General Assembly 6 (LEGAL)
Topic 2: The Question of Identity Fraud and Theft in The Digital Age

Northbridge International School Cambodia
Model United Nations 2025

Head Chair: Sothea Tan

Deputy Chair: Sunpeng Lim

Table of Contents

Introduction:

With the rapidly growing advancements in technology over the past few decades, the issue of identity fraud and theft emerged as pressing challenges in the Digital Age, in the twenty-first century.

Individual's personal data has become vulnerable to being leaked online through various methods of cyber threats. For instance, this can include hacking, data breaches, and phishing scams (EUROPOL, 2021). These aspects enable criminals to exploit sensitive information, cause not only reputational damage, but also to severe repercussions, including financial loss, unauthorized access to accounts, fraudulent transactions and being confronted with legal liabilities (Javelin, 2021).

Stolen personal information is usually associated with identity theft, where individuals may find themselves accused of crimes they did not commit or burdened by debts they never incurred. This issue is further exacerbated by the growing reliance on the internet in daily life (INTERPOL, 2022). Such problems threaten the trust in digital infrastructure, especially as critical services such as banking, healthcare, education, and government identification systems increasingly rely on online platforms.

While there have been efforts to regulate digital privacy and security measures including cybersecurity protocols and data protection laws, more needs to be done to combat the evolving attacks from cybercriminals.

Identity theft has caused widespread disruptions to the economy, with a scope that can be seen on a global level. Identity theft accounted for nearly 1.4 million complaints in the United States alone (FTC, 2022), and similar trends have been observed globally (INTERPOL, 2022), as seen during 2021, causing financial losses exceeding 56 billion USD (Javelin, 2021). This pervasive problem has demonstrated difficulty in maintaining policy and integrity for all users in the Digital Age, demanding attention and responses from all nations.

Key Terms:

Identity Theft and Fraud

Identity theft and fraud refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. These crimes encompass all types of actions involving misuse of personal information. For instance, these data can be wrongfully obtained through phishing scams, data breaches, or websites that can collect user information without proper consent. By collecting credit card details or Social Security numbers, crimes committed could involve making unauthorized purchases, opening fraudulent accounts, or other financial crimes that causes harm, to the victim, deeming as illegal by the nation's security law. (U.S. Department of Justice)

Cybercrime

The complex nature of the crime as one that takes place in the borderless realm of cyberspace, often-time described as having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse. (UNDOC)

Data Breach

A data breach is an incident in which confidential or personal information of an individual is exposed. This can include bank details, social security number, driver's license number, medical record, financial record and more. This exposure can occur either electronically or in paper format. (Identity Theft Resource Center).

Phishing

In the field of computer security, phishing is the practice of tricking individuals into providing sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in electronic communication (UNESCWA). For example, a cybercriminal may impersonate a well-known, credible organization, such as a bank, and send an email requesting the recipient to verify their account information through a provided link. Other may include scam calls and social media text scams. These tactics are typically employed for the purpose of acquiring personal information, financial fraud, or other forms of malicious activity (EUROPOL, 2021.

Cybersecurity:

Cybersecurity refers to the measures taken to protect computing systems, networks, and sensitive information from unauthorized access, theft, or damage (ITU-T X.1205). It involves the use of technology, process, and practices designed to secure digital devices, networks, and data from cyber threats such as hacking, malware, phishing attacks, and more (National Institute of Standards and Technology, 2020). Cyber security plays a crucial role in preventing identity theft and fraud and preventing such cyberattacks in the digital world (FTC, 2022).

Digital Age

The Digital Age refers to the present era, characterized by the widespread use of technology that began with the first invention of computing and the rapidly evolving of network throughout the 21st century. Technological advances, such as the development of low-cost computing, the internet, and mobile connectivity, have transformed society, making the Digital Age a defining period of increasing interdependence and accelerating change (UN). This era plays an important role in shaping each aspect of how individuals interact, access services, and manage their private information.

