01/tech-giants-new-gatekeepers-1548976974].
[8] Secrecy Order, 37 C.F.R. § 5.2(a) (2020).

II. THE PROBLEM: THE FAILED MARRIAGE BETWEEN THE SCIENCE AND THE LAW

> In July 2019 FBI Director Christopher Wray stated, *"there is no country that poses a more severe counterintelligence threat to this country right now than China."*[9] He noted that the Bureau had around 1,000 investigations involving attempted theft of U.S. Intellectual Property ("IP"). The White House, in its 2017 National Security Strategy, also highlighted the importance of the issue. The US Trade Representative calculates that the annual cost of *'the theft of trade secrets could be as high as $600 bn/year"* not including "the full cost of patent infringement, nor the estimated $400 billion per year lost to economic espionage via cyber attacks."[10] Recommendations include strengthening the Committee on Foreign Investment in the United States (CFIUS), which was accomplished through the passage of the Foreign Investment Risk Review Modernization Act of 2018.[11]

Cybersecurity is a multi-faceted problem with failures and successes in different fields. However, in the IP arena, common tasks carry continued risks during the storage, transmission, negotiation, and selective dissemination of IP. It has been argued that the Committee on Foreign Investment in the United States ("CFIUS")

---

[9] MARTIJN RASSER ET AL., THE AMERICAN AI CENTURY: A BLUEPRINT FOR ACTION 20 (2019); Agence France-Presse, *FBI has 1,000 investigations into Chinese intellectual property theft, director Christoper Wray says, calling China the most severe counter-intelligence threat to US*, SOUTH CHINA MORNING POST (July 24, 2019), https://www.scmp.com/news/china/article/3019829/fbi-has-1000-probes-chinese-intellectual-property-theft-director [https://perma.cc/X698-9RTN].

[10] RASSER ET AL., *supra* note 9; *The Theft of American Intellectual Property: Reassessments of the Challenge and United State Policy*, IP COMMISSION REPORT UPDATE (Feb. 2017).

[11] RASSER ET AL., *supra* note 9.

carries the responsibility to reduce this risk. In fact, recent Acts[12] have strengthened CFIUS.

This article parallels recommendations to strengthen CFIUS. This article focuses on cyberattacks that are organized with the aim to steal U.S. intellectual property, and this article proposes a new solution that can be integrated with evolving cybersecurity maturity models to reduce successful cyberattacks. This risk to IP theft could be reframed from a timeline perspective of data theft. Ultimately, by integrating recent quantum advances, agencies can complement their existing advanced cybersecurity models and thereby deploy cybersecurity models which are more responsive to evolving threats. The increased security realized from this evolving security model would be expected to reduce the risk of IP theft during the storage, communication, transmission, negotiation, and selective dissemination of our IP.

A. The Science Exists and the Law is Lacking

The tools, processes, and practices required to meaningfully enhance the integrity of Internet and communications security are widely available and, in fact, are routinely applied in selected sectors of our world. However, they are not common practice for "development and deployment in many other sectors for many reasons, including lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives."[13] These

[12] Foreign Investment Risk Review Modernization Act of 2018, H.R. 5841, 115th Cong. (2018).

[13] LEON REZNIK, INTELLIGENT SECURITY SYSTEMS: HOW ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA SCIENCE WORK FOR AND AGAINST COMPUTER SECURITY, §1.1, 3 (Ekram Hossain et al. eds., Wiley 2022).

deficiencies provide a wealth of opportunity, creating a hacker's paradise.[14]

When actual identity theft or fraudulent charges result from a data breach, some courts find injury is in fact satisfied. "Courts disagree, however, on whether increased risk of identity theft alone can satisfy the injury in fact requirement."[15] The Federal Cybersecurity Enhancement Act of 2015 ("FCEA") requires the Secretary of Homeland Security and the Director of the OMB to create a method to detect intruders in federal systems.[16] However, at the point where we are "detecting intruders in federal systems," it is already too late. Data breaches occur at incredibly fast speeds because the data is in the form of electrons which are traveling on wires (or traveling via radio waves wirelessly on its way to hitch a ride on a wire). But it is important to note, wireless radio waves and wired communications are both forms of electromagnetic radiation. This means that it is possible for communications to travel at the speed of light because electromagnetic radiation travels at this speed. The speed of light is an astonishing $3.00x10^8$ m/s or, in plain language, 671,000,000 miles per hour.

Since data breaches also occur at 671 million miles per hour, this should inform those who are making new law. Gone are the days of capturing a chattel in hot pursuit. Data is, at the instant it is breached, converted by its mere existence on the remote device of the intruder. The data breach occurs at the speed of light. However, current laws were not created with recapture of data in mind because

---

[14] *Id.*

[15] Hannah Vail, *Cybersecurity Reform in the Wake of the OPM Breach*, 50 SUFFOLK UNIV. L. REV. 221, 227 (2017).

[16] *Id*. at 231; Cybersecurity Act of 2015, H.R. 2029, 114th Cong. § N (stemming from the proposed Cybersecurity Information Sharing Act ("CISA") and Federal Cybersecurity Enhancement Act of 2015 (FCEA), which are collectively referred to as the "Cybersecurity Act,"; S.754 is the current state of the law for Cybersecurity Law) [hereinafter *S.754*].

horses run faster than thieves of old could convert a chattel. Thus, recapture on the American Frontier was possible and recapture laws on the American Frontier were fit for purpose.

Given the massive difference in the speed of conversion during a data breach, existing laws that were designed to aid in the recapture of a stolen chattel—a chattel moving away on a horse or a train to reach fateful conversion—are not suitably aligned to recapture stolen data today. The conversion of stolen data is at the speed of the breach. As these unwanted breaches occur at the speed of light, their conversion cannot be undone.[17] Recapture of the stolen data becomes more difficult because transfer, utilization, duplication, and transfer of the data (for later manipulation) are all likewise made at the speed of light. Thus, sensitive data should never be in the hands of an intruder—not for an attosecond.[18] Assuming they can move

[17] At the time of this writing, we are not yet able to travel at the speed of light.

[18] An attosecond is a fraction of a second; it is exactly 1×10^{-18} of a second. The "attosecond" is used here to provide a scientific analogy. Today, the success of cyber theft is *not dependent how much time* they have to commit the crime. Rather, successful cyber theft depends on whether a thief can *move* the data. In a single attosecond of possessing stolen data, it can be shown mathematically that a thief traveling at the speed of light (671,000,000 mph) would only be able to *move* his packet of stolen data a mere 0.3 nanometers, which is an imperceivable distance. This scientific analogy is provided to illustrate the extreme speed of data theft cybersecurity professionals are dealing with when they contemplate solutions that are adequate given the ultra-fast speed at which the data breaches are occurring. The extra layer of security provided by QKD is extraordinary because the time afforded to cyber thieves of today is no longer relevant to their success. This is because regardless of whether cyber thieves have an attosecond or an eternity to plan their getaway, applying QKD principles will bind data thieves by scientific laws of quantum physics. A quantum restriction ensures that the *distance* they travel with the packet of stolen data will always be *zero*. QKD allows cybersecurity professionals to operate *Independent of Time*. If coupled with the currently available state-of-the-art protocols that detect and

the data, intruders instantaneously have what they need once they are inside our systems. With a data breach, intruders no longer need time to make photos, develop the film in a darkroom, contact their handler, and have the operational officer send the stolen asset back to base. The efforts of cyber-attackers seeking to steal data today are not time dependent and we cannot recapture stolen data after the data is moved outside of our systems.[19] Thus, removing their dependency on time—whether the defending agency is able to respond within the breakout window—would be an invaluable advance in their defense arsenal.

Because many systems are already capable of preventing an attack before a meaningful compromise occurs (e.g. Zero Trust Architectures "ZTA"),[20] emerging

---

prevent breaches (e.g. Zero Trust), QKD offers a superior gloss. Thus, QKD compliments existing advances and thereby affords a gigantic leap forward in cybersecurity.

[19] *See 2023 Global Threat Report*, CROWDSTRIKE (2023), https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf [https://perma.cc/9DNY-KLJR] (advocating that time-to-response to a cyberthreat incident is critical to reduce cost and damage: "The average breakout time for interactive eCrime intrusion activity declined from 98 minutes in 2021 to 84 minutes in 2022. Thus, defenders can minimize cost and damage by responding within the breakout time window.").

