INTERNATIONAL MONETARY FUND

The Rise of Cyber Events and Digital Fraud in the Financial Sector

Tanai Khiaonarong and Shanyuan Zheng

WP/26/62

2026
MAR

WORKING PAPER

WP/26/62

IMF Working Paper
Monetary and Capital Markets Department

The Rise of Cyber Events and Digital Fraud in the Financial Sector

Prepared by Tanai Khiaonarong and Shanyuan Zheng*

Authorized for distribution by Jay Surti
March 2026

IMF Working Papers **describe research in progress by the author(s) and are published to elicit comments and to encourage debate.** The views expressed in IMF Working Papers are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

ABSTRACT: Cybersecurity and digital fraud are closely intertwined in financial services, as vulnerabilities in digital systems enable both institutional cyber incidents and fraud against users. This paper uses publicly available data to review and examine important trends underlying the growing concern of digital fraud. The results indicate that, across 20 industry sectors in 162 countries, cyber events in the financial sector accounted for about 10 percent over the past decade and were concentrated primarily in the banking and securities sectors. Cyber-enabled fraud has nearly tripled but remains underestimated due to underreporting and data gaps across jurisdictions. Credit transfers and credit cards dominate scam payments, with rising reports of payment fraud in some jurisdictions alongside increased crypto-related cyber events and fraud. Industry studies also suggest that scam losses represent a higher share of gross domestic product in developing economies, while advanced economies tend to incur higher individual losses. Targeted regulatory and infrastructure measures have been taken to strengthen trust in digital finance in some jurisdictions.

RECOMMENDED CITATION: Khiaonarong, T., and Shanyuan, Z. (2026) The Rise of Cyber Events and Digital Fraud in the Financial Sector, IMF Working Paper WP/26/62.

JEL Classification Numbers:	E5, G21, G22, G23, G28, K4, M15
Keywords:	Banks; cyber events; cyber-enabled fraud; digital fraud; financal sector; payment fraud
Author’s E-Mail Address:	tkhiaonarong@imf.org; szheng@imf.org

* The authors would like to thank Tohid Atashbar, Tobias Lindqvist, Majid Malaika, Garth Nicholls, Anca Paduraru, Marco Reuter, Puja Singh, Frankosiligi Solomon, Jay Surti, Tomohiro Tsuruga, and Ying Xu for providing comments on an earlier version of the paper. Marie-Bernadette Amand de Mendieta provided editorial assistance.

WORKING PAPERS

The Rise of Cyber Events and Digital Fraud in the Financial Sector

Prepared by Tanai Khiaonarong and Shanyuan Zheng[1]

[1] The authors would like to thank Tohid Atashbar, Tobias Lindqvist, Majid Malaika, Garth Nicholls, Anca Paduraru, Marco Reuter, Puja Singh, Frankosiligi Solomon, Jay Surti, Tomohiro Tsuruga, and Ying Xu for providing comments on an earlier version of the paper. Marie-Bernadette Amand de Mendieta provided editorial assistance.

Contents

ANNEX

FIGURES

TABLES

Introduction

Analyzing the threat landscape is a critical part of understanding the nature, scope and intensity of cyber risks in the financial sector. This task is rendered challenging for several countries due to incomplete and missing information regarding incidence of cyber-attacks and digital fraud, fragmented sourcing, recording and storage of information of such events, inadequate frameworks for cybersecurity incident reporting, and arrangements for domestic and cross-border information sharing.

The IMF's recent study of the macrofinancial stability implications of cyber risk found that almost one-fifth of reported cyber incidents during 2004 and 2023 impacted the financial sector, with banks being the most frequent targets followed by insurers and asset managers (IMF, 2024). The number of cyberattacks has almost doubled relative to the period before the COVID-19 pandemic.

Few jurisdictions have a generic threat landscape report or one that is tailor-made for the financial sector. Where data is available, this is often from multiple official sources which could have conflicting or missing information. To increase awareness of the cyber threat landscape and protect the public, law enforcement agencies in some jurisdictions monitor and publish progress and statistics to address scams, fraud, and cybercrime. Such efforts have helped address cyber-enabled fraud in the face of rapid growth in digital finance, including specific areas like online digital payments and cryptocurrency activities.

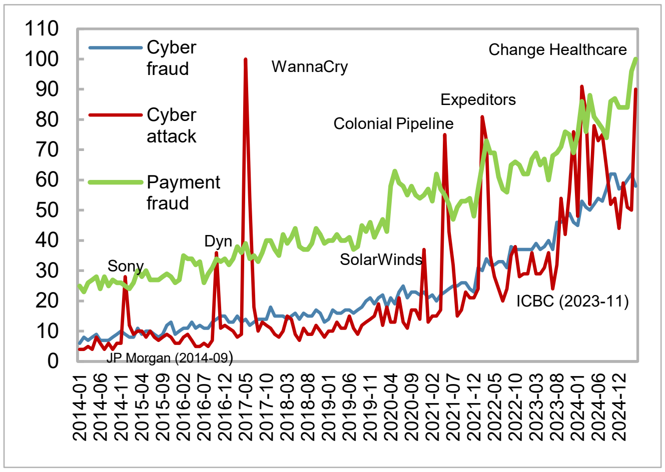
Threat intelligence information is typically obtained from public agencies and private sector firms. In some jurisdictions, information on cybersecurity incidents is collected, administered, and shared by the national Computer Emergency Response Team (CERT). This often covers all economic sectors, including the financial sector. For some jurisdictions, cyber threats in the financial sector are also reported through regional efforts.[2] Financial sector authorities also collect information on cybersecurity incidents through regulatory reporting by supervised entities. Private sector firms have service offerings that provide threat intelligence to financial sector authorities and entities.

Information on cybersecurity incidents is often confidential and market sensitive. Therefore, such information is not publicly available or would require access to a service offered by a private sector agency. Under many circumstances, information such as the number of cyber-attacks may also lack consistency due to differences in the taxonomy used to define a cyber incident. This complicates the analysis of the cyber threat landscape, and as such, has led to efforts by international standard-setting bodies to establish a common cyber lexicon and approach to achieving greater convergence in cyber incident reporting. Such efforts resonate with the gradual increase of interest over time in internet searches of "cyber attack", with peaks occurring during events that had potential to create widespread and global disruptions (Figure 1).[3] Similarly, "cyber fraud" and "payment fraud" searches have trended upwards during the same period.

[2] The European Union Agency for Cybersecurity and the Nordic Financial CERT are examples of regional efforts to publicly report on the cyber threat landscape for the financial sector. See ENISA (2024) and Nordic Financial CERT (2024).

[3] Interest over time is a methodology used by Google which finds the period with the most searches and assigns it a score of "100" over the given time frame. Interest during other periods is then calculated in relative terms.

Figure 1. Cyber Attack, Cyber Fraud, and Payment Fraud Interest Over Time, 2014–2024



Source: Google trend analysis

We explore cyber events and digital fraud to help us understand the evolving threat landscape in this paper. Cyber events are largely aimed at financial organizations. Digital fraud includes cyber-enabled and payment-related fraud that target the wider public. Cybercrime is often reported by victims to law enforcement agencies. Payment fraud is reported by regulated entities to financial authorities. The objective is to use publicly available data on cyber events and digital fraud to review developments over the past decade and examine trends.

The paper is organized as follows. Section 2 describes the data and methodology. Section 3 explores cyber events in the financial and ICT sectors, analyzing data and trends at the sector-level. Section 4 reviews trends in digital fraud—covering cyber-enabled and payment-related fraud—at the aggregate level and in selected jurisdictions. Section 5 concludes.

Data and Methodology

The analysis in this paper is based on three major sources of publicly available information, including (i) the Cyber Events Database of the Center for International and Security Studies at Maryland (CISSM), University of Maryland; (ii) the cyber-enabled fraud database from the United Nations Office on Drugs and Crime (UNODC) and jurisdictions[4] that publicly report cybercrime; and (iii) payment-related fraud. This provides a comprehensive approach towards analyzing the threat landscape and trends in cyber-enabled events and digital fraud in finance (Figure 2).

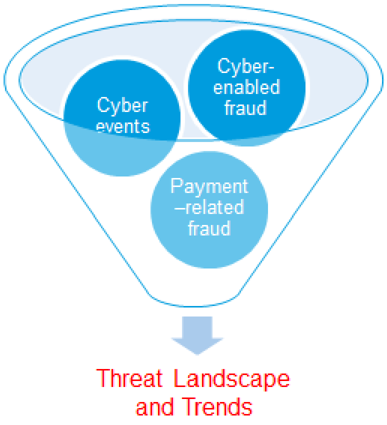
[4] The jurisdictions referenced here include Canada, the United States, the United Kingdom, the European Union, and India.

Cyber Events

The Cyber Events database (CISSM) collects publicly available information on cyber events, has sufficient information on cyber events in the financial and information and communications technology (ICT) sectors that are highly relevant to the objectives of this study, and provides a consistent and well-structured approach to support strategic decision-making and response to cyber events.[5] Other databases are also publicly available.[6]

An important caveat to note is that while the database is comprehensive, it may not capture all cyber events reported globally as the original source of information may have been publicized exclusively in local languages. The database also provides historical and time-series data for research purposes, albeit lacks the timeliness and technical details, such as the tactics, techniques and procedures used by criminals to plan and execute cyberattacks.

Figure 2. Framework for Analyzing Cyber Events and Digital Fraud



The Cyber Events Database is guided by a cyber event taxonomy, where a cyber event refers to "*the result of any single unauthorized effort, or the culmination of many such technical actions, that engineers, through use of computer technology and networks, a desired primary effect on a target*" (Harry and Gallagher, 2018).

This taxonomy guides this paper. Based on this taxonomy, a given cyber event is interpreted as having one of two types of primary objectives. The first objective is to disrupt the functions of the target organization. Disruptive effects themselves can be classified into five sub-categories, i.e., message manipulation; external denial of service; internal denial of service; data attack; and physical attack. The second objective is to exploit or steal information, including customer data; intellectual property; classified national security information; and sensitive details about the organization itself. Exploitative effects can themselves be further classified into five sub-categories, including exploitation of: sensors, end hosts, infrastructure, application servers, and data in transit. Using this taxonomy, cyber events were collected from systematic web searches and the results coded to include *date*; *event type*; *organization type*; *event description*; and (a link to) *the source* (Harry et al., 2023). For organization types, coding was guided by the North American Industrial Classification System (NAICS) (Annex I).[7]

[5] The Cyber Events Database has been leveraged by central banks (Bank of Japan, Banco de España, Deutsche Bundesbank, European Central Bank); supervisory authorities (European Securities and Markets Authority); standard setting bodies (National Institute of Standards and Technology); and international organizations (World Bank Group). IMF staff have also utilized this database for bilateral and multilateral surveillance of the financial sector.

[6] The European Repository of Cyber Incidents (EuRepoC) is an independent research consortium that provides evidence-based analysis of cyber incidents. The Carnegie Endowment for International Peace (CEIP) provides a timeline of cyber incidents involving financial institutions.

[7] In principle, classification is also possible under the various financial services activities as defined in the Annex on Financial Services of the General Agreement on Trade in Services of the World Trade Organization.

