Expert Report

Table of Contents

[Cyber Identify Theft Manifested in China 2](#_Toc118074721)

[Cyber Identity Fraud Transformation 2](#_Toc118074722)

[China Fraud Types 3](#_Toc118074723)

[Romance and Pig Butchering Scam 3](#_Toc118074724)

[Impersonating Officer, Acquaintance, Public Procuratorate Law or Government Organs Fraud 4](#_Toc118074725)

[Fake Credit Investigation, Online Shopping, Logistics or Customer Service Fraud 5](#_Toc118074726)

[Rights and Ethics 6](#_Toc118074727)

[Internet Regulation and Censorship 6](#_Toc118074728)

[Liberty and National Security 6](#_Toc118074729)

[The National Law’s Effectiveness 7](#_Toc118074730)

[Restriction on Anonymous Posts 7](#_Toc118074731)

[National Standards for Cybersecurity and Data Protection 7](#_Toc118074732)

[CSL 8](#_Toc118074733)

[DSL 8](#_Toc118074734)

[PIPL 8](#_Toc118074735)

[Effectiveness 9](#_Toc118074736)

[Investigative Tools 10](#_Toc118074737)

[Aspects Concerning 11](#_Toc118074738)

[Victims 11](#_Toc118074739)

[Harm 11](#_Toc118074740)

[Perpetrator 11](#_Toc118074741)

[Social Perception 12](#_Toc118074742)

[Conclusion 12](#_Toc118074743)

[References 13](#_Toc118074744)

# Cyber Identify Theft Manifested in China

## Cyber Identity Fraud Transformation

In the past, telephone scams like "Guess who I am" calls were common in China. Callers would gain people's trust by asking people to guess their identity or by pretending to the friends before stealing their money.

In China, the phone fraud investigation resulted in hundreds of arrests in 2016 (Stephen, 2016). Over the first two months of 2020, there has been an alarming increase in confidence tricks in Hong Kong, close to 270 people have fallen victim to love scams (Clifford, 2020).

Cyber identity theft is the act of obtaining another personal or financial information to use it for fraud, such as making unauthorized purchases or transactions. Identity theft can be done in a variety of ways, and the victims frequently have their reputations, finances, and credit damaged.

Along with cyberspace popularisation, the scam has been transformed into more systematic with online methods like automated phone calls with fake identities and cyberstalking from a bank, government agency, or delivery service. Prompted to respond with personal data by doing as their instructed.

## China Fraud Types

China's Cybersecurity Product Industry Competition Analysis Report showed the top 10 fraud types regarding the average losses in 2021 as below (Yang, 2022).

1. Pig Butchering Scam
2. Pretending Officer or Acquaintance Fraud
3. Impersonating Public Procuratorate Law or Government Organs Fraud
4. Romance or Friendship Scams
5. Fake Credit Investigation Fraud
6. Click Farming Fraud
7. Fake Online Shop Logistics Customer Service Fraud
8. Loan or Credit Card Fraud
9. Fake Online Shopping or Service Fraud
10. Online Game Product Fraudulent Transaction

Among the numbers 1, 2, 3, 4, 5, 7, and 9 fraud types could be defined as cyber identity theft.

## Romance and Pig Butchering Scam

Romance scammers may approach the target person using well-known social media platforms like Instagram or Facebook or build phoney profiles on dating websites and apps. To gain trust, the con artists establish a rapport by conversing with the target person frequently. Afterwards, fabricate a tale to demand payment.

Pig Butchering Scam is an internet slang like a larger-scale romance scam. The perpetrators of fraud specifically use telecommunications and network information technology to fabricate virtual images to gain the trust of the victim, and then establish an intimate relationship, and finally achieve the purpose of defrauding public and private property. Due to the tight organization, complete industrial chain, long fraud cycle, many victims, and high amount of money involved, this method has attracted social attention.

After finding success in China, some con artists expanded internationally. They build romantic ties with different country victims before persuading them to make false investments (Mandy, 2021). Some criminal groups could recruit the victims of the scam and build their teams. These cyber slaves could move across different nations and be forced to do the work (Erin et al, 2022).