[20] SCOTT ROSE ET AL., *Zero Trust Architecture*, NAT'L INST. OF STANDARDS AND TECH. (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [https://perma.cc/NA28-W6FE] (the National Institute of Standards and Technology ("NIST") Special Publication ("SP") provides the following Zero Trust and ZTA definition: "***ZTA*** *provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.* ***ZTA*** *is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a Zero Trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan*.").

cybersecurity measures should be integrated as appropriate to agencies dealing with IP data. Integration reduces the risk that an agency's sensitive IP data might be compromised. Improving our national cybersecurity is viewed under Zero Trust Models as an evolution, "one of many paths," that should be "specifically tailored for federal agencies as required by EO 14028."[21] Thus, emerging infrastructure and cybersecurity measures could be interwoven with the Zero Trust cybersecurity models to provide specific cybersecurity tailoring that IP agencies require. Strengthening cyberattack countermeasures, would therefore make asportation of IP data more difficult. This extra layer of security, integrated with an agency's evolving ZTA, would complement existing cybersecurity efforts that are already aimed at *detection* and *prevention.* This match would therefore provide an enhanced degree of certainty that, for example, sensitive IP patent applications or Secrecy Orders are not moved from the secure fortress of the USPTO. However, in the absence of an integration, notwithstanding noble efforts to modernize the law, current cybersecurity laws are deficient.

III. CURRENT GOVERNMENT PROTOCOLS (GUARD PROTOCOLS & ATTACK PROTOCOLS)

> "We already know many of the steps necessary to reduce the likelihood of a cyber 9/11, yet many of these actions have not yet been taken in either the government or in the private sector."[22]

[21] Exec. Order No. 14,028, 86 Fed. Reg. 26633 (May 17, 2021); *Zero Trust Maturity Model*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Apr. 2023), https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf [https://perma.cc/VWT6-BP2V].

[22] Vail, *supra* note 15, at 221 (citation omitted).

A. Guard Protocols

1. How nations prevent hacking, piracy, and theft of Intellectual Property ("IP").

Throughout history, it was common to observe statutes changing with the needs of society. Later sections of this article, *WHY IT MATTERS TO THE LAW* and *PROPOSED SOLUTIONS,* will further discuss changes in technology and policy currently needed to keep pace with today's cyber threats.

Currently, IP theft cases are prosecuted in the U.S. under IP statutes.[23] For example, a new 2023 law aiming to prevent the theft of trade secrets provides that the "President may, pursuant to the International Emergency Economic Powers Act, block and prohibit all transactions in all property, (50 U.S.C. 1701 et seq.)" among other sanctions.[24] Older laws also provide punishment.[25] But, like the 2023 law,[26] the older laws similarly cannot undo the economic harm to the U.S. because at the point when these sanctions are imposed, the trade secret is out of the bottle and cannot be put back in. Sanctions cannot undo a conversion of IP. Consequently, the problem is not a lack of devoting proper

[23] *E.g.*, 18 U.S.C. § 2318 (covering the trafficking in of counterfeit labels, illicit labels, or counterfeit documentation or packaging); 18 U.S.C. § 2319 (covering criminal infringement of a copyright); 18 U.S.C. § 2320 (covering the trafficking in of counterfeit goods or services); and Protecting American Intellectual Property Act of 2022, Pub. L. No. 117–336, 136 Stat 6147 (2023) (codified at 50 U.S.C. §1709). For additional discussion on IP statutes dealing with IP theft see Arnold Reisman, *Illegal Transfer of Technologies: A Taxonomic View* 5–15 (Apr. 30, 2004), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=532522 [https://perma.cc/6EE5-S54X].

[24] Protecting American Intellectual Property Act of 2022, Pub. L. No. 117–336, 136 Stat 6147 (2023) (codified at 50 U.S.C. §1709).

[25] *See*, *e.g.*, 18 U.S.C. §§ 2318–20.

[26] 50 U.S.C §§ 1701, 1709.

resources to cybersecurity, it is that defenders are not successful in combating IP theft of patent applications and other confidential IP data.

In fact, there are international and multinational efforts to stop physical or cyber theft of IP. For example, there are trade associations whose mission is to preempt theft of IP. These associations include the Business Software Alliance ("BSA"), the International Anti-Counterfeiting Coalition ("IACC"), and others.[27] However, these trade associations are presently losing pace with the rapid onslaught of today's cyber threats. By comparing recent comments related to existing IP cyber threats to the trade associations' original stated goal of preempting theft of IP, an inference could be drawn which suggests their stated goals are losing ground because of the explosion of web platforms.[28] Web platforms often provide fertile ground for the proliferation of counterfeit products.[29] For example, comments provided by IACC illustrate the extreme difficulty faced by the trade associations in keeping pace with mounting cyber threats.[30] Specifically, some trade

---

[27] *See* Reisman, *supra* note 23, at 14.

[28] *See* 2020 Review of Notorious Markets for Counterfeiting and Piracy: Comment Request, 85 Fed. Reg. 62006 (Oct. 1, 2020).

[29] American Apparel & Footwear Association, Comment on 2020 Review of Notorious Markets for Counterfeiting and Piracy: Comment Request, 11 (Nov. 9, 2020) https://www.regulations.gov /comment/USTR-2020-0035-0002 ("counterfeiters knowingly use the platform to hide behind privacy regulations.").

[30] International Anti-Counterfeiting Coalition, Comment on 2020 Review of Notorious Markets for Counterfeiting and Piracy: Comment Request, 16 (Nov. 9, 2020) https://www.regulations.gov /comment/USTR-2020-0035-0010, [https://perma.cc/6YKL-2F4T] (arguing that penalties are "insufficient to serve as any real deterrent"); *see also* Union des Fabricantes, Comment on 2020 Review of Notorious Markets for Counterfeiting and Piracy: Comment Request, 23 (Nov. 9, 2020), https://www.regulations.gov/comment/USTR-2020-0035-0004 [https://perma.cc/M4RM-YVL5] (stating that user restrictions are "minimal and unlikely to serve as a deterrent to infringement")).

associations implied that Tencent Holdings Limited, the Chinese holding company for the web messaging platform "WeChat," is a company "engaging in and facilitating substantial copyright piracy or trademark counterfeiting." [31] These IP concerns hit home when one further considers foreign efforts to convert novel U.S. technology that is developed and commercialized domestically.[32]

Thus, while great strides in *detection* and *prevention* of breaches have been made, progress can be made by eliminating cybercriminals' ability to *move* stolen IP for exploitation in the future.

2. How the USA currently guards against data breaches.

Toolboxes used to stop Foreign States from transferring U.S. Technologies

Presently, CFIUS, export controls, and scrutiny of visas are the three most utilized tools by the U.S. Government to impede the transfer of technology to States where it is believed the tech would lead to undesirable outcomes. These tools are described in Appendix III.[33] Unfortunately, regardless of the availability of these tools, China's efforts in both industrial espionage and cyber-attacks are ramping up in the face of an uninspiring U.S. response, which includes a dire need for additional programs

---

[31] International Anti-Counterfeiting Coalition, Comment on 2020 Review of Notorious Markets for Counterfeiting and Piracy: Comment Request, 16 (Nov. 9, 2020) https://www.regulations.gov /comment/USTR-2020-0035-0010, [https://perma.cc/6YKL-2F4T] (arguing that penalties are "insufficient to serve as any real deterrent"); *see also* Union des Fabricantes, Comment on 2020 Review of Notorious Markets for Counterfeiting and Piracy: Comment Request, 23 (Nov. 9, 2020), https://www.regulations.gov/comment/USTR-2020-0035-0004 [https://perma.cc/M4RM-YVL5] (stating that user restrictions are "minimal and unlikely to serve as a deterrent to infringement")).

[32] *See infra*, Section III.C.1: *Attack Protocols*: China's efforts to capture U.S. technology.

[33] *See infra* Appendix III.

and added manpower to the existing programs. The result: exponential growth of the transfer of U.S. technologies to China.[34]

B. Efficacy of CFIUS

CFIUS works in concert with fourteen U.S. Agencies, including three Security Agencies (DOD, DOJ, and DHS) and, among several others, the most notable non-security Agencies are the White House, the Secretaries of Defense, Treasury, Commerce, and the Attorney General.[35] Noteworthy, however, is that these different agencies are not tasked to collaborate in identifying sensitive technologies and facilities.[36] Because the U.S. does not have an interagency strategy, and private companies often lack the depth of resources needed to handle the complexity of trade compliance, current Chinese cyber targets are likely well outside the scope of our radar.