Before probing further, a basic understanding of the data is important to provide context. Following our minor adjustments, there were a total of 14,055 cyber events recorded during the period January 2014 to December 2023 in the Cyber Events Database.[8] This represents data from 162 jurisdictions spread across 20 industry sectors. During this sampling horizon, there were 1,246 cyber events in the financial sector, which represented 9 percent of the total number of cyber events. Notably, during this 10-year period, the share of cyber events in the financial sector doubled from 6 percent in 2014 to 13 percent in 2023.

At the aggregate level, the top five industry sectors where the share of cyber events were large were for public administration (18 percent); health care and social assistance (13 percent); ICT (10 percent); educational services (10 percent); and finance and insurance (9 percent) (Table 1).[9] A majority of cyber events were exploitative (54 percent) though the share of disruptive events was also significant, at 46 percent. Exploitative methods were largely targeted at the application servers (40 percent) and end hosts (11 percent) of target organizations. Comparatively, disruptive methods were largely through message manipulation (9 percent) and external denial of service (11 percent).

Table 1. Cyber Events by Type and Industry Sector, 2014-23

		Disruptive Effects *(Percent)*					Exploitative Effects *(Percent)*					
Sector	**Observations**	**Message Manipulation**	**External Denial of Service**	**Internal Denial of Service**	**Data Attack**	**Physical Attack**	**Exploitation of Sensors**	**Exploitation of End Hosts**	**Exploitation of Network Infrastrucutre**	**Exploitation of Application Server**	**Exploitation of Data in Transit**	**Share of all Events** *(Percent)*
Accommodation and Food Services	298	0.07	0.04	0.04	0.37	0.00	0.59	0.16	0.01	0.83	0.02	2.12
Administrative and Support and Waste Management and Remediation Services	165	0.02	0.16	0.01	0.29	0.00	0.00	0.07	0.01	0.61	0.01	1.17
Agriculture, Forestry, Fishing and Hunting	23	0.01	0.02	0.00	0.08	0.00	0.00	0.00	0.00	0.06	0.00	0.16
Arts, Entertainment, and Recreation	420	0.68	0.35	0.01	0.36	0.01	0.06	0.31	0.01	1.20	0.01	2.99
Construction	46	0.00	0.05	0.00	0.21	0.00	0.00	0.00	0.00	0.07	0.00	0.33
Educational Services	1379	0.91	0.54	0.12	3.32	0.01	0.03	0.98	0.02	3.87	0.01	9.81
Finance and Insurance	1246	0.32	1.45	0.04	1.26	0.00	0.18	1.05	0.06	4.35	0.16	8.87
Health Care and Social Assistance	1877	0.18	0.27	0.09	4.35	0.01	0.02	2.15	0.06	6.22	0.01	13.35
Information	1446	1.46	1.94	0.11	1.32	0.04	0.02	0.97	0.18	4.17	0.07	10.29
Management of Companies and Enterprises	25	0.01	0.01	0.00	0.06	0.00	0.00	0.01	0.00	0.08	0.01	0.18
Manufacturing	637	0.16	0.42	0.04	2.16	0.03	0.01	0.31	0.01	1.38	0.01	4.53
Mining, Quarrying, and Oil and Gas Extraction	73	0.04	0.04	0.01	0.16	0.04	0.00	0.04	0.00	0.21	0.00	0.52
Other Services (except Public Administration)	1019	1.33	0.65	0.02	0.70	0.00	0.06	1.49	0.00	2.87	0.12	7.25
Professional, Scientific, and	1174	0.24	0.29	0.06	2.72	0.00	0.04	0.59	0.11	4.29	0.02	8.35
Public Administration	2646	3.12	3.62	0.18	3.76	0.06	0.06	2.20	0.09	5.68	0.06	18.83
Real Estate and Rental and Leasing	89	0.05	0.04	0.01	0.19	0.01	0.00	0.05	0.01	0.28	0.01	0.63
Retail Trade	472	0.06	0.10	0.01	0.77	0.01	0.20	0.44	0.01	1.76	0.01	3.36
Transportation and Warehousing	439	0.16	0.91	0.05	0.86	0.08	0.02	0.12	0.01	0.90	0.01	3.12
Utilities	269	0.05	0.28	0.02	0.63	0.21	0.00	0.10	0.01	0.61	0.01	1.91
Wholesale Trade	104	0.01	0.10	0.01	0.25	0.00	0.01	0.05	0.00	0.31	0.00	0.74
Undetermined	208	0.03	0.11	0.01	0.48	0.01	0.02	0.14	0.01	0.67	0.00	1.48
All Industries	14055	8.89	11.38	0.83	24.30	0.51	1.32	11.21	0.60	40.41	0.53	100.00

Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

Note: Adjustments were made to the number of observations to account for mixed types of cyber events.

[8] The Cyber Events Database recorded 13,407 cyber events during January 2014 to December 2023 for all sectors. Our adjustments, for all sectors, involved classifying some events as mixed types. For example, an event was classified as both "Data Attack" and "Exploitation of Application Server"). In such cases, we counted them separately for each category. To improve the accuracy of data analysis and reduce interference factors, we also removed events classified as "Undefined." As a result, we identified a total of 14,055 distinct events. The adjustment follows the approach taken by Harry and Gallagher (2018, page 9) which notes: "In complex cases where the victim suffered multiple effects (e.g. website defacement and DDoS), the dataset counts each effect as a separate, but overlapping, event registered to the victim."

[9] Percentages are rounded.

Digital Fraud

Digital fraud is covered here because of its relevance for regulated financial institutions, including operational, reputational, and payment system risks. Digital fraud risks also arises with the widespread use of digital financial services and social media platforms where users of financial services could be victimized. This has particularly been evident for fraud associated with payment services provided by banks and payment service providers.

Cyber-Enabled Fraud

The UNODC collects and reports data on corruption and economic crime, including cyber-related fraud. Data are collected from national authorities through the annual United Nations Crime Trends Survey and the methodology is guided by the International Classification of Crimes for Statistical Purposes (ICCS), providing useful statistics on counts at the country-level (UNODC, 2023). After the adoption of the ICCS in 2015, many countries have started to report data that correspond more closely to ICCS categories.

Additionally, the UNODC also provides a cybercrime repository that includes databases for legislation, case law, and lessons learned. Fraud is generally referred to as '*obtaining money or other benefit or evading a liability through deceit or dishonest conduct' while cyber-related fraud occurs 'if the use of computer data or computer systems was an integral part of the modus operandi of the crime*' (UNODC, 2024). The ICCS analyzes cybercrime and other information and communications technology (ICT) use for criminal purposes through a classification that facilitate the measurement of *cyber-dependent crimes* and *cyber-enabled crimes*.[10] For the purpose of this report, we use data on cyber-enabled crimes. While 60 jurisdictions have reported cyber-related fraud statistics to the UNODC, and some, like India and the United States (U.S.) have made these publicly available, as of April 2025, only 13 countries have reported sufficient data over a 10-year period to make the study of cyber-related fraud trends possible.[11]

Payment-Related Fraud

Some jurisdictions have made data available publicly on payment-related fraud. We review official sources from Canada, the European Union, India, the United Kingdom (U.K.), and the U.S.[12]

Methodology and Limitations

The use of statistical data enables the analysis of the occurrence of, and trends in cyber events and cyber-enabled fraud. However, this is subject to the following limitations. First, we are guided by "cyber-enabled fraud" as defined by the UNODC. For the purpose of this paper, this term is interchangeable with digital fraud, which has been used by the Basel Committee on Banking Supervision (BCBS) for its study into digital fraud in banking and payments. Second, aggregate figures for global cyber-enabled fraud are rough estimates based on cyber-enabled fraud statistics reported by law enforcement agencies to the UNODC. While complete

[10] The ICCS defines cyber-dependent crimes as "offences that target a computer or a computer system per se. These crimes can only be committed through an ICT infrastructure and are often criminalized as unauthorized access to, interception of, interference with, or misuse of computer data or computer / information systems." Cyber-enabled crimes are "offences where computers are used to commit traditional crimes such as theft, harassment or fraud. These are offences that can be committed without a computer but can also be facilitated by ICTs." (UNODC, 2023).

[11] In particular, the National Crime Records Bureau of India's Ministry of Home Affairs publishes an annual report on Crime in India, which includes statistics on cybercrime cases. The Singapore Police Force publishes mid-year scams and cybercrime briefs. The United Kingdom Action Fraud publishes fraud and cybercrime national statistics. The Internet Crime Compliant Center (IC3) of the U.S. Federal Bureau of Investigation (FBI) publishes annual reports on internet crime, which includes statistics on cyber complaints. IC3 fraud reports also focus on elder fraud and cryptocurrency fraud.

[12] This list is non-exhaustive. For other jurisdictions, see Basel Committee on Banking Supervision (2023).

statistics are available from many countries, there is also data missing for several jurisdictions for our 10-year sampling window. Importantly, a common issue faced by many jurisdictions is the under-reporting or non-reporting of fraud by victims to law enforcement agencies. Third, cross-country comparisons should be treated with caution. As guided by the UNODC, differences still exist between the legal definitions of offences in countries, the methodology of counting and recording offences, and reporting rates. Therefore, these caveats should be observed while making cross-comparisons. Fourth, a cause-and-effect analysis across the three data sources—cyber events, cyber-enabled fraud, and payment fraud—is not practicable although there could be possible interrelationships.[13] To address some of these limitations, this study also makes references to industry studies and media reports to complement the analysis, where specific events in given jurisdictions are likely relevant. For example, in-depth industry studies by the Global Anti-Scam Alliance (GASA) into fraud and scams have helped provide insights into their impact at the global and country-levels.

Cyber Events

What has the experience been so far with cyber events across jurisdictions? This section analyzes cyber events in the financial sector at the global and subsector levels.

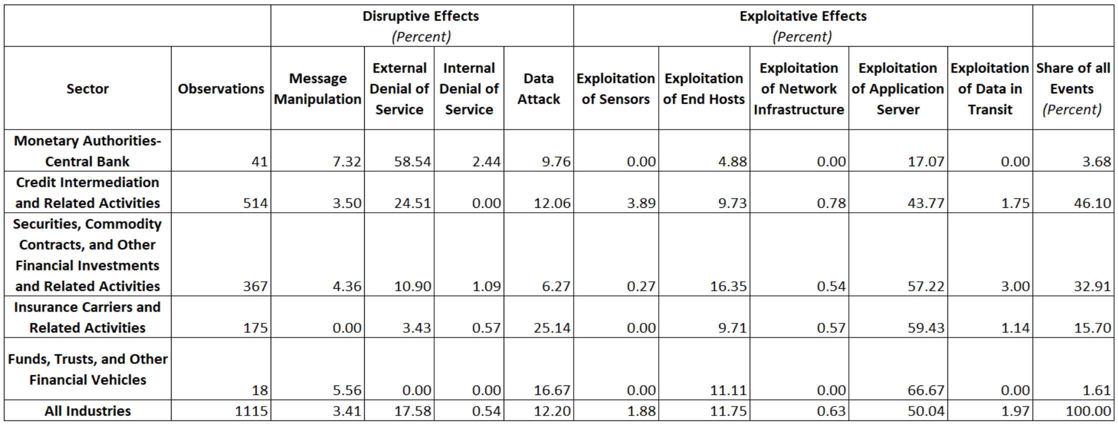
Using NAICS, cyber events classified under the finance and insurance sector were further coded and organized into 5 subsectors, including:[14] (i) monetary authorities (central banks); (ii) credit intermediation and related activities; (iii) securities and commodities markets, other financial investments and related activities, including market intermediaries; (iv) insurance carriers and related activities; and (v) funds (custodial, trustee, and fund administration–related entities), trusts, and other financial vehicles; the organization is based on three principal types of activities and defined based on their unique production processes. During the process to further classify cyber events into subsectors, some items contained insufficient information in the description field to enable validation.