## Impersonating Officer, Acquaintance, Public Procuratorate Law or Government Organs Fraud

After the swindler obtains the victim's mobile phone address book and other relevant information through illegal channels, fake acquaintances or leaders take the initiative to add the victim's friends through messenger, use a caring tone to reduce the victim's vigilance, and even offer to help the victim solve difficulties. After defrauding the victim's trust, the liar will take advantage of the situation to ask for a variety of transfer and remittance requests, such as borrowing money, giving gifts, and treating guests, thereby defrauding money.

Fraudsters will also pretend to be government officials from different departments, and commit fraud on the grounds of receiving subsidies, and scholarships, freezing medical insurance cards, securities, and financial accounts, and abnormal or invalid entry and exit documents. They even pretend to be disease control staff or the Department of Health during the COVID-19 period (GOV.HK, 2021).

## Fake Credit Investigation, Online Shopping, Logistics or Customer Service Fraud

Fraudsters publish product advertisement information through webpages, text messages, phone calls and other channels, usually using discounts, overseas purchasing, low-cost transfers, credit issues or free shopping as bait to induce victims to contact them. After the victim pays, the victim will be blocked or lose contact; or tricking the victim into transferring money and committing fraud on the grounds of additional tariffs, deposits, transaction taxes, handling fees, etc.

# Rights and Ethics

## Internet Regulation and Censorship

China ranks among the top nations with the highest rating for censorship. The entire internet is heavily censored and under their iron grasp. The usage of western social media, porn, torrents, VPNs, VoIP programs, and messaging services are all prohibited. The government heavily censors and shapes all of the political media that is published in the nation. Banned messaging applications from other countries as well, forcing citizens to use domestically produced (and probably governed) ones instead, like WeChat in China. WeChat not only lacks end-to-end encryption and includes backdoors that allow other parties to view communications (Paul, 2022).

The Civil Rights and Livelihood Watch website has documented several instances of activists and petitioners being imprisoned in their homes, forced deported, and jailed before the 20th Communist Party Congress. The website also reported on human rights abuses in China throughout this congress. Many have received sentences of up to 15 days in prison for the ill-defined offence of "picking fights and causing problems". The Ministry of Public Security reported two weeks before the congress that 1.43 million individuals had been detained due to sharing or sending the image of the protest banner on social media starting in June (Verna, 2022).

## Liberty and National Security

Internet restriction might be useful from a security perspective in tracking down and identifying criminal or prospective threats. From a standpoint of rights and ethics, the government is required to establish a balance between liberty and national security, avoiding the impression that censorship is being applied unfairly for political reasons.

# The National Law’s Effectiveness

## Restriction on Anonymous Posts

The new set of rules intended to ban anonymous user posts on online forums and other channels was unveiled in 2017 by the nation's chief internet censor. On October 1st, 2017, the Cyberspace Administration of China (CAC) began implementing these regulations (CAC, 2017). When users register, internet corporations and service providers must ask for and confirm their genuine identity and quickly report any unlawful material to the authorities. Additionally, the CAC clarified what content is prohibited from publication in the new rules on anonymous posts, citing a section of a law that was issued in 2000 to control Internet information services in China (CAC, 2017).

## National Standards for Cybersecurity and Data Protection

In 2021, China emphasised government sovereignty over cyberspace and data by implementing various laws and regulations, modernizing its security and data policy quickly, and developing national standards for data protection and cybersecurity. The PRC Constitution, Civil Code, and National Security Law are the three well-established legal foundations upon which privacy rights and security principles are based. These pillars include the Cybersecurity Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL).

Both the DSL and the PIPL assert extraterritorial authority to safeguard the data and private information handled by CSL-protected infrastructure. A secure management system is required for data throughout its lifespan, including its collection, storage, usage, processing, transmission, supply, and disclosure. Every step of the workflow and every individual business operation should include data security management (NPC, 2021).

### CSL

Due to its establishment of the whole security infrastructure, the CSL is essential to cyberspace sovereignty. The CSL enhances the multi-level protection standards for networks and information systems. Network application operators are required to evaluate their network applications and associated risks under the Multi-Level Protection Scheme 2.0 (MLPS 2.0) regime. Each application is given a "security level" based on the nature, significance, and severity of any potential negative effects if it is compromised (CAC, 2021).

### DSL

The DSL intends to safeguard the security of collected information and will penalize any data processing carried out outside of the PRC if it compromises the public interest, national security, or any legitimate rights and interests of any Chinese organization or citizen.