There are current attempts to expand CFIUS' reach under Foreign Investment Risk Review Modernization Act ("FIRMA") legislation.[37] However, Congress has not dedicated additional funding for critical CFIUS reviews, and this means all critical reviews must be handled within the current budgets of the various Agencies.[38] Furthermore, in combination with this lack of dedicated Congressional funds, CFIUS critical reviews are surpassing more than 150 critical reviews each year.[39] Thus, CFIUS resources are already stretched to the limit in these Agencies.

---

[34] Michael Brown & Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, DEFENSE INNOVATION UNIT EXPERIMENTAL (DIUX) 14, 15 (Jan. 2018).
[35] *Id.* at 23.
[36] *Id.* at 43.
[37] *Id.* at 23.
[38] Brown & Singh, *supra* note 34, at 23.
[39] *Id.*

If modernization is to occur to ensure that CFIUS is an effective stop gate—allowing the U.S. to keep up with ever increasing foreign offensives to pirate US IP via a multitude of methods—then Congress must increase dedicated funding for critical CFIUS reviews.[40] Also important in this transition to modernize our efforts would be to ensure an interagency strategy. An interagency strategy is critical to introduce a concerted defense effort that provides both a comprehensive view of the technology landscape,[41] and an end to the asportation of our rich IP.[42]

C. Attack Protocols

1. China's efforts to capture U.S. technology.

Theft of intellectual property ("IP") can be carried out under the auspices of sophisticated technology transfer strategies, which may appear legal on the surface. Illicit transfer can employ multiple strategies, including "a network of naïve or sophisticated and/or deranged individuals who may or may not be enabled by governments of a sovereign state, a corporation or some institution."[43] Illegal transfer of technology may be carried out "for a host of reasons or motivations ranging from recreation to terrorism. The theft can involve hardware, software, or any other form of IP. It can take place via downloading, copying, reverse engineering, or espionage."[44] "It can breach

[40] *See infra* section titled "*Attack Protocols*: China's efforts to capture U.S. technology" (describing a variety of technology transfer vehicles used by China to transfer U.S. technologies via eight *offensive strategies* into Chinese commerce).
[41] Brown & Singh, *supra* note 34, at 43.
[42] *See infra* Section III.C.A.1.a "How China transfers Technology: 8 Vehicles for asportation of USA's IP Jewels."
[43] Reisman, supra note 23, at 15.
[44] *Id*.

contracts, trade secrets, national and international laws involving patents or copyrights."[45] This is the subject of concern for many Academic and Corporate entities and Government Agencies from law enforcement, policy making, intelligence, and counterintelligence.[46] Their efforts are entirely disconcerted at the time of the writing of this article.

a. How China transfers Technology: 8 Vehicles for asportation of USA's IP

China has eight principal resources for technology transfer in addition to various other investment and acquisition methods it employs.[47] Investment and acquisition methods are beyond the scope of this article. Of the eight principal technology transfer strategies used by China, only the eighth resource, which is *Cyber Theft*, will be discussed in this article. For a brief discussion of China's other seven principal resources for illicit technology transfer, see Appendix IV.[48]

Cyber Theft:[49] China is ahead of all other players in cyber-attacks simply because of the utter scale of their activity. For example, China dedicates a massive army to its global activities, which, according to U.S. FBI intelligence, includes 250,000 to 300,000 soldiers in the People's Liberation Army ("3PLA") dedicated to cyber espionage. This is in addition to another 30,000-50,000 spies in the U.S. working on insider Ops. Much of this effort is deployed in support of China's economic goals to steal valuable IP to

[45] *Id*.
[46] *Id*.
[47] Brown & Singh, *supra* note 34, at 16–22.
[48] *See infra* Appendix IV of this article, which details another 7 principal resources used by China to transfer Technology away from the USA.
[49] Brown & Singh, *supra* note 34, at 17–18; *see also id.*, at 39–40 (App. 8).

support China's Technology Transfer agenda.[50] China's cyber capabilities are the strongest on the planet, and it owes much of this success to the fact that the U.S. system for protecting loss of this kind is rife with vulnerabilities.[51] Examples of the loss from cyber theft, including IP theft, include:[52]

- U.S. companies losing $250 billion per year in IP theft and another $114 billion per year due to monitoring and prevention of cybercrimes.[53]
- 96% of the world's cyber espionage originates in China.[54]
- $100Bn is lost in sales, and 2.1 million jobs are lost due to this theft.[55]

Cyber Theft is the heart of this article. *Why [Cyber Theft] Matters to the Law* is presented in § V, and *Proposed Solutions* to this exponentially growing problem is discussed in § VI. For an overview of recent IP theft and related sophisticated cyber-attacks, see Table 1 below.

[50] *Id*. at 17–18, (citing Joshua Philipp, *Rash of China Spy Cases Shows a Silent National Emergency*, THE EPOCH TIMES (Apr. 25, 2016), https://www.theepochtimes.com/article/china-security-rash-of-chinese-spy-cases-shows-a-silent-national-emergency-2038850 [https://perma.cc/B57Z-ZNKZ].
[51] *Id.* at 17–18.
[52] *Id*. at 17–18.
[53] *Id.*
[54] Brown & Singh, *supra* note 34, at 17–18
[55] *Id.*

Table 1: Eight Examples of Chinese Cyber-Attacks,[56] Providing an Overview of China's Most Significant Cyber-Attacks[57]		
Year of Breach	Trade Secret, Design, or PII taken	Footnote
2003	Coordinated attacks on government computers, starting in 2003: "Titan Rain."	[58]
October 2006	The Commerce Department's Bureau of Industry and Security – attack on export licenses for technology items bound for China.	[59]
2009+	"Hidden Lynx" has a long history of attacking defense, tech, and finance sectors of the West with unprecedented high levels of sophistication.	[60]
January 2010	PLA Unit 61398 penetrated networks of hundreds of blue-	[61]

[56] *See* Brown & Singh, *supra* note 34, at 39–40 (App. 8).
[57] *Id.* at 39.
[58] *Id*.
[59] *Id*. at 40.
[60] *Id*. at 39.
[61] *See* Brown & Singh, *supra* note 34, at 39.

	chip companies in the following industries: aerospace, satellite, telecom, and IT.	
2011-2012	DHS found that 23 gas pipeline companies were targets of cyber hacks, which stole information used for sabotage purposes.	[62]
February 2012	This breach took more than two dozen major weapons system designs.	[63]
2015	Chinese hackers attached U.S. hosting site GitHub.	[64]
April 2014/2015	Breach of U.S. Office of Personal Management ("OPM") took 21.5 million security clearances as well as 4.2 million former and current government	[65]

[62] *Id*.
[63] *Id*.
[64] *Id*.
[65] *See infra* Section IV.B; *see also* Brown & Singh, *supra* note 34, at 40.

	employee personnel files.	

IV. A BRIEF HISTORY OF DATA THEFT OVER THE CENTURIES[66]

The Great Byzantine Silkworm Heist was led by Emperor Justinian. The medieval Byzantine Empire was well known for its production and use of luxurious silk, but until the mid-6th century, Byzantine artisans were forced to import raw silk from China.[67]

A review of the history of data theft, including several examples of Trade Secret theft, illustrates that there are many such examples over the centuries. Given the fact that thieves can walk off with the crown jewels of prominent innovators, adding greater security to existing cybersecurity protocols currently protecting U.S. Intellectual Property would be advantageous. The United States is currently positioned to reduce additional cyberattacks, yet some advanced techniques are not readily deployed.[68] The examples in this section, including "Private Sector Data

[66] *See infra* Appendix I.

[67] The Histories, *How Byzantine Monks Stole Silkworms From China*, YOUTUBE (Oct. 8, 2022), https://www.youtube.com/watch?app=desktop&v=NeqBTUFcU80 [https://perma.cc/H3QD-2ZMH].

[68] Vail, *supra* note 15, at 236 (*quoting* Jennifer Steinhauer, *Cybersecurity Bill Is Latest to Be Delayed in Senate*, N.Y. TIMES (Aug. 5, 2015), https://www.nytimes.com/2015/08/06/us/politics/cybersecurity-bill-is-latest-to-be-delayed-in-senate.html [https://perma.cc/N3BB-JWSE] (*quoting* U.S. Senator Susan Collins)).