At the financial sector level, the share of cyber events for each subsector were: monetary authorities (4 percent); credit intermediaries (46 percent); securities and commodities markets and market intermediaries (33 percent); insurance (16 percent); and funds and trusts (1 percent) (Table 2). Cyber events were largely exploitative (66 percent) as compared to disruptive (34 percent) and exploitative methods were largely targeted at application servers (50 percent) and end hosts (12 percent) of target organizations. On the other hand, disruptive methods reflected primarily external denial of service (18 percent) and data attacks (12 percent).

[13] For example, some jurisdictions have reported cyber incidents in the banking sector as possibly caused by a data breach at the national registry where personal information was stolen and sold on the dark web. As a result, this compromised the use of digital payments by affected bank customers.

[14] See also Annex I.

Table 2. Cyber Events in the Financial Sector by Subsector and Type, 2014-23



		Disruptive Effects *(Percent)*				Exploitative Effects *(Percent)*					
Sector	**Observations**	**Message Manipulation**	**External Denial of Service**	**Internal Denial of Service**	**Data Attack**	**Exploitation of Sensors**	**Exploitation of End Hosts**	**Exploitation of Network Infrastructure**	**Exploitation of Application Server**	**Exploitation of Data in Transit**	**Share of all Events** *(Percent)*
Monetary Authorities-Central Bank	41	7.32	58.54	2.44	9.76	0.00	4.88	0.00	17.07	0.00	3.68
Credit Intermediation and Related Activities	514	3.50	24.51	0.00	12.06	3.89	9.73	0.78	43.77	1.75	46.10
Securities, Commodity Contracts, and Other Financial Investments and Related Activities	367	4.36	10.90	1.09	6.27	0.27	16.35	0.54	57.22	3.00	32.91
Insurance Carriers and Related Activities	175	0.00	3.43	0.57	25.14	0.00	9.71	0.57	59.43	1.14	15.70
Funds, Trusts, and Other Financial Vehicles	18	5.56	0.00	0.00	16.67	0.00	11.11	0.00	66.67	0.00	1.61
All Industries	1115	3.41	17.58	0.54	12.20	1.88	11.75	0.63	50.04	1.97	100.00

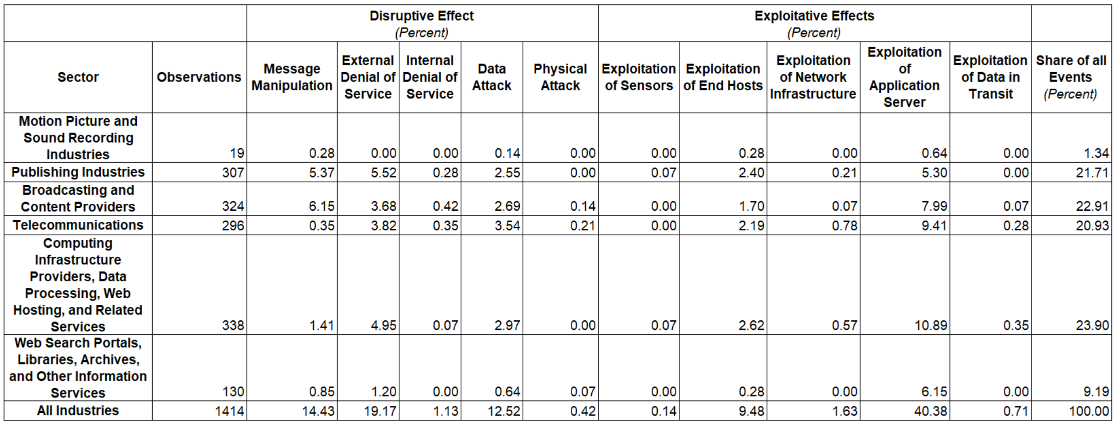
Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

Note: Adjustments were made to the number of observations to account for mixed types of cyber events and undetermined events.

At the subsector level, banking, securities and insurance entities were typically targeted through the exploitation of application servers (respectively, 44 percent, 57 percent and 59 percent).

Given the digitalization of the financial sector and its extensive use of ICT service providers, we also examine cyber events in the ICT sector to check for potential interdependencies (Table 3). Under the ICT sector, we are particularly interested in two subsectors, viz., telecommunications and computing infrastructure providers, data processing, web hosting, and related services. There were 1,414 cyber events in this sector during our sampling horizon, representing 10 percent of total events, with 21 percent of these events impacting telecommunications and 24 percent impacting computing infrastructure. Both sectors represent the ICT sector (45 percent) in this report.

Table 3. Cyber Events in the Information Sector by Subsector and Type, 2014-23



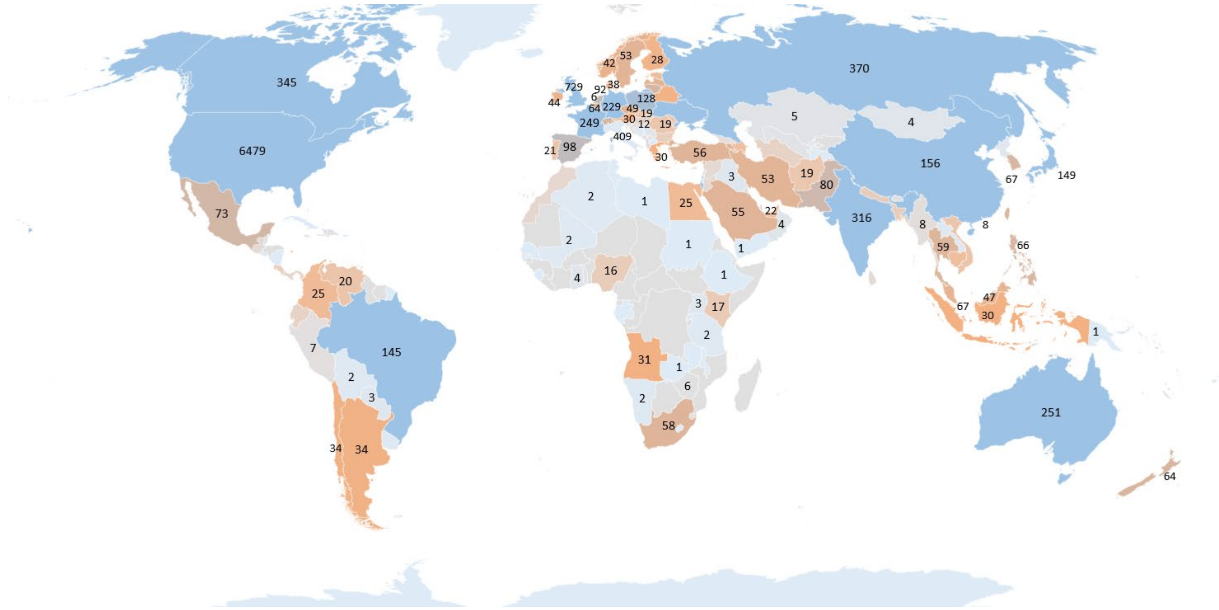
		Disruptive Effect *(Percent)*					Exploitative Effects *(Percent)*					
Sector	**Observations**	**Message Manipulation**	**External Denial of Service**	**Internal Denial of Service**	**Data Attack**	**Physical Attack**	**Exploitation of Sensors**	**Exploitation of End Hosts**	**Exploitation of Network Infrastructure**	**Exploitation of Application Server**	**Exploitation of Data in Transit**	**Share of all Events** *(Percent)*
Motion Picture and Sound Recording Industries	19	0.28	0.00	0.00	0.14	0.00	0.00	0.28	0.00	0.64	0.00	1.34
Publishing Industries	307	5.37	5.52	0.28	2.55	0.00	0.07	2.40	0.21	5.30	0.00	21.71
Broadcasting and Content Providers	324	6.15	3.68	0.42	2.69	0.14	0.00	1.70	0.07	7.99	0.07	22.91
Telecommunications	296	0.35	3.82	0.35	3.54	0.21	0.00	2.19	0.78	9.41	0.28	20.93
Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services	338	1.41	4.95	0.07	2.97	0.00	0.07	2.62	0.57	10.89	0.35	23.90
Web Search Portals, Libraries, Archives, and Other Information Services	130	0.85	1.20	0.00	0.64	0.07	0.00	0.28	0.00	6.15	0.00	9.19
All Industries	1414	14.43	19.17	1.13	12.52	0.42	0.14	9.48	1.63	40.38	0.71	100.00

Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

Note: Adjustments were made to the number of observations to account for mixed types of cyber events and undetermined events.

Cyberattacks exhibit a clear geographical pattern during 2014-2023 (Figure 3). The U.S. stands out, recording 6,479 incidents—far more than any other country—highlighting the highly digitalized nature of its financial services sector as well as its significant exposure to cyber threats. In addition, countries in North America, Western Europe, East Asia, and parts of South Asia have become primary targets. Many of these are global financial hubs, countries with large and rapidly growing financial markets and offerings of digital financial products and services, or increasingly complex digital public infrastructures, factors which could make them more exposed to or vulnerable to cyberattacks. In contrast, emerging markets and developing countries report significantly fewer incidents.