Personal Data

Personal data is any information that is related to an identified or identifiable natural person. This includes references to names, addresses, identification numbers, and digital identifiers like IP addresses. (GDPR)

Background Information:

The era of rapidly advancing technology and the digital transformation of global connectivity have redefined how individuals interact, communicate, and store their personal data. At the same time, the issue of identity fraud and theft has emerged as a significant global challenge.

Most prevalent throughout the 20th century, identity theft existed in rudimentary forms, such as forging physical documents, such as passports, IDs, birth certificates, driver's licenses, and impersonating individuals to gain unauthorized access to resources (United Nations, 2019). Impersonation and document forgery were commonly used to access resources, evade authorities, or commit financial fraud, especially tax evasion (Interpol, 2024).

During the industrial revolution and the rise of bureaucracy worldwide in the 19th to early 20th centuries, standardized documentation for identity verification, such as social security numbers and government-issued IDs, were introduced (United Nations Economic and Social Commission for Western Asia, 2024). Despite all these innovative efforts, they also created new opportunities for fraudsters to exploit the vulnerabilities in the system.

Most remarkably, during the Cold War, the second half of the 20th century, agencies and spies committed espionage —the act of spying on or obtaining confidential information from rival governments—by taking advantage of the weak points of the identification systems to forge fake IDs to gather confidential information from both the United States and the Soviet Union (Sikka, n.d.). Today, while this was historically evident in the U.S. and U.S.S.R., the practice of espionage continues to affect government agencies and organizations around the globe.

Furthermore, the development of the internet in the late 20th century and the subsequent rise of digital technologies in the 21st century have escalated the scale and intricacies of this crime (International Telecommunication Union, 2020).

In the digital-dependent world, personal information has been stored and transmitted digitally on an unprecedented scale. Online infrastructures, such as online banking, e-commerce, social media, and government databases, are becoming lucrative targets for cyber-attacks (World Bank, 2023).

Not only that, but cybercriminals have also evolved to employ many other advanced techniques, such as phishing scams, malware attacks, and certain aspects of social engineering, to exploit vulnerabilities of digital systems (Federal Trade Commission, 2024). Once personal information is obtained, it can be used to open fraudulent accounts, steal money, or even develop fake identities using the user's data (United Nations Office on Drugs and Crime, 2024).

Current Situation:

The modern world, where digitalization is being globalized internationally, has ushered in a larger scale of attacks that impacted millions—those impacted include individuals, businesses, and the government. The widespread adoption of digital technology for financial transactions, communications, and governmental services has become a main reliance for all users on keeping their data online (World Bank, 2023).

In 2003, payment processor PayByTouch, based in the U.S., suffered a breach exposing 2.4 million credit card numbers and authentication details. At the time, it was the largest identity theft case on record, according to CSO Magazine (CSO, 2003). Other breaches would dwarf this in just a few years later. Even big corporations and governments fell victim. In 2007, retail giant TJX, also based in the U.S., discovered a breach in their wireless networks that exposed over 45 million credit and debit cards worldwide (United Nations, 2019). In 2015, hackers infiltrated the US Office of Personnel Management and federal worker records, compromising personal details of over 21 million people—including social security numbers, addresses, and even fingerprints (United Nations Office on Drugs and Crime, 2024). In addition to that, in 2019, the Marriott International breach exposed sensitive information of 500 million customers, which included passport numbers and payment details, stressing the weaknesses within corporate systems (Interpol, 2024).

The rise of synthetic identity fabrication has become a prominent problem that further complicates the issue. Criminals can now combine real and fake information to create many versions of identities by using the information from stolen data (Federal Trade Commission, 2024).

This crime has become one of the fastest-growing forms of fraud globally. In the United States alone, the Federal Reserve estimates that this form of identity theft accounts for 20% of credit card fraud and is responsible for billions in financial losses annually (United Nations Economic and Social Commission for Western Asia, 2024).