Theft," "Government Sector Data Theft," and those provided in Appendix I, would seem trivial in comparison to a concerted cyberattack, which could play out by nefarious governments seeking to take regular snapshots of the United States' entire database of IP, which is confidential and sheltered at the USPTO. When cyberattacks occur, deciding how to prevent future hacks should not be done in hindsight. Instead of focusing on preventing *entry* to the database fortress, arresting any *movement* of data out of its fortress should be the goal.

A. Private Sector Data Theft: PII

Today it is common to hear on the news that your Personal Identifying Information ("PII") may have been breached. With the ubiquitous nature of cybersecurity incidents in the world today, it is not uncommon to receive notifications in the mail alerting you to the extent of said breaches of your PII.[69] The remedy offered in all recent cases of PII breaches is Identity Theft Protection ("ITP"). Banks, hospitals, and other defendants that are sued for violations of the Privacy Act and failure to comply with the Privacy Act resulting in damages from these breaches, customarily offer ITP after the fact by providing "*complimentary*" credit monitoring and identity restoration.[70] While this remedy is unacceptable and in the aggregate, the endless barrage of personal data breaches cost

[69] *See infra* Appendix VI (*e.g.,* the *GAFG Letter Proving Notice of "Cybersecurity Incident,"* which notified the individual of a data breach incident involving their PII and the *PBI Letter Offering "Credit Monitoring & Identity Restoration*," which offered "complimentary" monitoring as a remedy for a breach of an individual's PII [hereinafter *The PBI Letter*]).

[70] The *PBI Letter Offering "Credit Monitoring & Identity Restoration"* shows exemplary language where PBI offers "*complimentary*" ITP as follows: "*PBI is offering you access to 24 months of complimentary credit monitoring and identity restoration services through Kroll.*" *Id.*

U.S. citizens untold loss, frustration, and anxiety, this article aims to amplify the current spotlight on cyberattacks, which are breaching U.S. databases with ever-increasing sophistication and frequency. A well-known example in recent history is the Office of Personnel Management's ("OPM") Breach of 2015, which is described in the next section. While this breach did not target IP, the OPM breach gives a worrisome glimpse into the sophistication and extent of damage that could be lurking if U.S. IP databases were also targeted.[71]

B. Government Sector Data Theft: The 2015 OPM Breach

The OPM's breach of Personal Identifying Information ("PII") in 2015 is the most notable of cyber-attacks launched on a U.S. government database in recent memory. This event was a series of breaches, which collectively exposed 21.5 million federal employees' PII, including sensitive PII such as social security numbers.[72] It is believed this breach was attributed to Chinese hackers.[73] In relatively recent years, identical cyber-attacks, each of which gathers millions of individuals' PII, have occurred with increasing frequency.[74] Thus, the series of OPM breaches and the increasing frequency of these breaches serve to stress an alarming trend—the federal government's

---

[71] IP theft is commonplace throughout history—Appendix I provides several examples that span back to ancient times. *See infra* Appendix I. Thus, the OPM breach gives a glimpse into the sophistication and extent of damage that could lurk if U.S. IP databases were to be targeted.

[72] Vail, *supra* note 15, at 221.

[73] *Id.*

[74] *Id.* (citing Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUMBIA BUS. L. REV. 613, 615 (2015) (noting *explosion of recent data security breaches* and resulting boardroom pressure from regulators and plaintiffs) (emphasis added).

vigilance in protecting data is utterly lax, leading to cybersecurity incidents that should have been avoided *ab initio*.[75] In fact, "[a]n OPM computer systems audit occurring prior to the OPM breach unveiled alarming security failings."[76]

There have been several attempts in recent history to enact legislation and regulations to shore up the integrity of data.[77] However, given ongoing breaches of data and the observed tiny effect of recently enacted legislation and regulations, it should be concluded that these recent attempts are futile in stopping breaches. Thus, it is clear there is an existing need for new legal infrastructure. When it comes to stopping foreign states from accessing the United States' data, especially confidential IP data, agencies and parties to an IP license require a reliable IP data fortress. This fortress should provide impenetrable encrypted communications. For example, the following communications need to be secure: transfer of IP data to and from USPTO during prosecution of patent applications; secrecy agreements and non-publication requests must be secured for many years; and, during license negotiations, multiple parties need to securely inspect and transfer confidential data (e.g. the

[75] Vail, *supra* note 15, at 221–22.

[76] *Id.* at 222; *see also* U.S. OFF. OF PERS. MGMT., OFF. OF THE INSPECTOR GEN., OFF. OF AUDITS, REP. NO. 4A-CI-00-14-016, FINAL AUDIT REP.: FED. INFO. SEC. MGMT. ACT AUDIT FY 2014 (2014), [hereinafter Final Audit Report 2014] (recounting years of OPM's informational security weaknesses); Derek Major, *After the OPM breach: ripple effects and lingering questions*, GCN (Sept. 18, 2015), [http://perma.cc/SPK4-VBKK] (revealing OPM breach resulted from stolen vendor credentials).

[77] Vail, *supra note* 15, at 224; *see, e.g.*, The Federal Information Security Management Act of 2002 (FISMA), 40 U.S.C. § 11331; 44 U.S.C. § 3551(1) (describing the purpose of the 2014 amendment to FISA). *See generally* Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 19, 2013) (outlining President Obama's approach to protecting critical infrastructure); National Cybersecurity Protection Act of 2014, 6 U.S.C. § 659.

selective dissemination of IP data to restricted audiences during license negotiations).

C. Government and Private Sector IP Theft: Attempted or Successful IP theft & conversion

In early 2022, Slippy Spider carried out a series of high-profile data theft and ransomware incidents targeting large technology companies, including Microsoft, Nvidia, Okta, and Samsung.[78] Slippy Spider used social media "to leak data including victim *source code*, employee credentials and PII."[79] This heist captured *source code* and such activity certainly falls under the auspices of IP theft.

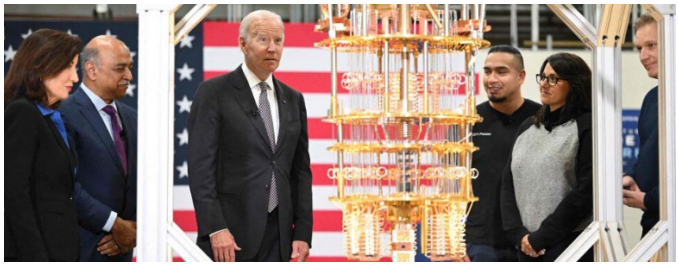
Also in 2022, China-nexus adversaries targeted nearly forty global industry sectors and twenty different geographic regions. "These intrusions were likely intended to collect strategic intelligence, compromise *intellectual property* and further the surveillance of targeted groups, all of which are key Chinese Communist Party (CCP) intelligence goals."[80] These intrusions compromised *IP* and such activity again falls under the umbrella of IP conversion.

Finally, in the countries neighboring China, "[t]echnology entities face ongoing economic espionage campaigns targeting research and development data, proprietary information and *trade secrets*."[81] These persistent economic campaigns targeted *trade secrets* and such activity is categorized as IP theft.

[78] CrowdStrike, *supra* note 19, at 12.
[79] *Id.* (emphasis added).
[80] *Id*. at 25 (emphasis added).
[81] *Id.* (emphasis added).

Several additional examples of IP theft in both private and government sectors are briefed and provided in an appendix to this article.[82]

V. WHY IT MATTERS TO THE LAW



President Joe Biden looks at a quantum computer as he tours the IBM facility in Poughkeepsie, NY, on October 6th, 2022.[83]

A. Application of the Law

Manipulation of economic control and superiority by way of devious methods of technology transfer is outright theft or conversion of IP. Such schemes are prohibited by U.S. law and the World Trade Organization ("WTO").[84] Recent testimony before the U.S.–China Economic and Security Review Commission indicates that applicable

[82] *See infra* Appendix I. The six briefs in Appendix I that are specifically trade secret theft, or another form of IP theft, are examples A, C, D, E, F, and G. However, briefs B and H are not IP theft *per se*.