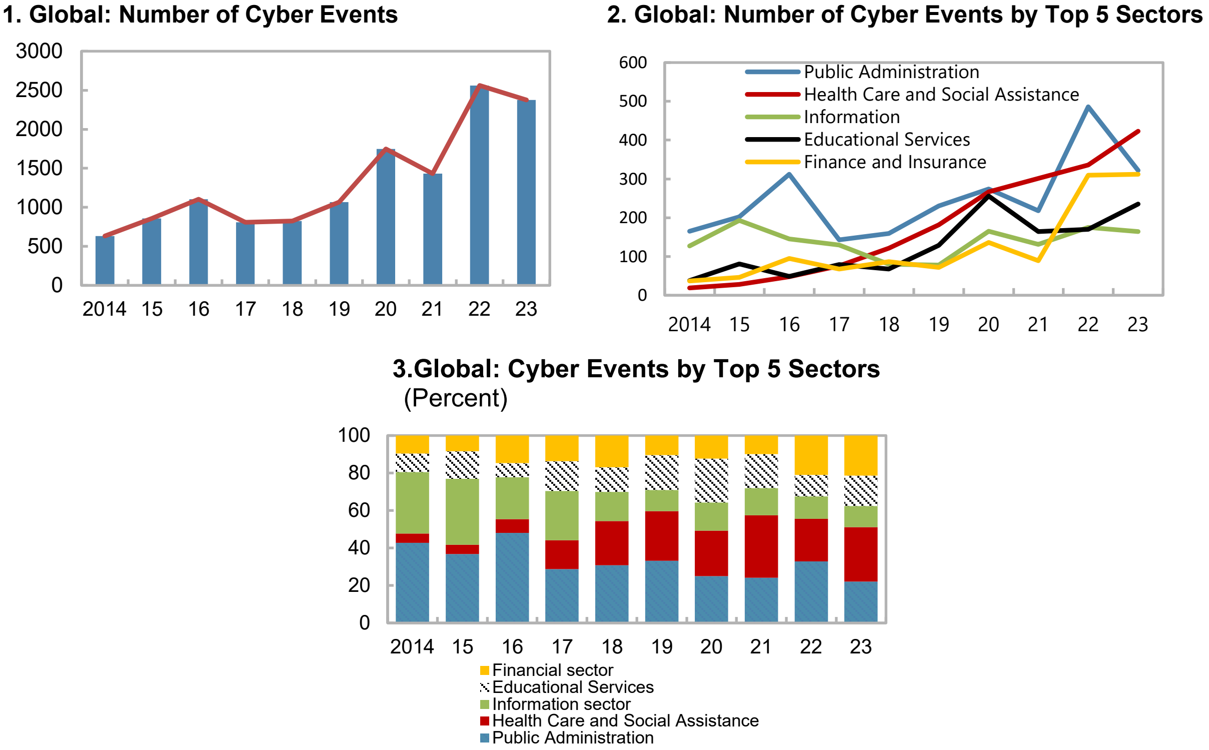
Figure 1. Number of Cyber Events in the Financial Sector Across Jurisdictions, 2014-2023



Sources: University of Maryland CISSM Cyber Events Database; Microsoft Bing; and IMF staff calculations.

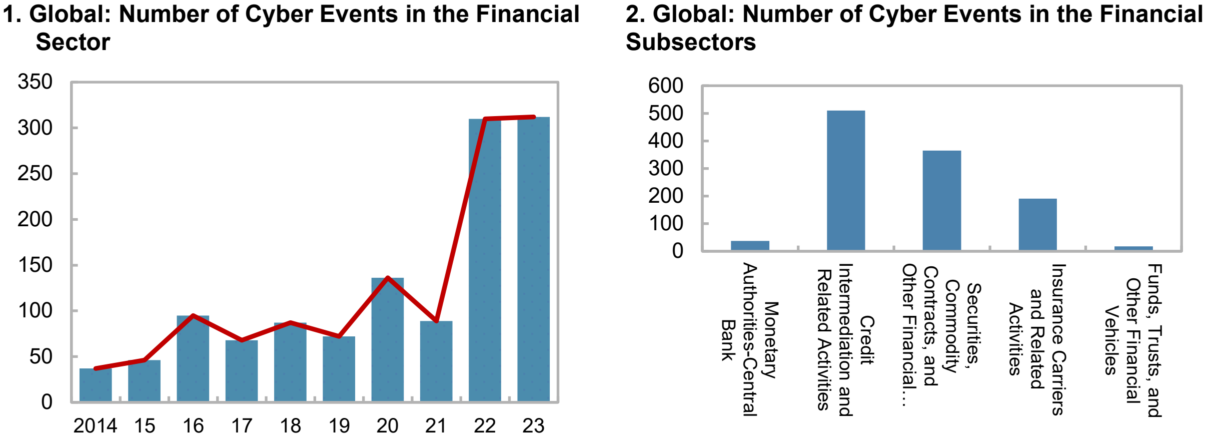
Figure 4 illustrates the global distribution of the incidence of cyber events from 2014 to 2023, along with a breakdown of incidents across the top five affected sectors—public administration, health care and social assistance, ICT, educational services, and financial services. It captures a global trend of a steady increase in the frequency of cyberattacks, with particularly sharp growth over the past five years. The trend is reflected in all of the top five sectors affected. In the financial sector, the number of cyber events in the financial sector showed a fluctuating, albeit upward trend between 2014 and 2020, followed by a sharp surge beginning in 2021 (Figure 5). Moreover, while the incidence of cyber events first increased sharply in the education and health sectors starting around 2017-18, the growth of cyber events in the financial sector has been especially striking during the last five years, as reflected in its continuous, significant and rapidly rising share of total cyber events since 2020. Among subsectors of the financial sector, credit intermediation and securities markets accounted for the largest shares, representing approximately 46 percent and 33 percent of total incidents, respectively.

Figure 2. Global Cyber Events, 2014-2023



Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

Figure 3. Cyber Events in the Financial Sector, 2014-2023



Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

Monetary Authorities[15]

Central banks[16] play a vital role in the functioning of national economies, and so, even though cyber events involving central banks account for only around four percent of all reported incidents within the financial sector, they are critically important due to the systemic role and unique responsibilities of these institutions. While central banks typically play a limited role in direct financial intermediation, such as retail deposit-taking and credit provision, they play a central role in the operation and oversight of key financial infrastructures, including payment systems, settlement arrangements, and liquidity facilities (Gaidosch et al., 2026). Central banks appear to be facing growing cybersecurity challenges as financial systems become increasingly digitalized. In recent years, both the frequency and sophistication of cyberattacks targeting central banks have reportedly increased. Cyber events are now widely regarded by central banks as an increasingly critical threat to financial stability, with cyber risks showing the sharpest increase in perceived importance among all risk categories (Mendez-Barreira and Popowicz, 2022).[17]

Analysis of cyber event data suggests that incidents involving central banks exhibit three notable characteristics.

First, cyber events at central banks remain a small but likely underreported share of total incidents, with relatively stable annual counts except for a few notable spikes. Between 2014 and 2023, cyber events involving central banks have remained consistently low, averaging about three incidents per year in nine out of the ten years. This figure is significantly lower than that for other financial subsectors such as banking institutions, securities firms, insurance providers, trusts, and investment funds (Figure 6, panel 1). One possible explanation is that central banks tend to exhibit relatively strong corporate governance and cybersecurity frameworks, particularly relative to smaller supervised financial entities. Central banks conduct internal cyber simulations and have increased cybersecurity investments in recent years, reflecting a more proactive and well-resourced approach to cyber risk management. At the same time, the BIS survey results also suggests that important gaps and areas for improvement remain (Doerr et al., 2022).

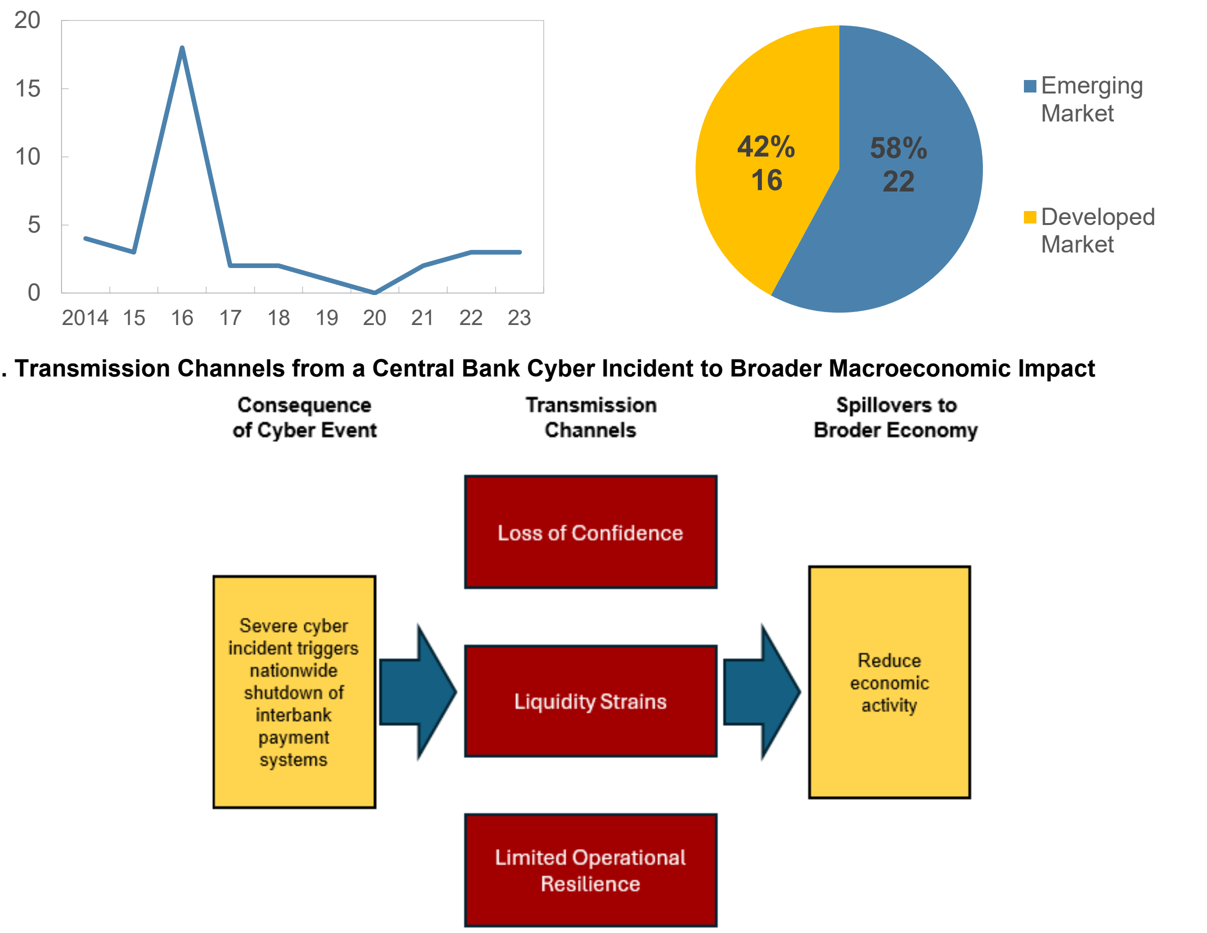
Another plausible explanation is that central banks may have limited incentives or obligations to disclose cyber incidents. Very few countries impose legal requirements for disclosure of such attacks, and publicly available data on these events remains scarce (Wall Street Journal, 2024). Central banks may fear reputational damage or a loss of public confidence, which may also discourage them from reporting such incidents openly. An outlier in this trend occurred in 2016, when reported incidents involving central banks spiked to eighteen (Figure 6, panel 1), possibly due in part to the emergence of new malware strains during that period. In May 2016, as part of Anonymous' month-long Operation Icarus, hacktivists carried out Distributed Denial of Service (DDoS) attacks against the websites of multiple central banks across Europe, Latin America, Africa, and Asia (PYMNTS, 2016). This campaign was explicitly framed as a protest against perceived economic injustice, explaining the unusually high number of reported events in that year.

[15] In the University of Maryland's CISSM Cyber Events Database, this sector is classified as Subsector 521: Monetary Authorities–Central Bank. For simplicity, the term "central bank" is used throughout the text.