In developing nations, this impact is more magnified due to weaker cybersecurity frameworks, which lack adequate resources to manage and secure (World Bank, 2023). Countries like Nigeria and Kenya heavily rely on mobile banking and digital identities, which are part of their financial inclusion initiatives implemented by their federal government (United Nations, 2019). These platforms make them prone to cybercriminal attacks on these systems for the purpose of defrauding individuals and institutions (International Telecommunication Union, 2020).

These cases are also evident in many other African and South Asian nations, which often lack stringent data protection laws and agencies (Sikka, n.d.). This is clearly demonstrated by the breaches of the Aadhaar system, one of the world's largest biometric identification programs (United Nations Office on Drugs and Crime, 2024). As a result, millions of personal data have been exposed, further threatening the security of individuals and the trust in their government's regulation (Interpol, 2024).

The contrast in the global context highlights disparities in cybersecurity between MDCs and LDCs. In other words, wealthier nations can invest in safer protocols and more advanced protection systems, while less-developed nations often lack these aspects, further stressing global inequalities (International Telecommunication Union, 2020). In this advancing Digital Age, this issue persists as a difficult challenge, necessitating global efforts to resolve and develop a safer and more protected digital world for all sovereign nations (United Nations, 2019).

Major Parties Involved:

European Union (EU):

The EU has been proactive in trying to solve the issue of identity fraud through restrictive regulations such as the General Data Protection Regulation (GDPR). GDPR enforces strict data protection and privacy standards across Europeans nations associated with the EU. However, they still face problems regarding cross-border identity theft, due to the globalization of the economies and shared data systems between their member states. (GDPR)

INTERPOL:

INTERPOL also known as the International Criminal Police Organization provide several specialized tools for the law enforcement community to help detect fraudulent documents – technical databases, online reference tools, a forensic laboratory and tailored training programs. They work with other sectors to improve the level of security of official documents and implement initiatives such as the Global Complex for Innovation (GCI). (Interpol)

United States of America (U.S):

The U.S. continues to be a primary target for cybercriminals. They actively try to address widespread digitalization and high-profile data breaches, such as the 2017 Equifax breach. The country has made efforts to implement various laws, including the Identity Theft and Assumption Deterrence Act (ITADA) and promoted cybersecurity measures to protect confidential data via the CIA. Nonetheless, the U.S. still faces the thousands of cyber-attacks each year. (FTC)

Cybercrime Convention Committee (T-CY):

The T-CY of the Council of the Council of Europe (CoE) is giving Member States guidance on interpreting the Budapest Convention on Cybercrime. Adopted in 2001, it has now been ratified by 39 States and is one of the best-known frameworks for States in the fight against cybercrime.

EUROPOL:

EUROPOL’s European Cybercrime Centre (EC3) addresses large-scale identity fraud and theft within the EU. Working across various member states and their international partners, EUROPOL conducts investigations on cybercriminal networks and shares intelligence data to address those operations effectively.

International Telecommunication Union (ITU):

The ITU established international standards for data protection and promoting secure communication technologies following the Global Cybersecurity Index (GCI) focal points. (ITU Publications)

Timeline of Relevant Events:

Title and Date (Year, Month, Day)	Description
Identity Theft and Assumption Deterrence Act (1998, October 30)	This U.S. law defined identity theft as a federal crime and establish punishments for those that commit these crimes, marking the earliest legislative stages that combat the issue of identity fraud in the Digital Age.
Adoption of the Budapest Convention on Cybercrime (2001, November 23)	The CoE's Budapest Convention became the first international treaty that addressed cybercrime, structuring a security framework and setting guidelines for more efficient solutions to combat cybercrime for international cooperation.
Creation of the National Strategy for Trusted Identities in Cyberspace (2011, April 15)	The U.S. federal government issued a new tactic to improve the privacy, security and convenience of sensitive online transactions through collaborative efforts with the private sector, advocacy groups, government agencies, and other organizations.
LinkedIn Data Breach (2012, June 6)	LinkedIn, a professional networking site, was the victim of unauthorized access and disclosure of some members' passwords. Hackers stole over 6.5 million hashed passwords and leaked them online.
Yahoo Data Breach (2013, August 1)	Yahoo reported a massive data breach in which hackers gained access to over 3 billion user accounts, compromising their personal information, which includes email addresses, passwords, and security questions, marking one of the largest breaches in digital history.
China's Cybersecurity Law Enactment (2017, June 1)	This law requires network operators to store select data within China and allows Chinese authorities to conduct spot-checks on a company's network operations. It has raised concerns among some foreign companies over greater data controls as well as increased risks of intellectual property theft.
Aadhaar Data Breach (2018, January)	This is the largest data breach in Indian history, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens. It was reported in January that criminals were selling access to the database at a rate of 500 rupees for 10 minutes, while in March a leak at the state-owned utility company allowed anyone to download names and ID numbers. (WEF's Global Risks Report 2019)
Adoption of African Union Data Protection Framework (2020, February 10)	The AU Data Policy Framework represents a significant step toward creating a consolidated data environment and harmonized digital data governance systems to enable the free and secure flow of data across the continent while safeguarding human rights, upholding security and ensuring equitable access and sharing of benefits. They adopted the

	Digital Transformation Strategy (DTS) for Africa 2020-2030, along with the operationalization of the African Continental Free Trade Area (AfCFTA),
CAM4 Data Breach (2020, March)	The recent CAM4 data exposure left nearly 11 billion records exposed, including sensitive personal information from the adult streaming website, it is estimated that just over 6.5 million of those records were from users in the U.S.. The information leaked included full names, email addresses, and payment logs. The database was immediately taken down by parent company Granity Entertainment once the CAM4 data exposure was discovered. However, the logs appear to have been exposed since March 16, 2020. (ITRC)
Pegasus Spyware Scandal (2021, July 18)	The Pegasus spyware scandal was revealed by investigations conducted by a global consortium of media outlets, exposing the use of Pegasus software, created by the Israeli company NSO Group. The spyware was used to hack into the smartphones of journalists, activists, politicians, and lawyers in multiple countries, including Mexico, India, Hungary, and Saudi Arabia. Pegasus allows attackers to remotely gain access to private data, such as text messages, call logs, contacts, and location.

Previous Attempts:

Due to the persistence of identity fraud and theft leading to global issues, many actions have been taken to resolve the severity of the issue.

In 2000, the United Nations recognized the problems of cybercrimes by adopting Resolution 55/63, which urges member states to prevent the criminal misuse of information technology and introduces certain measures to combat such misuse (United Nations, 2000).

This was then followed by Resolution 56/121 in 2001, which further emphasizes international cooperation to prevent the crimes of exploiting information technologies, including identity-related crimes (United Nations, 2001).

Also, in December 2019 the UN General Assembly adopted Resolution 74/247, which established an open-ended Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (United Nations, 2019).

In 2020, they also adopted Resolution 75/240, which created a new five-year Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (United Nations, 2020).

The European Union has stepped up by implementing the General Data Protection Regulation (GDPR) that went into effect on May 25, 2018. It is a law that protects individuals' personal data and ensures that organizations that collect data do so responsibly, allowing users greater control over their digital identities (European Commission, 2018).

Similarly, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), adopted in 2014, provides general rules and principles on three broad themes: personal data protection; electronic commerce; and cybersecurity and cybercrimes on the continent (African Union, 2014).

Singapore's Personal Data Protection Act (PDPA), established on January 2, 2013, implements a data protection law that comprises various rules governing the collection, use, disclosure, and care of personal data (Personal Data Protection Commission, 2013).

Multinational organizations have also taken initiatives like INTERPOL's Cybercrime Directorate, which coordinates law enforcement operations internationally and delivers secure data-sharing platforms, analysis, and training in order to reduce cyber-threats (INTERPOL, 2020).