According to the significance of data to economic activity, national security, the interests of society, as well as the possible severity of harm in the event of a security breach, the DSL defines a basic requirement on data classification protection and management. The top tier of the three-tier structure is core data, it is subject to the toughest security measures and is anticipated to be chosen by central government entities. Data categorization and classification will be used to complete and fully execute DSL development throughout all sectors and administrative areas (NPC, 2021).

### PIPL

The objective of PIPL is to control how personal information is processed and maintenance of compliance across the lifecycles of data. Data collection is the first step in the lifecycle of data, making it essential for total compliance. Whether the source of the data is legitimate is a frequently asked question by stock exchanges, regardless of whether the data were actively acquired or purchased. Stock exchanges frequently concentrate on whether the real extent of data use for firms wishing to list exceeds the pre-agreed restriction. Therefore, it is necessary to analyse and review the source, category, collecting method, and authorization.

The stock exchanges will assess whether a company's data processing practice is significantly different from industry practice and if industry practice in turn complies with the legislation if data processing is an integral part of its core business (NPC, 2021).

## Effectiveness

It is highly effective to find and trace most cybercriminals by requiring actual names for registration and prohibiting anonymous posting. Additionally, the international ramifications were defined in the National Standards for Cybersecurity and Data Protection. Many criminal organizations must relocate their bases outside of China or focus on non-China applications.

Therefore, the citizen data that has been acquired must be protected. According to two hackers claimed they stole data on 48.5 million users of the Shanghai COVID app in August 2022 (Sarah, 2022) and one billion Chinese citizens from the Shanghai police database in July 2022 respectively (The Standard, 2022). The Shanghai administration, public security, and Alibaba have not commented on the related police database issue, despite that these data leaks have not been proven.

# Investigative Tools

Since identity theft on mobile devices is on the rise, it is challenging for mobile investigative procedures and technology to generate trustworthy results for international investigations. A fresh branch of digital forensics that has lately grown in prominence is mobile forensics. Since mobile forensics may facilitate the prompt and effective production of digital evidence or relevant data in circumstances connected to litigation or investigations.

Concerns over data security and human rights led Cellebrite, the top producer of forensics equipment in the world, to withdraw from the China market in 2020. Cellebrite claims to only pursue customers that they believe will behave morally and not in a way that would violate human rights or privacy (Cellebrite, 2020).

On the other hand, it is challenging to investigate each type of mobile phone made by various Chinese phone makers. Furthermore, the increase in the use of counterfeit Chinese knockoff phones by criminals makes forensic analysis more difficult. Internal flash storage, like other smartphones, acts as the main component for data storage in knockoff phones. However, it is hard to find any official documentation for such phones, especially when it comes to flash storage, file systems, and other details concerning the phones' storage capabilities. Additionally, there has not been much research on knockoff phone forensics published, so it can be particularly challenging to retrieve evidence from Chinese phones (Junbin et al., 2012).

Nevertheless, instead of analysing the devices, it is far more effective to use the data gathered from the service providers, network providers, banks, public security, or the government within China. In the cross-border case handled by the Supreme People's Procuratorate (SPP), it was demonstrated that the investigator was able to gather any electronic data on other countries, as well as extract and recover any chat logs, Excel, and Word files relevant to the case. The list of internet phone calls as well as other non-contaminated identified data (SPP, 2021).

# Aspects Concerning

## Victims

Data from the National Anti-Fraud Center shows that among the victims of telecom and internet fraud in 2021, 2% are under the age of 18; 65.5% are 18 to 35; 31.3% are 36 to 59; 1.4% are 60 and over. It stated that it is due to the lack of secure income for young people and the abundance of online incentives to purchase. Young people who looking for quick money will fall victim to scams (Public Security of Shantou, 2022).

## Harm

In 2021, the National Anti-Fraud Center effectively prevented over 2800 fraud attempts, intercepted 1.55 billion fraud calls, and halted over CNY 320 billion that was engaged in the case that year. The public security organs uncovered over 441,000 telecom and internet fraud cases, demolished 39,000 unlawful and criminal gangs, detained more than 690,000 criminal suspects, and recovered and returned CNY 12 billion in defrauded funds to the people (Public Security of JiLin, 2022).