[16] Cyber event risks at central banks are relevant both where they operate critical infrastructures and in their broader financial stability role.

[17] For the purposes of this study, the terms "cybercrime," "cyberattack," "cyber incidents" and "cyber event" are used interchangeably to refer to malicious cyber incidents targeting financial institutions, including but not limited to data breaches, system disruptions, and unauthorized access.

Figure 4. Cyber Events in Central Banks



1. Global Cyber Events Trends in Central Bank

2. Share of Central Bank Cyber Events in Emerging versus Developed Economies

3. Transmission Channels from a Central Bank Cyber Incident to Broader Macroeconomic Impact

Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

Second, central banks in emerging markets and developing economies are significantly more likely to be targets of cyberattacks. Descriptive incident data reveal that central banks in emerging markets and developing economies account for 58 percent of reported cyber events, significantly higher than the share of advanced economies (Figure 6, panel 2). One contributing factor may be that central banks' cybersecurity policy frameworks in emerging markets and developing economies tend to remain underdeveloped in the sense that many of these countries lack comprehensive legal, regulatory, and institutional mechanisms to manage cyber risks effectively, resulting in weaker national cyber defense capabilities and greater exposure to external threats.

This assessment is consistent with survey findings, which show that fewer than half of central banks and supervisory authorities in emerging market and developing economies had established a national cybersecurity strategy focused on the financial sector as of 2023, and that formal supervisory or cyber threat/stress testing frameworks remain only partially implemented across many of these jurisdictions (IMF, 2024). The vulnerability created by cyber events may be further compounded by a shortage of cybersecurity expertise within central banks in these regions. Without an adequate number of technical personnel, these institutions may lack the capability to prevent cyber incidents and to respond effectively when they occur, making it difficult to contain risks and prevent spillover effects to the financial sector. This challenge was highlighted in evidence presented by the World Bank (2023), which noted that the global cybersecurity workforce gap has reached record levels, with developing countries facing the most severe shortages. In turn, the absence of robust cybersecurity policy frameworks and shortage of cybersecurity expertise, may also make emerging markets and developing economies more attractive targets for cybercriminals, who perceive them as low-risk, high-reward environments. Legal and technical deterrents also tend to be weaker while attackers obtain substantial returns through ransomware campaigns, data breaches, or financial fraud.

Third, an attack on central bank operated interbank payment systems could pose systemic risks and trigger ripple effects across the broader economy. For example, a cyber event that occurred in 2023 in a southern African country disrupted interbank payment operations at the national level for over a week. Although the central bank reported that the event did not result in observable financial losses, the shutdown of the payment system was likely to have threatened to exacerbate systemic vulnerabilities and cause spillover effects to the macroeconomy. Such disruptions, especially when occurring under stressed financial conditions, could significantly amplify liquidity strains, accelerate shocks across institutions, and pose a greater threat to financial stability (Eisenbach et al., 2023).

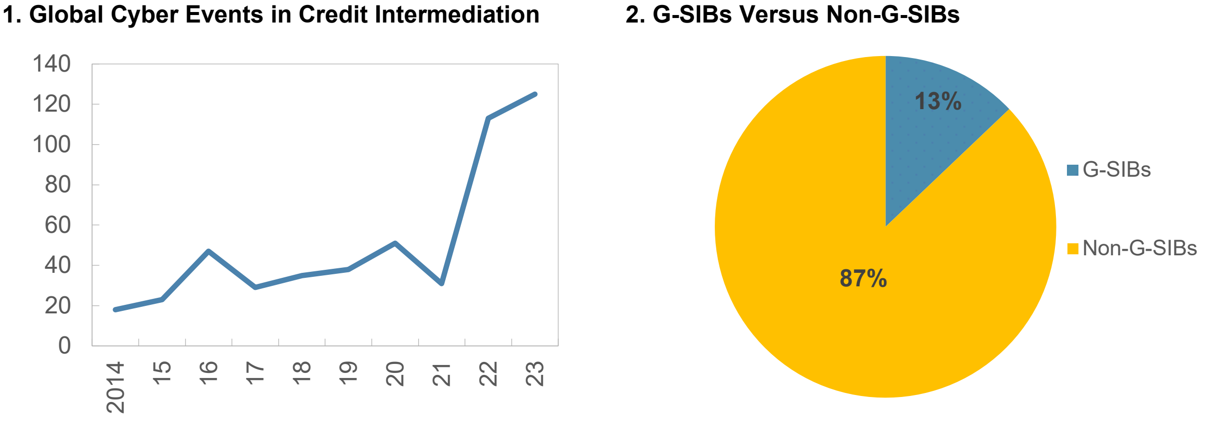
A cyber event that disrupts interbank payment systems has the potential to propagate to the real economy through three principal transmission mechanisms (Figure 6, panel 3). Initially, a deterioration in public confidence could arise if there are questions on the central bank's operational capacity, while foreign investors could reassess the credibility of the financial system. In certain contexts, particularly in emerging markets, such disruptions may also have implications for money demand. Subsequently, liquidity disruptions could result if the central bank is unable to clear transactions with commercial banks and interbank transfers are suspended, leading to delays in wage payments and broader settlement failures. In addition, limited operational resilience is particularly evident in developing economies where backup systems and contingency frameworks may be lacking. These mechanisms may interact and ultimately give rise to a broader economic slowdown.

Credit Intermediation[18]

The credit intermediary sector operates at the core of the financial system, connecting various economic actors and supporting the infrastructure essential for financial intermediation. The smooth functioning of banks and other credit intermediaries is fundamental to maintaining financial stability and supporting the real economy. According to the University of Maryland's CISSM Cyber Events Database, cyber incidents related to credit intermediaries account for 46 percent of all cases within the financial sector. This disproportionate concentration highlights both the sector's central role in financial operations and its heightened exposure to cyber risk. Over the past decade, cyber events targeting credit intermediaries have generally increased, with a notable surge following the COVID-19 pandemic (Figure 7, panel 1).

[18] In the University of Maryland CISSM Cyber Events Database, the banking sector is classified under Subsector 522: Credit Intermediation and Related Activities. For simplicity, the term "banking sector" is used throughout the text.

Figure 5. Cyber Events Impacting Credit Intermediaries


1. Global Cyber Events in Credit Intermediation

2. G-SIBs Versus Non-G-SIBs

Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

This surge coincided with a structural shift in how individuals accessed banking services, as the pandemic accelerated the transition to digital channels. Consequently, banks became increasingly exposed to cyber threats. Three important developments can be drawn from recent cyber incidents targeting the credit intermediation sector: (i) the vulnerability differential between globally systemically important banks (G-SIBs) and non-G-SIBs;[19] (ii) the prevalence of data breaches as a common and persistent outcome; and the growing influence of geopolitical tensions in shaping attack motivations.

Between 2014 and 2023, only 13 percent of cyber incidents in the global banking sector involved G-SIBs, while most events targeted other banks and credit intermediaries (Figure 7, panel 2). These differences may reflect variation in exposure, reporting practices, institutional scale, and resource allocation across banks, rather than differences in resilience alone. This stark imbalance highlights significant disparities in cybersecurity resilience within the banking system. Non-G-SIBs appear to be more frequent targets, possibly due to weaker investments in cybersecurity, limited redundancy, and less robust incident response mechanisms. Smaller institutions have modest earnings, which constrains their ability to invest more extensively in cybersecurity and resilience (S&P Global, 2025). These institutions may also operate under lighter compliance and regulatory frameworks, which, together with limited resources, legacy systems, and uneven cybersecurity capabilities, may contribute to higher exposure during the digital transformation process. Although G-SIBs account for a smaller share of incidents, their systemic importance means that any successful attack on them could have far-reaching consequences.

Data breaches are among the most frequent outcomes of cyber incidents, with third-party vendors often constituting one of the more vulnerable links in the security chain.[20] Despite the high sensitivity of the information often exposed, such as clients names, social security numbers, bank account details, and credit or payment data, many breaches do not originate within banks themselves, occurring frequently at external entities providing services on behalf of, and to financial institutions. These third parties may include IT vendors,

[19] G-SIBs refer to global systemically important banks. See 2024 List of Global Systemically Important Banks (G-SIBs).

[20] In the context of cyber-attacks, data breaches can involve various types of sensitive information — from personal and financial data to health records and business secrets — and arise from different causes, such as hacking, phishing, malware, misconfiguration, or insider threats.

payment processors, file transfer providers, and marketing firms. Given their integration into core banking operations, compromises at these vendors may inadvertently provide pathways into critical systems, thereby amplifying the impact of breaches that might otherwise remain contained.

One contributing factor is the limited capacity of the banking sector to monitor and manage the cyber risk posture of these third-party service providers. Banks have long relied on outsourcing and other third-party service relationships, and in recent years this reliance has extended to a broader and more complex ecosystem of providers (FSB, 2023). Hence, while many banks have developed relatively robust internal cybersecurity frameworks, this increasing dependence on external providers introduces new layers of risk, increasing potential exposure, especially when they lack full visibility into, and control over cyber risk postures of these service providers. The problem is magnified in cases where a service provider prioritizes contractual deliverables over cybersecurity responsibilities. This misalignment of priorities may give rise to structural vulnerabilities, allowing threat actors to exploit these vendors as relatively low-cost and less-defended entry points into the banking ecosystem.

Geopolitical tensions have emerged as an important underlying factor behind cyber incidents targeting the banking sector. Empirical observations suggest a broader link between political conflict and cyber incidents (IMF, 2024). As a cornerstone of economic stability and public trust, the banking system is often viewed as a symbolic and strategic target during periods of geopolitical conflict, wherein cyberattacks may be strategically motivated not by financial gain, but by political objectives. For example, incidents recorded in the University of Maryland's CISSM Cyber Events Database highlight a recurring pattern of politically charged attacks on banks, often involving temporary website takedowns, defacements with political messaging, or denial-of-service campaigns. These incidents typically aim to disrupt public access rather than compromise core systems, signaling the attackers' intent to provoke rather than to profit. While such operations may not always result in immediate financial losses, they expose critical cybersecurity vulnerabilities.

Securities and Commodities Markets and Market Intermediaries[21]

The securities sector constitutes a critical pillar of the modern financial system, facilitating capital formation, resource allocation, and market liquidity. Over the past decade, the frequency of cyber incidents targeting the securities sector has steadily increased, driven by the rapid growth of financial technology, the expansion of crypto-asset ecosystems[22], the deepening digitalization of securities services, and other related developments (Figure 8, panel 1). As highlighted by the International Organization of Securities Commissions (2016), cybersecurity risks extend across all major components of the securities sector—reporting issuers, trading venues, market intermediaries, asset managers, and financial market infrastructures (FMIs)—underscoring the sector's broad, multifaceted, and highly interconnected exposure to cyber threats.