[83] Mandel Ngan/AFP via Getty Images, Photograph of President Joe Biden looking at a quantum computer as he tours the IBM facility in Poughkeepsie, *in* Andrea Vittorio, *Quantum Computer Strides Spur Cyber Defenders to Prep for 'Y2Q'*, BLOOMBERG LAW (Jan. 23, 2023), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/XF2C2JO000000?bna_news_filter=privacy-and-data-security#jcite [https://perma.cc/A5PP-G632].

[84] *Chinese Investment in the United States: Impacts and Issues for Policy Makers: Hearing Before the U.S.-China Econ. and Sec. Rev. Comm'n*, 115th Cong. 42 (2017) (Statement of Jeff Johnson, President and CEO, SquirrelWerkz) [hereinafter Statement of Jeff Johnson].

WTO law includes: (1)Annex 1, §17, Barriers-to-Entry; (2) Annex 1, §19, Anti-Dumping; and (3) Annex 1, §24, Subsidies & Countervailing Measures.[85]

However, it may be that this body of law may not have any teeth—or, at least, WTO law is not applied appropriately. With no serious repercussions to evading the law, rogue states are free to launch cyber-economic campaigns that appear at first glance to be docile, but this is merely because their objectives "extend well beyond western norms, and in many cases, our imagination."[86] In fact, their economic objectives are part of "a much bigger, and more complex, strategic mosaic. . . 'a Pandora's Box.'"[87] This colossal strategy is so complex that it "discourage[s] us all from fixing it."[88] Thus, by launching a complex cyber economic campaign, certain foreign states hope to create "conditions of hopelessness,"[89] ushering in an era of economic dystopia to the future of the U.S. economy, and which is expected to cultivate an attitude of the United States "submitting" to its economic adversaries "without firing a shot."[90] Because some foreign states prefer that the United States "accept the hopelessness. . .and just enjoy the opium of foreign investment,"[91] Johnson recommends a two-part strategy to halt opening this "Pandora's Box" of China's cyber-economic campaign.[92] A two-part strategic solution was summarized during Testimony before the U.S.–China Economic and Security Review Commission, which was summarized as follows: (1) Enhancing current laws and regulations to address cyber-economic threats, as well as

---

[85] *Id.*
[86] *Id.* at 45.
[87] *Id.*
[88] *Id.*
[89] Statement of Jeff Johnson, *supra* note 84, at 45.
[90] *Id.*
[91] *Id.* at 47.
[92] *Id.*

drafting *new* laws and regulations; and (2) Enhancing the United States' command-and-control structure to address cyber-enabled economic campaigns designed to convert U.S. IP.[93]

B. International laws are evaded: At first glance these examples appear to be low risk; alternatively, some examples are long-term strategies, which are carried out under the auspices of legitimate, foreign governmental law.

The acts committed by foreign states often appear to be low risk. However, the consequences unfolding from these acts illustrate that when foreign states execute the full scope of their complex strategy, the result, in hindsight, would have categorized the original act as high-risk. For example, China's strategic campaign entails a complex web of goals which include: (1) gaining vast U.S. political influence, (2) acquiring increased control over U.S. infrastructure, and (3) harvesting U.S. technology secrets via the transfer of U.S. IP—all of which is designed to eventually benefit their stature among the world's economic elite and control of the U.S. economy.[94]

If this campaign were "understood by U.S. oversight organizations such as CFIUS, [then this would] help shed light on the risk of certain foreign led investments and acquisition efforts that appear to be low risk."[95] Put differently, many of these acts are carried out successfully because they do not appear to portray risky acts that might be perceived as "economic warfare." Thus, these acts are effectively evading the law and, given the application of this cyber-economic campaign is yielding exponential results,

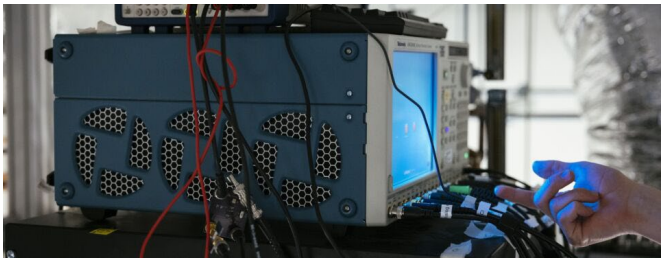
[93] *Id.*
[94] Statement of Jeff Johnson, *supra* note 84, at 45–59.
[95] *Id.* at 53.

these acts need to be stopped before we reach a tipping point.[96] A few examples of seemingly unassuming and low risk acts are described in Appendix V.[97]

C. Economic impact: What are the observed results of these economic campaigns?

It is outside the scope of this article to go into the depths of the resultant economic impacts of the foreign state cybersecurity campaigns aimed at converting U.S. Intellectual Property. For a discussion on these economic impacts see the testimony of Jeffrey Z. Johnson, which provides an exhausted overview of emerging threats and the economic results.[98]

VI. PROPOSED SOLUTIONS



An arbitrary waveform generator at a quantum computing lab inside the University of Chicago's Eckhardt Research Center in Chicago.[99]

---

[96] *Id.* at 47.

[97] *See* Appendix V of this article because the listed sources show foreign States' strategies to (1) gain U.S. political influence, (2) acquire control over U.S. infrastructure, and (3) harvest U.S. technology secrets via conversion of U.S. IP. *See also* Statement of Jeff Johnson, *supra* note 84.

[98] Statement of Jeff Johnson, *supra* note 84.

[99] Taylor Glascock/Bloomberg, Photograph, *in* Caleb Harshberger, *Quantum Contractors Wary of Global Activity Curbs to Foil China*, BLOOMBERG LAW (Dec. 7, 2022), https://news.bloomberglaw.com/privacy-and-data-security/quantum-contractors-wary-of-global-activity-curbs-to-foil-china [https://perma.cc/5YA2-DTZ4].

Cybersecurity professionals have made significant advances reducing the risks related to two intertwined concerns. First, Foreign State's campaigns for economic domination. And second, disparate efforts, which have traditionally been the U.S. response to legitimate concerns to stop foreign cyber-economic campaigns to convert U.S. technology. Significant, ubiquitous, and persistent foreign strategies have placed the U.S. at a pivotal point. Cybersecurity is multi-faceted and while much has been accomplished in the overall field of cybersecurity, combating IP theft is still an area with opportunity for growth. Thus, providing greater security for patent applications is an evolving area of cybersecurity. We arrived at this pivotal point in part due to a general disbelief that any Foreign State, traditionally so far behind us, could out pace us. This general disbelief combined with myriad strategies to exploit, copy, and convert U.S. IP have slowly eroded our comfortable position on the center pedestal and, unfortunately, this change has now positioned some foreign states to leapfrog ahead. Because of this environment many U.S. technologies are of keen interest to, and are being converted and commercialized by, foreign competitors. This is all happening at an unprecedented pace. Specifically, with the exponential rate at which these foreign campaigns are advancing, we are now seeing persistent conversion of U.S. Intellectual Property.

The rest of this article focuses on a known quantum tool that can be implemented along with changes in Policy to plug the torrential drain of technology. There are several foreign cyber-economic campaigns described in this article that, by design, hack and drain our economy for incalculable value. There are also several suggested responses, which the U.S. might deploy to hedge against these illicit activities. Examples include tightening Export Controls, stringent

review of foreign Visa applications, designing and implementing more sophisticated encryption protocols, and bringing greater resources to CFIUS. However, paramount in our catalogue of responses to be deployed is stopping the illicit transfer of U.S. technologies, which is our Intellectual Property ("IP") and our future. Because IP represents the future of the U.S. economy, and not a present-day tangible chattel, we can employ an existing cyber security tool to protect IP; to protect our future. While there are several methods to illegally transfer IP out of the U.S., there are two activities that can be unequivocally stopped: (1) Viewing confidential IP on secure databases ("IP Repositories") and (2) the interception of communications between parties with authorized access to confidential IP (transmission of "Confidential Information ('CI')"). Quantum Key Distribution ("QKD") is a quantum tool that ensures IP repositories are impenetrable. This is guaranteed because with QKD the transmission of the data within a repository, which might include sensitive IP, is not possible.