The reporter of Xinwen News Agency learned from the Ministry of Public Security that from April 2021 to July 2022, a total of 594,000 telecom and internet fraud cases were cracked nationwide. The continuous upward trend of telecom and network fraud crimes has been effectively curbed in recent years. (GOV.CN, 2022)

## Perpetrator

The characteristics and trends of information-related cybercrime reports show that from 2017 to 2021, more than 660,000 defendants were involved in cybercrime cases, and the average number of defendants involved in each cybercrime case was about 2.4. The age of the defendants is mainly concentrated between 18 to 39 years old, and the proportion of 29 years old and above is decreasing year by year. (China Youth Daily, 2022)

## Social Perception

Besides the social perception education by the government, China currently has the most extensive surveillance network in the world. Facial recognition is frequently used in daily life and the AI-driven policing was promoted. The Chinese government aspires to keep tabs on and regulate residents' offline behaviour in addition to monitoring, directing, and controlling internet behaviour. Cameras are present in most public areas. Long-distance public transport is only permitted with real-name registration and identity verification.

The rise in the number of secure residential areas and cities is a significant indicator. These show a desire to enhance social governance with a focus on promoting "social stability" as well as building a seamless and secure cyberspace in China (Katja & John, 2021).

# Conclusion

Cyber identity crime may decline due to the rapidly growing regulatory and censorship system. In comparison, the strident attempts to limit free speech and disregard data privacy regulations violate laws and moral standards elsewhere.

To facilitate the investigation of cybersecurity and the gathering of electronic evidence, the United Nations should motivate them to conduct discussions with other states to improve international judicial support and enforcement collaboration by optimizing pertinent procedures or other methods. It should consider adopting international model clauses on the investigative power on the gathering of electronic evidence and investigate the prospect of drafting a legally enforceable international instrument for combatting cybercrime within the framework of the United Nations.

# References

Brett, M. (April 26, 2021) The Limits of Free Speech in Social Media. *Constitutional Law*. Available from: https://accessiblelaw.untdallas.edu/limits-free-speech-social-media [Accessed 1 Oct 2022].

CAC. (August 25, 2017) Provisions on the Administration of Internet Forum Community Services. *China Netcom*. Available from: http://www.cac.gov.cn/2017-08/25/c\_1121541921.htm [Accessed 29 Oct 2022].

CAC. (August 25, 2017) The relevant person in charge of the Cyberspace Administration of China answers reporters' questions on the "Regulations on the Administration of Internet Forum Community Services". *China Netcom*. Available from: http://www.cac.gov.cn/2017-08/25/c\_1121541845.htm [Accessed 29 Oct 2022].

CAC. (June 11, 2021) Data Security Law of the People's Republic of China. *Xinhua News Agency*. Available from: http://www.cac.gov.cn/2021-06/11/c\_1624994566919140.htm [Accessed 29 Oct 2022].

Cellebrite. (October 7, 2020) Cellebrite Provides Facts About its Business and Solutions. *Cellebrite Facts*. Available from: https://cellebrite.com/en/cellebrite-facts/ [Accessed 8 Oct 2022].

China Youth Daily. (August 1, 2022) Information Network Crime Big Data Report Released: In the past five years, nearly 90% of the defendants in the crime of 'helping trust' were born in the 1980s and 1990s. *Client of China Youth Daily*. Available from: https://baijiahao.baidu.com/s?id=1739958869723814808&wfr=spider&for=pc [Accessed 29 Oct 2022].

Clifford, L. (June 14, 2020) Coronavirus: Hongkongers lose HK$222 million in romance and telephone scams during Covid-19 crisis. *Scams and swindles*. Available from: https://www.scmp.com/news/hong-kong/law-and-crime/article/3088944/coronavirus-hongkongers-lose-hk222-million-romance-and [Accessed 29 Oct 2022].

Erin, H. et al. (September 15, 2022) Inside the 'pig-butchering' scams seeing thousands trafficked into cyber slavery. *News*. Available from: https://www.abc.net.au/news/2022-09-16/cambodia-human-trafficking-online-scam-pig-butchering/101407862 [Accessed 29 Oct 2022].

GOV.CN. (August 17, 2022) The number of telecommunications and network fraud cases on file has dropped year-on-year for 14 consecutive months. *Xinhua*. Available from: http://www.gov.cn/xinwen/2022-08/17/content\_5705790.htm [Accessed 29 Oct 2022].