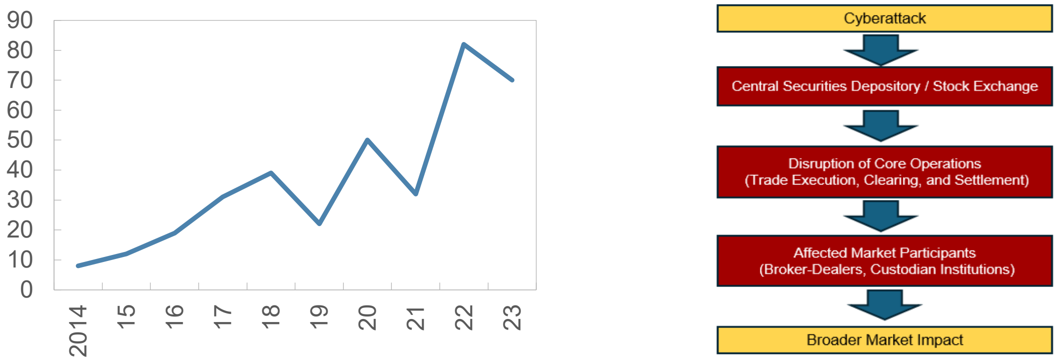
[21] In the University of Maryland CISSM Cyber Events Database, the securities sector is classified under Subsector 523: Securities, Commodity Contracts, and Other Financial Investments and Related Activities. For simplicity, the term "securities sector" is used throughout the text.

[22] Crypto-related incidents are discussed within existing financial sector categories where they intersect with regulated institutions.

Figure 6. Cyber Events in Securities

1. Global Cyber Events Trends in Securities

2. Cyberattack Transmission Through Capital Market Layers



Sources: University of Maryland CISSM Cyber Events Database; and IMF staff calculations.

According to the University of Maryland’s CISSM Cyber Events Database, cyber incidents affecting the securities sector accounted for approximately 33 percent of all observed financial-sector events, reflecting the sector’s pronounced vulnerability and strategic importance. This section discusses three commonly observed characteristics of cyber threats in the securities industry.

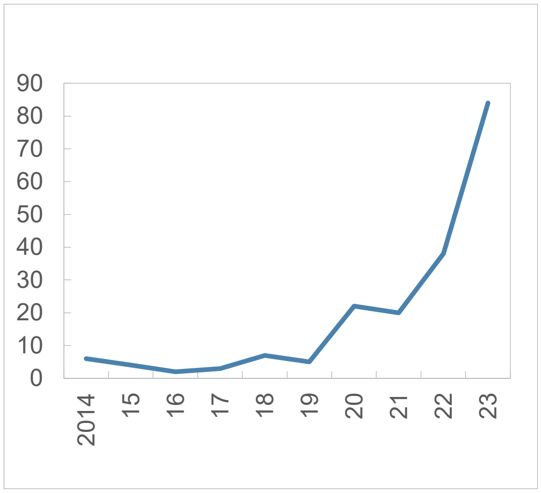
First, cyber incidents may contribute to broader market volatility, particularly when they target securities exchanges, trading systems, or other critical market infrastructure. Given the central role of exchanges and post-trade infrastructures in capital markets, these disruptions may also carry financial stability implications. Such events can lead to trading disruptions, delays in price quotations, execution failures, and breakdowns in clearing and settlement processes. These operational disturbances can quickly erode investor confidence and amplify short-term market fluctuations. Moreover, when cyber incidents receive widespread media attention, their effects may spill over to other markets, triggering broader reactions such as increased risk aversion, reduced liquidity, or abrupt asset repricing. While empirical research on the causal link between cyber events and market volatility remains at an early stage, accumulating case evidence suggests the relationship warrants greater scrutiny and further investigation.

Second, cyberattacks in the securities sector disproportionately target high-value systemic nodes, such as stock exchanges and central securities depositories (CSDs) highlighting the sector’s structural reliance on a limited set of critical market infrastructures. These FMIs serve as critical hubs for trade execution, clearing, and settlement, making them especially attractive targets for cyber threat actors. A successful attack on such entities can trigger widespread operational disruptions and lead to systemic spillover effects (Figure 8, panel 2). For example, in 2022, a leading CSD in an Asian jurisdiction experienced a malware incident. While official disclosures did not confirm any large-scale data compromise or direct financial losses, the attack reportedly disrupted core system operations, with potential downstream effects on connected market participants such as broker-dealers and custodian institutions.

Beyond traditional FMIs, the rise of digital asset ecosystems has introduced a new vector of cyber vulnerabilities within the securities sector. The growing prominence of crypto assets and decentralized finance (DeFi) applications appears to coincide with a rising number of crypto-related incidents, some of which have been associated with large financial losses. Overall financial losses from crypto-related cyberattacks have demonstrated an upward trajectory, alongside a growing sophistication and diversification of attack vectors and targets (Chainalysis, 2024). These dynamics are increasingly visible at the platform level. For example, in 2023, a crypto platform based in a Southeast Asian jurisdiction experienced two major digital asset losses within the span of a single week—one involving, an approximately USD 125 million loss and the other resulting in an addition loss of USD 103 million. While the exact nature of the breaches remained unclear, both incidents were reportedly linked to the exploitation of application server vulnerabilities. The high frequency and magnitude of these attacks underscore the acute operational risks facing digital asset infrastructures and highlight how recurring vulnerabilities can amplify systemic exposure within the crypto-financial ecosystem.

Insurance[23]

Figure 7. Global Cyber Events in Insurance



Sources: University of Maryland CISSM Cyber Events Database; and IMF Staff Calculations.

Insurance is a core component of the modern financial architecture, playing a vital role in personal and corporate risk management and wealth accumulation. Over the past decade, cyber incidents targeting the insurance sector remained relatively stable between 2014 and 2019, as reflected in the CISSM Cyber Events Database. However, this trend shifted markedly following the outbreak of the COVID-19 pandemic, with a significant increase in reported incidents starting 2020 (Figure 9).

This surge may partly reflect previously undisclosed cases, but it also stems from the accelerated digitalization of insurance services and the heightened public awareness of protection needs during the pandemic, which have collectively made the sector a more attractive target for cyberattacks. Within the financial industry incidents recorded in the CISSM database, the insurance sector accounts for 16 percent—ranking just behind the credit intermediaries and securities markets sectors, indicating its growing prominence as a target of cyber threats. Overall, data breaches represent the predominant form of cyber incidents in this sector. Against this backdrop, data breaches affecting life and property & casualty (P&C) insurance exhibit both similarities and notable differences, which will be further examined in the following sections.

A common feature across cyber incidents affecting both life and P&C insurance is the exposure of sensitive data. Although such attacks may not result in immediate financial loss, they carry significant latent risks. Stolen data are frequently sold on the dark web and subsequently used in identity theft, financial fraud, and other illicit activities, resulting in broader secondary harm. Insurance data, particularly customers' medical records, is often considered more valuable than credit card data on dark web markets due to its long-term utility and non-replaceable nature (Nadrag, 2021). As a result, the heightened value of such data means that insurance customers' sensitive information tends to be an especially

[23] In the University of Maryland CISSM Cyber Events Database, the insurance sector is classified under Subsector 524: Insurance Carriers and Related Activities. For simplicity, the term "insurance sector" is used throughout the text.

attractive target for cyber threat actors. This observation is broadly consistent with Table 1, which indicates that the health care and social assistance sector, where large volumes of sensitive medical data are held, is among the sectors most frequently targeted by cyber incidents.

The key difference lies in the source of the breach. Data breaches in the life insurance sector are more frequently linked to vulnerabilities in third-party service providers, whereas those in the P&C sector tend to originate within the insurance companies' own systems. This distinction is largely attributable to differences in business structure. Life insurance policies often span several decades—or even a lifetime—making it difficult for insurers to manage such long-term, sensitive data internally. As a result, many life insurers outsource data storage and processing to specialized vendors, concentrating large volumes of valuable information in the hands of these "invisible but critical" third parties, which in turn become attractive targets for attackers. In contrast, P&C products are typically short-term, with more standardized and automated processes. Many of these operations are handled in-house, reducing reliance on third-party data outsourcing and shifting the primary attack surface toward internal systems.

Funds and Trusts[24]

Funds and trusts primarily serve functions such as pension management, retirement account custodianship, and long-term asset allocation. As foundational vehicles for intergenerational wealth transfer and long-term financial stability, they play a distinct role within the financial system. According to the CISSM Cyber Events Database, cyber incidents involving funds and trusts account for only about one percent of all recorded events in the financial sector, with nearly all cases concentrated in 2022 and 2023.

This relatively low proportion may reflect two key factors. First, there are limitations in disclosure practices. Many fund and trust entities operate under public or nonprofit structures and may not be subject to the same reporting requirements as other financial institutions. Some incidents are disclosed instead by third-party vendors—such as Pension Benefit Information (PBI)—and therefore may not be directly attributed to the fund or trust itself. Second, these institutions generally have a smaller digital attack surface. Unlike high-frequency banking or trading platforms, funds and trusts operate on more stable, low-volume transaction cycles, with fewer external system interfaces and limited customer interactivity—factors that may reduce their visibility and attractiveness to cyber threat actors.

Cyber incidents involving funds and trusts generally exhibit two notable characteristics. One prominent feature is the predominance of sensitive data exposure, often resulting from breaches at third-party service providers such as data processors or file transfer platforms. This trend reflects a structural vulnerability: many fund and trust entities, particularly those operating outside high-margin financial sectors, tend to have limited cybersecurity budgets, leading to uneven defensive capabilities and greater susceptibility to sophisticated attacks. In addition, the sector's cybersecurity risk exposure has expanded alongside the gradual involvement of pension funds in crypto asset markets. Interest among traditionally conservative pension schemes has grown following the launch of US crypto ETFs and the recent surge in bitcoin prices (McDougall et al., 2025). Although such involvement is typically indirect—through crypto investment vehicles or exchange-traded products—the underlying technologies introduce a broader range of vulnerabilities. Digital wallets, trading

[24] In the University of Maryland CISSM Cyber Events Database, the fund and trust sector is classified under Subsector 525: Funds (custodial, trustee, and fund administration–related entities), Trusts, and Other Financial Vehicles. For simplicity, the term "fund and trust sector" is used throughout the text.

platforms, and custodial services all present potential entry points for cyberattacks, increasing the likelihood that pension-related institutions could be affected by risks originating in the crypto ecosystem.

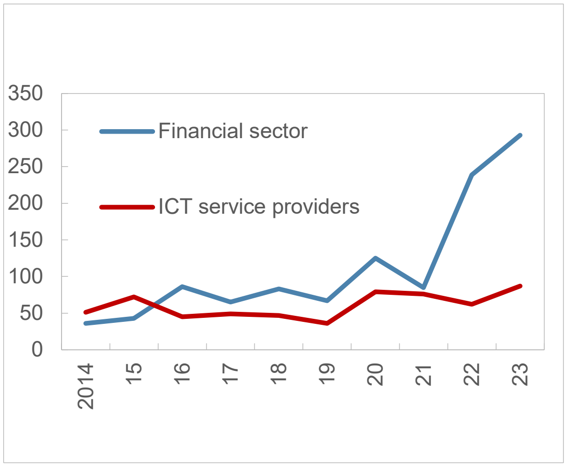
ICT Service Providers[25]

The financial sector relies heavily on a wide range of services provided by ICT service providers, including cloud computing, network infrastructure, and cybersecurity solutions. Insights drawn from CISSM's dataset suggest that the number of cyber incidents affecting the financial sector and ICT service providers followed a broadly similar trend from 2014 to 2020, with both sectors experiencing moderate fluctuations. However, starting in 2021, the number of incidents in the financial sector rose sharply, while growth among ICT service providers remained relatively stable (Figure 10).