A. Solutions to Protect IP during Cyber-Economic Campaign: A Marriage of Science and the Law

Some of the current solutions to combating Cyber-Economic Campaigns, now in place, including tighter Export Controls, greater scrutiny of Visa applications, and implanting greater encryption protocols, have disadvantages. For example, U.S. firms facing strict export controls will have trouble competing internationally due to increased controls. Likewise, U.S. Defense and national security arenas will not get the encryption they need to survive hacks unless vendors join the struggle against Cyber-Economic Campaigns.[100] This article provides a single

[100] Caleb Harshberger, *Quantum Contractors Wary of Global Activity Curbs to Foil China*, BLOOMBERG LAW (Dec. 7, 2022),

solution to the disadvantages currently observed, which arises from applying recent advances in quantum computing to an urgent need for greater cybersecurity in the Intellectual Property arena. This article offers a science-based solution, which the law can apply broadly apply to completely immobilize the cyber invasions of foreign actors in their campaigns of Cyber-Economic Campaigns.

B. Quantum Key Distribution ("QKD")

Once fully developed, Quantum Key Distribution ("QKD") can be implemented to (1) stop hacks into IP repositories; (2) prevent the interception and redirected relaying of confidential transmission of IP data, which is a major strategy used by foreign actors to convert U.S. IP today; and (3) employ safeguards for other Confidential Information ("CI") while preventing its theft or unauthorized access.

It is worth noting that full-scale quantum computing solutions in the U.S. are hampered by the fact that China and the U.S. are competing in a "neck-and-neck race" to arrive at a quantum breakthrough.[101] China is heavily invested in creating and implementing this technology and as of the writing of this article, a quantum solution is not known to be deployed on either side. This is an ironic situation because the competition between the U.S. and China is the primary reason why there are zero known current examples[102] of QKD being successfully deployed to encrypt data today.

If this competition to deploy a quantum solution did not exist we could witness a huge leap forward in available

---

https://news.bloomberglaw.com/privacy-and-data-security/quantum-contractors-wary-of-global-activity-curbs-to-foil-china [https://perma.cc/5YA2-DTZ4].

[101] *Id.*

[102] Perhaps one of the governments has a deployable quantum solution and it is top-secret?

cryptology technology, which would be evidenced by extreme advances in quantum data security.[103] The fundamental difference between security results observed by current encryption protocols as compared with the results of QKD is the latter "uses quantum technology to protect data *as it is transferred* from place to place rather than *post-quantum encryption which protects the data where it is stored*."[104] The latter can be hacked, collected and then decrypted later.

To better clarify this difference, the problem with current encryption protocols is that once the "data-storage-tank" is breached by unauthorized party, the data may be collected and transported, and the secret is out (it can be deciphered later by the unauthorized party). On the other hand, quantum technology using QKD prevents *any* transfer (e.g. an electronic transmission to the hacker's machine) because quantum technology protects *movement* of data. In short, traditional protocols protect against only breaching the walls of the fortress via an *unauthorized entry into the Fortress*. Conversely, QKD protocols safeguard *movement in and out of the fortress*.

Thus, it should be clear QKD is a viable solution to the onslaught of Cyber-Economic Campaigns currently encountered in the U.S. because it creates a barrier-to-movement that intruders are unable to overcome. In traditional security protocols, once the intruder enters a cyber fortress, it is game-over for the fortress. That data is breached and will be put to task later. On the other hand, with QKD the intruder is stopped at the fortress and, remarkably, will not be able to transport data in or data out. The enormously revolutionary advance realized by the utilization of a QKD protocol is *preventing movement* of the encrypted data into unauthorized hands (or in *preventing movement* of

[103] Harshberger, *supra* note 100.
[104] *Id.*

encrypted data out of authorized hands). QKD has nothing to do with encrypting or decrypting data. Rather, with QKD, a cyber intruder is unable to move data at all, which fully erases all opportunities to redistribute, copy, or decrypt the data in the future.

C. Quantum Solutions currently employed

Known examples for encrypting IP data using QKD.

Currently, there are no unclassified examples illustrating the deployment of cybersecurity strategies that integrate quantum models of encryption. As of 2023, integration of QKD offers an opportunity for cyber professionals who are seeking to reduce their risk of data exposure. Implementing QKD as part of a patent agency's evolving Zero Trust Architecture would mark a meaningful leap forward in any defensive model that envisions preventing the loss of IP data to competitors.

VII. CONCLUSION

Governments have held certain technologies to be Trade Secret since antiquity. Silk is one such example. While the U.S. Government currently employs several practices to combat the theft of Intellectual Property ("IP"), these strategies are disconnected, and the result is that foreign interest in converting U.S. technologies continue to threaten our position as the global technological forerunner. To stop the erosion of U.S. IP, designing and implementing revolutionary encryption protocols must be a top cyber security priority.

In the first three decades of the 21st Century, the U.S. finds itself in a defensive position in cyber-economic campaigns that target the conversion of U.S. IP. How to implement cybersecurity is a centerpiece of U.S. concern. Traditionally, *Secrecy Orders* ensured IP patent applications remained hidden from inquisitive foreign governments.

However, *Secrecy Orders* no longer provide an adequate solution. Their secrecy is no longer adequately addressed because the *storage location* of U.S. patent application are easily breached. Breaches remain possible because the *movement* of data to a remote location is not addressed by currently employed cyber security protocols.

However, Quantum Key Distribution ("QKD") provides advanced and unparalleled cybersecurity needed to impede foreign efforts to convert U.S. IP. It is advanced because it prevents *any* transfer of data. Because quantum technology provides a Key authorizing or denying the *movement* of data, unauthorized hackers are unable to carry the data away from a secure location. QKD is cutting-edge advancement in the cybersecurity space. Most significantly, its esoteric nature makes it the prime candidate for a new "lock and key" mechanism, which could be installed on any U.S. database that is expected to be impenetrable. The USPTO should consider implementing this leap in cybersecurity before it faces the next OPM-like breach.

The successful deployment of an ultramodern cyber-defense tactic such as QKD would ensure the U.S. maintains its global technological advantage by keeping U.S. IP secure. However, without the proper authority to oversee new cyber security protocols, to monitor effectiveness, and to distribute tax dollars to ensure deployment of this strategy, the U.S. reputation as the source of advanced technologies will be fleeting.

While it is important to ensure quantum technology is implemented quickly, deployment is not easily executed. This is because development of an efficient quantum infrastructure requires several agencies to commit to work together while funding a single mission with a new infusion of tax dollars. However, congressional commitment of tax dollars and inter-agency collaboration are not automatic. Yet, if successful, this defensive cybersecurity tactic will end most foreign cyber-espionage campaigns.

Appendix Table of Contents

I. APPENDIX I – EXAMPLES OF IP THEFT: [105] A BRIEF HISTORY OF ILLEGAL TECHNOLOGY TRANSFER (IP THEFT).

A. 200 BC: The Great Byzantine Silkworm Heist.

Silk was first produced in China. Originally, silk was reserved for Chinese Emperors. In fact, Emperors of China attempted to monopolize the production of silk by keeping sericulture knowledge secret. However, the spread of this knowledge to Korea around 200BC, to India by 300AD and eventually to Europe by around 500AD is one of the first known Trade Secret violations.[106] The medieval Byzantine Empire produced and used luxurious silk, but until the mid-6th century Byzantine artisans had to import raw silk from China.[107]

B. 9th Century: Gunpowder.

The discovery in the 9th century seems an accident when Alchemists had accidently mixed certain chemical compounds together in their quest for an elixir of immortality. Early alchemy texts flag a caution to avoid mixing certain chemicals. Consequently, while gunpowder was first discovered in China, the spread of that knowledge does not appear to violate any Trade Secrets. The discovery spread from China to Japan and Europe sometime between

[105] Of the eight briefs provided in Appendix I, only six are specifically Trade Secret theft, or another form of IP theft – and these are briefs A, C, D, E, F, and G. But note, briefs B and H are not IP theft *per se*.
[106] *See* Reisman, supra note 23, at 5.
[107] The Histories, *How Byzantine Monks Stole Silkworms From China*, YOUTUBE (Oct. 8, 2022), https://youtu.be/NeqBTUFcU80?si=LZvMaHZhQZIxqNmT [https://perma.cc/Y5TP-DA5A].

the 13th and 14th centuries. And by the mid 14th Century, cannons were everywhere in Europe and China.[108]

C. 19th Century: The Cartwright Loom, 1811.

After visiting England in 1811, Francis Cabot Lowell walked away with the biggest piece of the Industrial Revolution—the Cartwright loom. Lowell had memorized the plans to build the loom, which fortified his later success. The technique he pioneered to forge his success are the same techniques being used against us today.[109]

D. 20th Century: Development of the Tupolev, Tu-144 supersonic aircraft, circa 1959 to 1976.

In the 20th century, a stunning strategy to steal Intellectual Property was well played by Russia. It involved stealing the Trade Secrets of the Concorde. The plan involved industrial espionage and resulted in the development of the Tupolev, Tu-144 supersonic aircraft.[110]

E. 21st Century: Harvard Medical School, 2002.

Two people in San Diego were arrested arising from a complaint that they stole Trade Secrets while employed as research fellows at Harvard; they then engaged interstate transportation of the stolen Secrets. This was like the next case (see CCF) in that the stolen Trade Secrets included stolen reagents, which were used by Harvard to study genes and regulate enzymes *in vivo*.[111]

---

[108] Reisman, supra note 23, at 6.
[109] *Id*. at 8.
[110] *Id*. at 9.
[111] *Id*. at 21.