GOV.HK. (April 16, 2021) DH alerts public to fraudulent phone calls and emails purporting to be made by DH. *Press Releases*. Available from: https://www.info.gov.hk/gia/general/202104/16/P2021041600730.htm?fontSize=1 [Accessed 29 Oct 2022].

Junbin, F. et al. (2012) Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones. *DigitalForensics 2012: Advances in Digital Forensics VIII: 129–142*. Available from: https://link.springer.com/chapter/10.1007/978-3-642-33962-2\_9 [Accessed 8 Oct 2022].

Katja, D. & John, L. (June 15, 2021) The CCP in 2021: smart governance, cyber sovereignty and tech supremacy. *Mercator Institute for China Studies*. Available from: https://merics.org/en/ccp-2021-smart-governance-cyber-sovereignty-and-tech-supremacy [Accessed 29 Oct 2022].

Mandy, Z. (September 30, 2021) Online 'pig butchering' love scams have gone global after getting their start in China. *Scams and swindles*. Available from: https://www.scmp.com/news/people-culture/social-welfare/article/3150688/online-pig-butchering-love-scams-have-gone [Accessed 29 Oct 2022].

NPC. (December 29, 2021) Personal Information Protection Law of the People's Republic of China. *Laws*. Available from: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c\_694559.htm [Accessed 29 Oct 2022].

NPC. (June 10, 2021) Order of the President of the People's Republic of China No. 84. *Data Security Law of the People's Republic of China*. Available from: http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml [Accessed 29 Oct 2022].

Paul, B. (January 25, 2022) Internet Censorship 2022: A Global Map of Internet Restrictions*. Internet Studies*. Available from: https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/ [Accessed 1 Oct 2022].

Public Security of JiLin. (March 10, 2022) In 2021, the National Anti-Fraud Center will urgently stop paying more than 320 billion yuan of funds involved in the case. *Jilin Provincial Public Security Department*. Available from: http://gat.jl.gov.cn/jwzx/gayw/202203/t20220310\_8409625.html [Accessed 29 Oct 2022].

Public Security of Shantou. (April 27, 2022) National Anti-Fraud | Young people are more likely to be scammed by telecommunications? Believe it or not, it's true. *Shantou Public Security Bureau*. Available from: https://www.shantou.gov.cn/gaj/zwgk/gzdt/content/post\_2056349.html [Accessed 29 Oct 2022].

Sarah, Z. (July 4, 2022) Hackers Claim Theft of Police Info in China's Largest Data Leak. *Technology Cybersecurity*. Available from: https://www.bloomberg.com/news/articles/2022-07-04/hackers-claim-theft-of-police-info-in-china-s-largest-data-leak [Accessed 29 Oct 2022].

SPP. (May 18, 2021) Zhang Kaimin and other 52 people in telecom and network fraud case. *Fully perform the function of legal supervision and severely punish the crime of telecommunication and network fraud in accordance with the law*. Available from: https://www.spp.gov.cn/spp/dxwlzp2021/202105/t20210518\_518480.shtml [Accessed 29 Oct 2022].

Stephen, C. (March 31, 2016) Hundreds arrested in 'guess who I am' phone scam probe in China. *China society*. Available from: https://www.scmp.com/news/china/society/article/1932215/hundreds-arrested-guess-who-i-am-phone-scam-probe-china [Accessed 29 Oct 2022].

The Standard. (August 12, 2022) Hacker tries to sell data of 48.5m users of Shanghai's Covid app. *China*. Available from: https://www.thestandard.com.hk/breaking-news/section/3/193410/Hacker-tries-to-sell-data-of-48.5m-users-of-Shanghai%27s-Covid-app%C2%A0 [Accessed 29 Oct 2022].

Verna, Y. (October 14, 2022) Dissidents in China detained and harassed as Beijing prepares for party congress. *China*. Available from: https://www.theguardian.com/world/2022/oct/14/dissidents-in-china-detained-and-harassed-as-beijing-prepares-for-party-congress [Accessed 29 Oct 2022].

Yang, F. (March 6, 2022) Analysis of the development status and development suggestions of China's telecom network fraud in 2021. *Zhiyan point of view*. Available from: https://www.chyxx.com/industry/1100459.html [Accessed 29 Oct 2022].