This divergence reflects the post-pandemic acceleration of digital transformation in finance, particularly the rapid expansion of digital banking, remote work, and virtual asset services, all of which significantly increased the sector's exposure to cyber risk. Traditional financial institutions were forced to adopt digital service models in a short time frame, often outpacing their ability to upgrade security defenses. In contrast, many ICT service providers—especially those specializing in cloud and infrastructure services—generally possess stronger cybersecurity capabilities, resulting in fewer and less volatile incidents. The following analysis focuses on the transmission risk posed to the financial sector when ICT service providers experience cyberattacks, highlighting the critical interdependence between these two sectors.

In real-world cases, cyberattacks targeting ICT service providers often result not only in direct damage to the providers themselves but also in cascading effects on the financial institutions that rely on their services. For example, Cloudflare experienced multiple outages in 2020 and 2022, as well as repeated DDoS attacks, all of which had widespread repercussions for its downstream clients. As a key ICT provider serving many financial clients, Cloudflare offers edge computing, firewall protection, and content delivery services. Its customer base includes banks, insurance companies, and payment platforms. Although the immediate target of these attacks is the ICT provider, the heavy reliance of financial institutions on these services—for identity authentication, remote access, API connectivity, and code hosting—creates technical pathways for the disruption to be transmitted into the financial system. This amplifies the impact, potentially resulting in service outages, data breaches, and even systemic risk. At a broader level, large-scale disruptions to ICT or logistics providers may function as negative supply shocks, with potential implications for cost-push inflation when digital and physical supply chains are closely interconnected.

Figure 8. Global Cyber Events Trends in Financial Sector and ICT Service Provider



Sources: University of Maryland CISSM Cyber Events Database; and IMF Staff Calculations.

[25] In the CISSM Cyber Events Database, ICT Service Providers refer to Subsector 517 (Telecommunications) and Subsector 518 (Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services). For simplicity, the term "ICT Service Providers" is used throughout the text.

Digital Fraud

This section reviews past trends in digital fraud, including cyber-enabled and payment-related fraud where official statistics and public information are available. While data on cyber-enabled fraud largely reflect the number of cases and complaints (with financial losses reported in some jurisdictions), payment-related fraud further illustrate losses.

Cyber-Enabled Fraud

Figure 11 illustrates cyber-enabled fraud trends at the aggregate level and in selected regions and jurisdictions. The analysis of publicly available data points to important findings and observations as follows.

Global

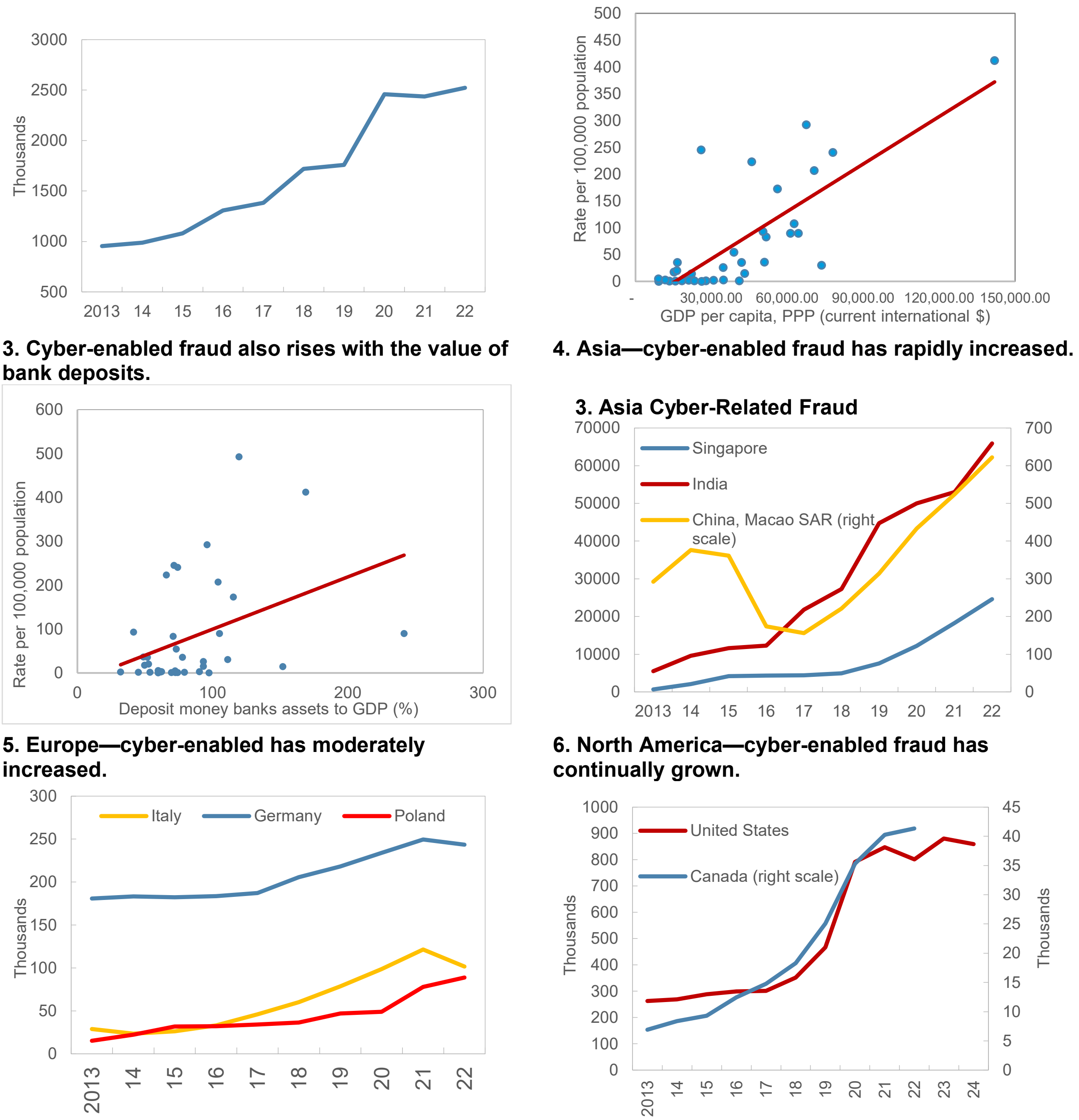
Cyber-enabled fraud has nearly tripled in the period of 10 years, reaching around 2.5 million cases in 2022 due to a sharp increase observed during COVID-19 (Figure 11, panel 1). One possible explanation is the proliferation of industrial-scale cyber-enabled fraud and scam centers driven by transnational criminal syndicates (UNODC, 2025). As noted earlier, the actual number of cases of cyber-enabled fraud need to be treated as estimates and with caution due to their underreporting in many jurisdictions.[26] Moreover, data from some jurisdictions are partially reported or unreported to the UNODC, making it difficult to observe trends in specific regions and countries (for example, Africa and the Middle East). Industry studies on the global state of scams have helped complement official statistics and point to their alarming rise, increasing complexity, and losses that amounted to around one trillion US dollars in 2024 (GASA, 2024a). Such studies provide further insights into developments and trends in regions and countries that are not covered through official statistics.[27] For some developing countries, such losses have been estimated to be around 2.5 percent to 4.2 percent of GDP. Global implications and the need to strengthen regulatory frameworks for effective prevention and enforcement, including the legal framework for addressing money laundering and virtual assets, oversight mechanisms, licensing and supervisory tools, and asset recovery, among other priority areas (UNODC, 2025). Law enforcement agencies have also observed the growing sophistication of fraud using ICT, including artificial intelligence, the prevalence of scam centers, and relationship-investment fraud (Europol, 2024; Interpol, 2024). Financial intelligence units have further identified money laundering networks that feature different types of financial institutions, including banks, payments and remittance service providers, and virtual assets service providers (Financial Action Task Force, Interpol, and Egmont Group, 2023); and ways to address them (FATF, 2025)

The number of cyber-enabled fraud cases appears to increase with rising national income bar a few outliers (Figure 11, panel 2). National income is measured as gross domestic product (GDP) per capita in purchasing power parity (PPP) rates. The scatter plot is based on an analysis of data from 38 countries. These findings are supported by industry studies which found that developed nations tend to sustain higher individual losses (GASA, 2024a). Emerging markets and developing economies, however, experienced a higher portion of their GDP lost to scams relative to developed nations. The results are subject to important caveats such as the availability or lack of centralized reporting mechanisms for fraud across countries.

[26] Houtti et al., (2024) also found widespread under-reporting in their survey of scams across 12 countries.

[27] Sum and Substance Ltd (UK) (2024) analyzes identity fraud trends and developments across regions and countries.

Figure 9. Cyber-Enabled Fraud: Numbers and Trends



1. Cyber-enabled fraud has increased by nearly three-fold at the aggregate level within 10 years.

2. Cyber-enabled fraud increases with rising income.

3. Cyber-enabled fraud also rises with the value of bank deposits.

4. Asia—cyber-enabled fraud has rapidly increased.

5. Europe—cyber-enabled has moderately increased.

6. North America—cyber-enabled fraud has continually grown.

Sources: UNODC (2024), UNODC Research - Data Portal – Corruption and Economic Crime. https://dataunodc.un.org/dp-crime-corruption-offences (Accessed on 26 February 2025); FBI (2013, 2018, 2024); National Crime Records Bureau of the Government of India (2016, 2022); World Bank. IMF staff calculations.

Note: Global cyber-enabled fraud is based on aggregated data from 60 jurisdictions obtained from the UNODC, India, and the United States. For India, data includes fraud and other cybercrimes. Deposit money to total assets are based on data from 2021 or the most recent data available from the World Bank.

The number of cyber-enabled fraud cases tend to also increase with the value of bank deposits (Figure 11, panel 3). Deposits are measured relative to GDP to make international comparisons of liquidity in the banking system. On the latter, bank deposits serve as the stock of money for account-based payment and settlement services provided by credit institutions.[28]

Regional Evidence

Asia. There has been a rapid increase in cyber-enabled fraud (Figure 11, panel 4). This is largely based on data reported by authorities from three jurisdictions. Industry surveys also suggest the total economic impact across 13 jurisdictions amounted to USD 688 billion in 2024 (GASA, 2024b).[29] In Singapore, the number of scams and cybercrime cases was reported to have increased to 28,751 cases with losses of around Singapore Dollar 385 million between January and June 2024 (Singapore Police Force, 2024). Industry surveys suggests that 65 percent of Singaporeans face scams at least once per month, while 68 percent of scam victims chose not to report their experience to law enforcement (GASA, 2024c). As of 2025, total scam cases and losses have fallen and remained a key priority for the government (Singapore Police Force, 2025). In India, authorities reported a total of 65,893 cases registered under cybercrimes where nearly 26.5 percent of cases (17,470 cases) were fraud-related (National Crime Records Bureau, 2022). While no data cyber-enabled fraud is available for Mainland, China, one approximation is using data for Macao, China, which has shown a sharp increase.[30]

Europe. There was a moderate increase in cyber-enabled fraud (Figure 11, panel 5). This is largely based on data reported by authorities in Germany, Italy and Poland.[31] Notwithstanding this trend, Europe’s law enforcement agency observed that millions of victims across the European Union are attacked and exploited daily (Europol, 2024). Moreover, the region’s cybersecurity agency has also analyzed 488 publicly related incidents that affected the finance sector in Europe, where the share of banks was 46 percent (ENISA, 2024).