F. 21st Century: Cleveland Clinic Foundation ("CCF"), 2002.

An employee of Kansas University Medical Center ("KUMC") was indicted with the theft of both research Materials and research Ideas from Cleveland Clinic Foundation ("CCF"). The employee is alleged to have stolen from CCF genetic materials in the form of DNA and cell line reagents. This theft resulted in the employee being charged with economic espionage by stealing the above-mentioned Trade Secrets from CCF and for altering and destroying the Trade Secrets that were the property of CCF.[112]

G. 21st Century: Boeing and Lockheed Martin, 2003.

Two former Boeing managers were charged with stealing Lockheed Martin Trade Secrets. The stolen Secrets were related to rocket programs for the U.S. Air Force. Both Boeing managers were charged with conspiracy, theft of Trade Secrets and violating the Procurement Integrity Act.[113]

H. 21st Century: OPM Breach of 2015.[114]

II. APPENDIX II – EXAMPLES OF GOVERNMENT RESPONSES TO PROTECT THEIR IP.

A. Britain's response: Industrial Revolution.

In 1729, Britain banned skilled worker migration in response to France's and Russia's attempts to extract British

---

[112] *Id*. at 21–22.
[113] *Id*. at 20.
[114] *See* § IV: A BRIEF HISTORY OF DATA THEFT OVER THE CENTURIES, on pgs. 795–800 of this article. This breach is not necessarily a theft of

technological advances by recruiting British workers. Britain punished such emigration by fine or imprisonment those who did not return home within 6 months could face losing their land, property, and citizenship. In 1750, Britain banned exportation of "'tools and utensils' in wool and silk industries." However, entrepreneurs in foreign States found numerous ill-famed paths to circumvent Britain's new law including taking advantage of their mother State's offer to pay a bounty for certain technologies![115]

B. Suisse Response: Germany's Sanctions.

In 1907, in response to Germany threatening trade sanctions, Switzerland lay the groundwork for a first major overhaul of Swiss patent law. And, to thwart the threat of losing valuable technologies in the pharmaceutical arena, Switzerland again enacted major changes to its patent law in 1978 that allowed chemicals and pharmaceuticals coverage.[116]

III. APPENDIX III – U.S. TOP-3 TOOLS TO IMPEDE UNWANTED TECHNOLOGY TRANSFER.

A. The Committee of Foreign Investment in the U.S. ("CFIUS"):

CFIUS is one of the few tools used today to stop transfer to technologies; however, CFIUS is not designed for this kind of policework. This is because any transactions that do not result in "foreign controlling interest are beyond CFIUS' jurisdiction."[117]

IP. However, the extent of stolen PII makes this a noteworthy cyber theft.

[115] *See* Reisman, supra note 23, at 8–9.

[116] *Id*. at 9.

[117] Brown & Singh, *supra* note 34, at 23.

B. Export Controls ("EC"):

These are designed to prevent technology transfer to certain adversaries, which are believed to be able to employ the tech toward undesirable outcomes. The biggest issue with EC is that compliance is a private responsibility and early-state tech companies neither have requisite EC controls nor do they command the depth of resources needed to handle the complexity of trade compliance. [118]

C. VISA Scrutiny:

Foreign national students who study in the U.S. are under the purview of the U.S. State Department. As such, these students, sometimes unfortunately, are not scrutinized with protection of critical technologies in mind.[119]

IV. APPENDIX IV – SEVEN (7) STRATEGIES USED BY CHINA TO ILLICITLY TRANSFER TECHNOLOGY OUT OF THE USA.

A. Industrial Espionage.

For years, China has "been engaged in a sophisticated industrial espionage program targeting key technologies and Intellectual Property to enhance commercial enterprises and support domestic champions."[120] The FBI has noted caseloads are increasing

---

[118] *Id*. at 24.

[119] *Id*. *See infra* for Case Studies of where it may have been advantageous to vet a foreign national student prior to their admission to the USA. Specifically, refer to example "E" and "F" in Appendix I of this article, which is titled "*Examples of IP Theft: A Brief History of Illegal Technology Transfer (IP Theft).*" These case studies are provided by Reisman, *supra* note 23, at 5.

[120] Brown & Singh, *supra* note 34, at 17 (citation omitted).

in recent years and an FBI survey of 165 companies revealed that 95% of those companies cite China as the perpetrator.[121]

B. Academia.

For years, China has sent a mounting number of students to the U.S. for studying.[122] China will often offer exciting incentives to the students to convince them to return to China once they graduate or once the student rises to the level of expert in the field.[123]

C. Open sources tracking of foreign innovation.

China has made the collection and distribution of science and technology a national priority since at least the 1980s.[124] In fact, as far back as "1985, there were 412 major science and technology intelligence institutions nationwide . . . . employing . . . . 60,000 workers [in China]. . . . [who were] investigating, collecting, analyzing, synthesizing, repackaging, benchmarking and reverse engineering."[125]

D. Chinese-based technology transfer organizations.

Within China, there are dozens of organizations that seek out U.S. technologies in addition to an expert scientist who agrees to further develop the U.S. technology in China.[126] Notably, these are in addition to the many clandestine services, open-sources, and procurement

---

[121] *Id.*
[122] *Id.* at 18.
[123] *See id*. at 17.
[124] *Id.* at 19.
[125] *Id*. at 19 (*quoting* Hannas, China Industrial Espionage, Chapter 2 at 22).
[126] *See* Brown & Singh, *supra* note 34, at 19.

offices.[127] The success of this tech transfer platform is evidenced by over 440,000 foreign experts working in China.[128]

E. Chinese research centers in the U.S. to access talent and knowledge.

There are ever-increasing Chinese firms that set up research centers in the U.S. with the explicit goal of accessing U.S. talent and technology.[129]

F. U.S.-based associations sponsored by the Chinese government.

There are many professional associations such as the Chinese Association for Science and Technology ("CAST") that bring Chinese engineers together and advocate for their success in the U.S. and then bring their success back to China.[130] This support (offered by China in the U.S.) is later coupled with tremendous offers of compensation, advancement, and opportunity to advance and transfer their research efforts back in homeland China.[131]

G. Leveraging technical expertise of U.S. private equity, venture firms, investment banks & law firms.

Many U.S. law firms have built practices advising Chinese companies how they should structure deals to ensure that they receive CFIUS approval.[132]

---

[127] *Id.*
[128] Brown & Singh, *supra* note 34, at 19.
[129] *Id*. at 20.
[130] *Id.* at 20–21.
[131] *Id*.
[132] *Id*. at 21.