Meanwhile, private-sector collaborations, most notably Microsoft's Digital Crimes Unit and Google's Advanced Protection Program, have collaborated to enhance their cybersecurity measures to maintain protection for their billions of users worldwide (Microsoft, 2024; Google, 2024).Yet despite these efforts, identity fraud and theft remain a major issue. Acording to the Federal Trade Commission (FTC), the U.S. alone recorded nearly 1.4 million cases of identity theft in 2022, while globally, losses attributed to digital fraud surpassed 55 billion USD (Federal Trade Commission, 2022).

Possible Solutions:

One of the solutions would be the development of blockchain technology, which ensures secure storage of personal information through decentralized and tamper-proof structures—making it extremely difficult to breach (Sovrin, 2020). Platforms like Sovrin Network have already demonstrated their effectiveness in the digital identification industry by making each data point more heavily secured (Sovrin, 2020). Widespread adoption of blockchains would be a major factor in securing personal data, while granting only access to authorized users (United Nations, 2020).

Similarly, there should also be biometric authentication systems to ensure the rightful owner by using existing identity verification processes. For easier and safer access to personal accounts, biometrics such as facial recognition, fingerprints, and voice identification would be much more efficient for access, while increasing the difficulty for criminals to replicate (Mell, 2018). Although this has already been issued in China regarding their biometric payment methods, this solution should also stress the security in maintaining the data of the biometrics being scanned to avoid replication through the systems (Zhang, 2021).

In concern of international legislation, a UN-led treaty on cooperating for global cybersecurity laws should be standardized and implemented. By setting up clear penalties and prosecution of the offenders, it guarantees a safer digital server worldwide (United Nations, 2020). Not only that, but such treaties would also prevent any corruption and ensure that no such perpetrators

could evade accountability by exploiting gaps in the law. Influenced by the effectiveness of the Budapest Convention on Cybercrime, this framework would be efficient in preventing further cybercrimes (Council of Europe, 2001).

Additionally, private organizations, NGOs, or MDCs should provide monetary funds and establish a clear funding system to less developed countries in efforts to help strengthen their cybersecurity infrastructure, especially with the improvements of biometric data and scanning. Managed by international bodies like the UN or World Bank, a support fund could be managed and allocated for targeted projects relating to cybersecurity (World Bank, 2021).

Raising public awareness by launching digital literacy programs is a way to prevent cyberattacks. Governments and private organizations should collaborate or launch awareness campaigns to teach individuals how to best keep themselves safe, such as recognizing the patterns of phishing scams via email or phone calls, using multi-factor authentication, creating strong passwords, and learning to avoid malware or virus attacks online (United Nations, 2020). Spreading information on how to keep personal data safe online is extremely crucial to ensure the safety of all individuals when relying on digital services.

Suggested Readings:

- UNODC Comprehensive Study on Cybercrime: DRAFT (link)

  This draft report by the United Nations Office on Drugs and Crime studies about cybercrime, which includes identity fraud and theft. It provides in-depth data and policy recommendations that are relevant when drafting resolutions and preambulatory clauses.

- UNESCO UIS A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2: INFORMATION PAPER NO.51 (link)

  An information paper about the role of education to promote digital literacy in preventing cyber-threats, understanding the significance of awareness.

- Identity Theft Resource Center (ITRC) 2023 Consumer Impact Report (link)

  Understanding the emotional, physical and psychological effects of identity theft on individuals and the economy.

- Cybersecurity Capacity Maturity Model for Nations (CMM) (link)

  This is a practical resource for many delegates who are proposing solutions for less developed countries and helping nations assess and improve their own respective cybersecurity measures.

- Identifying global privacy laws, relevant DPAs (link)

This resource by the International Association of Privacy Professionals (IAPP) details data protection laws globally and it is a helpful guide to research existing regulations and the gaps in privacy laws.

- A Review of the Economic Costs of Cyber Incidents (link)

  Published by the World Bank, this document exposes the direct costs of cyber incidents from the past, which helps with research and gather statistical evidence.

Bibliography:

" Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast." *Moneylife*, 2019, www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html.

African Union. Data Policy Framework for Africa. African Union, 2024, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf.

Council of Europe. "Giving Guidance on the Budapest Convention on Cybercrime." Cybersecurity Centre of Excellence (CCDCOE), 9 Sept. 2021, https://ccdcoe.org/incyder-articles/council-of-europe-giving-guidance-on-the-budapest-convention-on-cybercrime/.

CSO Magazine. "Biggest Data Breaches of the Decade." CSO, 2003, https://www.csoonline.com/article/2214857/the-biggest-data-breach-of-the-decade.

Federal Trade Commission (FTC). "Identity Theft Assumption and Deterrence Act: Text." Federal Trade Commission, 2024, https://www.ftc.gov/legal-library/browse/rules/identity-theft-assumption-deterrence-act-text.

Google. "Advanced Protection Program." Google, 2024, https://landing.google.com/advancedprotection/.

Identity Theft Resource Center. "Cam4 Data Exposure Leaks Billions of Records from Adult Streaming Website." *Identity Theft Resource Center*, 2020, www.idtheftcenter.org/post/cam4-data-exposure-leaks-billions-of-records-from-adult-streaming-website/.

International Telecommunication Union (ITU). "Cybersecurity." ITU-T Study Group 17, 2024, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

International Telecommunication Union (ITU). Global Cybersecurity Index 2020. ITU, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

Interpol. "Identity and Travel Document Fraud." Interpol, 2024, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Identity-and-

travel-document-fraud#:~:text=We%20provide%20a%20number%20of,of%20security%20of%20official%20documents.

Mell, Peter. Biometric Authentication Systems for Cybersecurity. National Institute of Standards and Technology, 2018, https://www.nist.gov/biometrics.

Microsoft. "Digital Crimes Unit." Microsoft, 2024, https://www.microsoft.com/en-us/security/digital-crimes-unit.

PBS. "Global Spyware Scandal: Exposing Pegasus." PBS Frontline, 2021, https://www.pbs.org/wgbh/frontline/documentary/global-spyware-scandal-exposing-pegasus/.

Personal Data Protection Commission (PDPC). "Personal Data Protection Act." Personal Data Protection Commission, 2024, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act.

Sikka, P. "Offshore Financial Centers and Money Laundering." International Monetary Fund, 2000.

Sovrin. "Sovrin Network: Securing Digital Identity." Sovrin, 2020, https://www.sovrin.org/.

United Nations. Digital Cooperation: A Shared Agenda for a Safer Internet. United Nations, 2020, https://www.un.org/en/digital-cooperation.

United Nations Economic and Social Commission for Western Asia (ESCWA). "Phishing." UNESCWA, 2024, https://www.unescwa.org/sd-glossary/phishing.

United Nations. "General Assembly Adopts Resolution 74/247 to Combat Criminal Use of Information and Communications Technologies." United Nations Press, 2021, press.un.org/en/2021/ga12328.doc.htm.

United Nations Office on Drugs and Crime (UNODC). "Privacy: What It Is and Why It Is Important." SHERLOC, 2024, https://sherloc.unodc.org/cld/zh/education/tertiary/cybercrime/module-10/key-issues/privacy-what-it-is-and-why-it-is-important.html#:~:text=Privacy%20enables%20the%20fulfilment%20of,disclosed%2C%20and%20shared%20about%20them.

United Nations. The Age of Digital Interdependence: Report of the Secretary-General's High-level Panel on Digital Cooperation. United Nations, 2019, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

United Nations. UN Resolution 55/63: Combating the Criminal Misuse of Information Technologies. International Telecommunication Union, 2000, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

United Nations. UN Resolution 56/121: Combating the Criminal Misuse of Information Technologies. International Telecommunication Union, 2001, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf.

Vergara Cobos, Estefania, and Selcen Cakir. A Review of the Economic Costs of Cyber Incidents. World Bank, 2024, https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf.

World Bank. Cybersecurity in Developing Countries: A Global Challenge. World Bank, 2021, https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity.

Zhang, Li. "Biometric Payment Methods in China: Current Trends and Future." Journal of Cybersecurity Studies, vol. 34, 2021, pp. 56-72.