V. APPENDIX V – EXAMPLES OF SEEMINGLY LOW-RISK ACTS, WHICH SHOULD HAVE BEEN FLAGGED AS HIGH-RISK ACTS.

Around 1997, one of the founders of NetScreen took positions at Intel and Cisco.[133] The original investors included U.S. and Taiwanese VC; but traditional due diligence would have flagged such investments as a high-risk venture.[134]

Around 2008, NetScreen and Juniper engineers adopt encryption models for their VPN solutions that is known to be susceptible to hacking, and they implement it in a way that further weakens it.[135]

The next three strategies seemingly allow theft of IP under the auspices of the Chinese government legitimately controlling and regulating their economy. The following are less unassuming tactics that demonstrate aggressive and (sometimes) disruptive strategies aimed at control and dominance of emerging technologies:

A. IP Coercion: A past campaign to access existing Technology.

Chinese use of "sales related incentives and dis-incentives to manipulate Rolls-Royce to . . . . provide access to sensitive propulsion-related engineering IP."[136] Later it was found out that China sold no less than two destroyers and two attack submarines—employing an identical sensitive propulsion technology—to Pakistan.[137]

---

[133] Statement of Jeff Johnson, *supra* note 84.
[134] *Id*. at 51.
[135] *Id.* at 52.
[136] *Id.* at 59.
[137] *Id.*

B. IP Fraud: A present campaign to open a new portal to Technology.

China's National Development and Reform Commission ("NDRC") is now "investigating foreign companies for perceived anti-trust violations[.]"[138] The end-result allows a "mechanism for accessing and sharing sensitive IP seized during [those] investigations."[139]

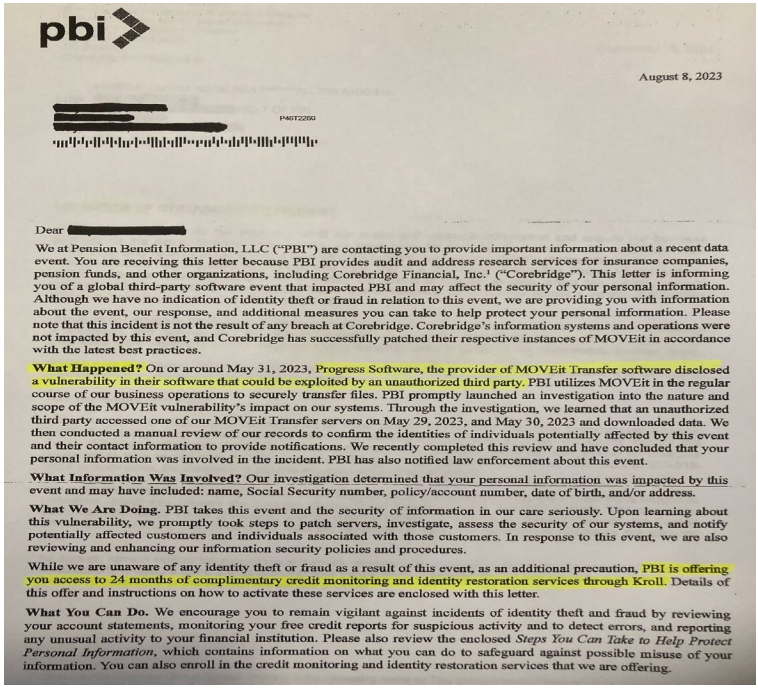
C. IP conversion: Government-sponsored campaigns designed to control emerging Technology.

ChinaCo is "executing an aggressive IP theft and conversion campaign, as well as a State-sponsored acquisition to corner the bitcoin and blockchain market[.]"[140] The result is a disruptive fintech and asset management innovation, which will undermine all current industry leaders.[141]

[138] Statement of Jeff Johnson, *supra* note 84, at 58.
[139] *Id.* at 58.
[140] *Id.* at 56.
[141] *Id.*

VI. APPENDIX VI – EXAMPLES OF LETTERS REGARDING 'IDENTITY THEFT' & 'CYBERSECURITY INCIDENTS.'

A. PBI Letter Offering 'Credit Monitoring & Identity Restoration':



pbi

August 8, 2023

[redacted]

P46T2269

Dear [redacted]

We at Pension Benefit Information, LLC ("PBI") are contacting you to provide important information about a recent data event. You are receiving this letter because PBI provides audit and address research services for insurance companies, pension funds, and other organizations, including Corebridge Financial, Inc.[1] ("Corebridge"). This letter is informing you of a global third-party software event that impacted PBI and may affect the security of your personal information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your personal information. Please note that this incident is not the result of any breach at Corebridge. Corebridge's information systems and operations were not impacted by this event, and Corebridge has successfully patched their respective instances of MOVEit in accordance with the latest best practices.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that could be exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that an unauthorized third party accessed one of our MOVEit Transfer servers on May 29, 2023, and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review and have concluded that your personal information was involved in the incident. PBI has also notified law enforcement about this event.

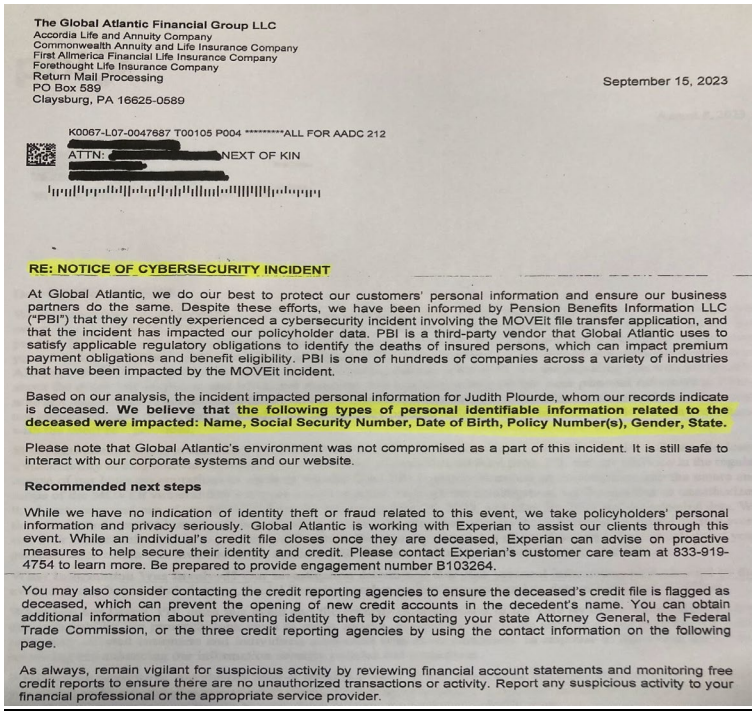
What Information Was Involved? Our investigation determined that your personal information was impacted by this event and may have included: name, Social Security number, policy/account number, date of birth, and/or address.

What We Are Doing. PBI takes this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, PBI is offering you access to 24 months of complimentary credit monitoring and identity restoration services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring your free credit reports for suspicious activity and to detect errors, and reporting any unusual activity to your financial institution. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring and identity restoration services that we are offering.

B. GAFG Letter Providing Notice of 'Cybersecurity Incident':



The Global Atlantic Financial Group LLC
Accordia Life and Annuity Company
Commonwealth Annuity and Life Insurance Company
First Allmerica Financial Life Insurance Company
Forethought Life Insurance Company
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 15, 2023

K0067-L07-0047687 T00105 P004 **********ALL FOR AADC 212

ATTN: [redacted] NEXT OF KIN
[redacted]

RE: NOTICE OF CYBERSECURITY INCIDENT

At Global Atlantic, we do our best to protect our customers' personal information and ensure our business partners do the same. Despite these efforts, we have been informed by Pension Benefits Information LLC ("PBI") that they recently experienced a cybersecurity incident involving the MOVEit file transfer application, and that the incident has impacted our policyholder data. PBI is a third-party vendor that Global Atlantic uses to satisfy applicable regulatory obligations to identify the deaths of insured persons, which can impact premium payment obligations and benefit eligibility. PBI is one of hundreds of companies across a variety of industries that have been impacted by the MOVEit incident.

Based on our analysis, the incident impacted personal information for Judith Plourde, whom our records indicate is deceased. **We believe that the following types of personal identifiable information related to the deceased were impacted: Name, Social Security Number, Date of Birth, Policy Number(s), Gender, State.**

Please note that Global Atlantic's environment was not compromised as a part of this incident. It is still safe to interact with our corporate systems and our website.

Recommended next steps

While we have no indication of identity theft or fraud related to this event, we take policyholders' personal information and privacy seriously. Global Atlantic is working with Experian to assist our clients through this event. While an individual's credit file closes once they are deceased, Experian can advise on proactive measures to help secure their identity and credit. Please contact Experian's customer care team at 833-919-4754 to learn more. Be prepared to provide engagement number B103264.

You may also consider contacting the credit reporting agencies to ensure the deceased's credit file is flagged as deceased, which can prevent the opening of new credit accounts in the decedent's name. You can obtain additional information about preventing identity theft by contacting your state Attorney General, the Federal Trade Commission, or the three credit reporting agencies by using the contact information on the following page.

As always, remain vigilant for suspicious activity by reviewing financial account statements and monitoring free credit reports to ensure there are no unauthorized transactions or activity. Report any suspicious activity to your financial professional or the appropriate service provider.