North America. Cyber-enabled fraud has sharply increased (Figure 11, panel 6).[32] Since the founding of the U.S. Federal Bureau of Investigation’s (FBI) Internet Crime Complaint Center (IC3) in 2000, the IC3 has received over 9 million complaints of malicious activity averaging more than 2,000 complaints per day (FBI, 2024). Complaints with reference to cryptocurrency (such as bitcoin, ether, tether) also continued to grow between 2017 to 2023 with a sharper increase between 2021 to 2023 (FBI, 2023a). In Canada, a similar rising trend (based on cyber-enabled fraud data from the UNODC) was also observed. In 2022, the Canadian Anti-Fraud Center (CAFC) received over 91,000 reports and noted that only 5 to 10 percent of fraud and cybercrime are reported (CAFC, 2023), prompting the need for a ‘whole-of-society’ approach to address fraud.

Payment-Related Fraud

International efforts to address the growing threat of payment-related fraud should be viewed from both, wholesale and retail perspectives. Wholesale payments fraud related to endpoint security highlighted its

[28] Alternative measures on the stock of money available for payments include narrow money supply (M1), total banknotes and coins in circulation, bank deposits held at the central bank, interbank deposits, and intraday credit extended by the central bank.

[29] For Asia, the survey involved 24,731 people from China, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam.

[30] In 2023, the Ministry of Public Security was reported to have solved 437,000 cases of telecom network fraud (See media report).

[31] For Europe, GASA has published industry surveys of scams in Denmark, France, the Netherlands, Spain, Sweden, and the United Kingdom.

[32] For North America, GASA has published industry surveys of scams in Canada and the United States.

potential financial stability implications, and therefore, call for developing a strategy and toolkit to address such threats (CPMI, 2019; CPMI, 2018). Digital fraud, conceptualized as credit transfers, card-based payments or other instruments, has also raised supervisory and financial stability implications, particularly with the financial losses to banks resulting from digital fraud; and reputation risks to banks and supervisors (BCBS, 2023).[33]

In a major study of the shifting threat landscape associated with transnational organized crime, cyber-enabled fraud, underground banking, and technological innovation, payment and money transfer infrastructures was identified as an important conduit (UNODC, 2024, p. 26). This has involved networks of money mules, virtual-asset service providers, along with third-party payment applications established and controlled by organized crime actors.

Figure 12 illustrates payment-related fraud losses and trends in selected jurisdictions. The analysis of publicly available data points to five important findings and observations as follows.

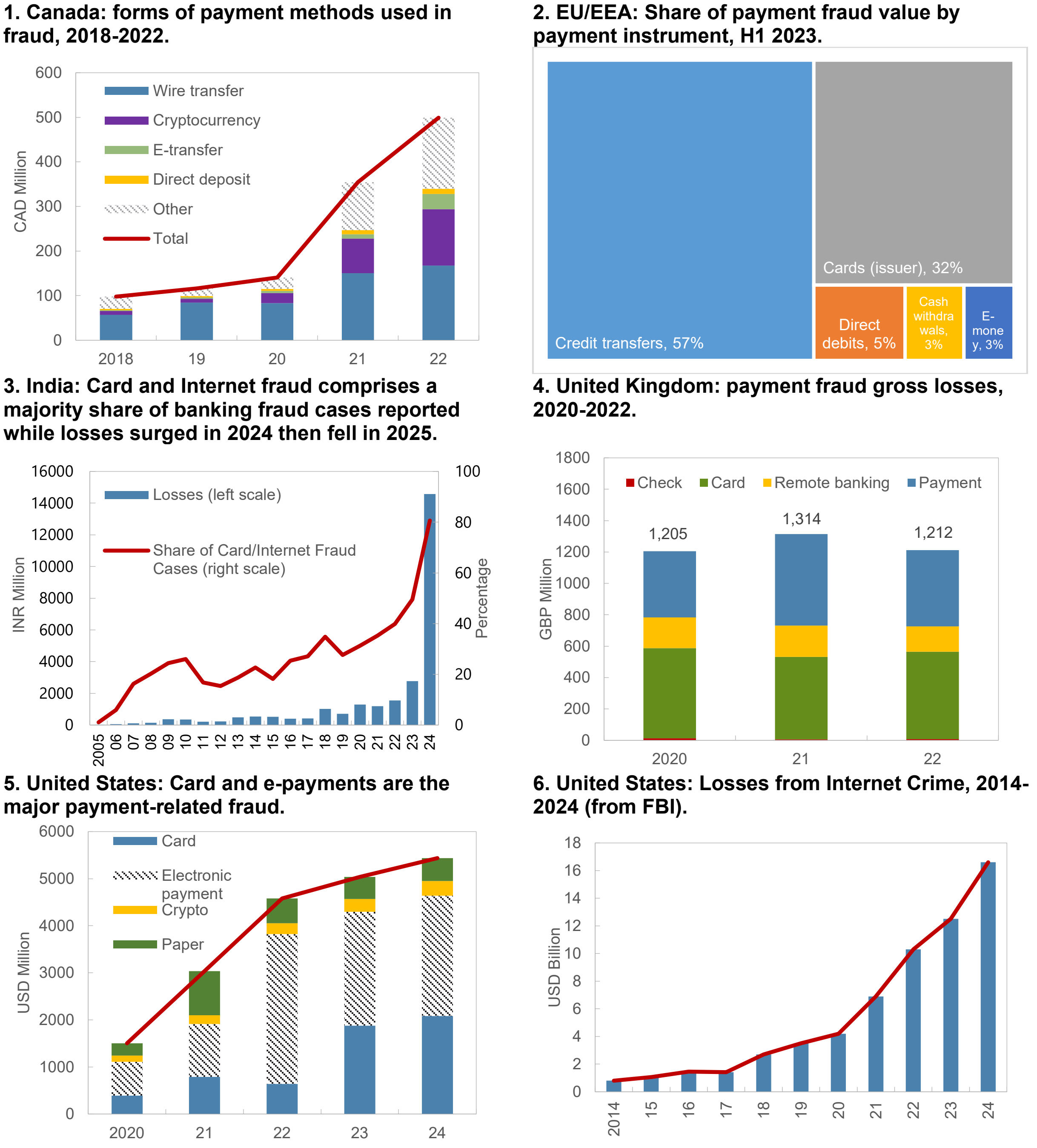
Canada. Reported losses increased sharpy between 2020 to 2022 and amounted to around Canadian Dollar (CAD) 500 million in Canada in 2022 (CAFC, 2023) (Figure 12, panel 1). In 2022, the CAFC noted CAD530 million in losses, the highest fraud losses on record and was of the view that the trend will not change. The CAFC also observed that while wire transfer was the top form of payment method used in Canada, cryptocurrency losses continued to grow at a much faster pace, from CAD8.2 million in 2019 to CAD22.5 million in 2020 and to nearly CAD126 million in 2022. E-transfers also grew as a popular payment method used in fraud.

Europe. The value of fraudulent payment transactions reported by the financial services sector amounted to EUR 4.3 billion in the European Economic Area (EEA) in 2022 where the major forms of payment methods used in fraud were credit transfers and cards (Figure 12, panel 2). As of the first half of 2023, the amount was nearly EUR 2 billion and authorities are of the view that the general outlook for overall payment fraud so far appears stable (EBA and ECB, 2024).[34] While card fraud was a major problem (from the use of magnetic stripe technology), they declined with measures such as using strong customer authentication (SCA) and card security codes. Effective fraud interventions such as daily payment limits, payee verification and improved fraud monitoring have been used, with ongoing efforts to improve liability for authorized push payments (de Ruijter, 2025; van Praag, 2025).The region has also benefitted from the development of a fraud taxonomy by the Euro Banking Association to capture and categorize fraud scenarios related to account-to-account and card payments. A growing concern, however, has been fraud in instant payments that featured notably higher fraud rates than traditional credit transfers along with more complex fraud types that leverage social engineering techniques. Such techniques are also among many others observed by the European Payments Council (EPC, 2024). As such, authorities have further considered strengthening the legal framework under the Payment Services Directive 3 and Payment Systems Regulation in Europe (EBA, 2024).

[33] The BCBS has grouped digital fraud into four broad categories: (i) unauthorized retail payment transactions; (ii) manipulating bank customers to issue retail payments; (iii) fraud related to other banking products; and (iv) fraud through customers' data or banks' systems. It has noted challenges in quantifying digital fraud due to data gaps and the lack of harmonized or comparable definitions and differences in collecting data across jurisdictions.

[34] See also, EBA and ECB (2025) for developments on payment fraud up to December 2025.

Figure 10. Payment-Related Fraud: Losses and Trends



1. Canada: forms of payment methods used in fraud, 2018-2022.

2. EU/EEA: Share of payment fraud value by payment instrument, H1 2023.

3. India: Card and Internet fraud comprises a majority share of banking fraud cases reported while losses surged in 2024 then fell in 2025.

4. United Kingdom: payment fraud gross losses, 2020-2022.

5. United States: Card and e-payments are the major payment-related fraud.

6. United States: Losses from Internet Crime, 2014-2024 (from FBI).

Sources: Canadian Anti-Fraud Center; EBA-ECB; Reserve Bank of India; UK Finance; FBI Internet Crime Complaint Center, U.S. Federal Trade Commission.

Notes: For India, frauds reported in a year could have occurred several years prior to year of reporting. Amounts involved are as reported and do not reflect the amount of loss incurred. For U.S., cards is the sum of credit, debit, gift, and reload cards. E-payments include payment app or service, bank transfer or payment, and wire transfer. Paper includes cash, check, and money order.

India. The Reserve Bank of India (RBI, 2024) noted that fraud in banking has been rising with card with online/ internet cases forming a large share of the total (Figure 12, panel 3). Based on media reports citing RBI statistics, online payment fraud grew INR14½ billion in the year ended March 2024 and this has coincided with the rise of instant payments.[35] As of March 2025, online fraud declined (RBI, 2025). Authorities have proactively been addressing payment fraud through central bank guidelines, the implementation of a Central Payments Fraud Information Registry, and development of an artificial intelligence and machine learning model to help banks and financial institutions detect mule accounts.[36] Additionally, measures to compensate customers for small-value digital fraud have also been proposed (as of February 2026).[37]

United Kingdom. Card and payments form the largest share of fraud. (Figure 12, panel 4). Payment types include faster payments, the Clearing House Automated Payment System (CHAPS), the Bankers' Automated Clearing System (BACS), intrabank transfers, and international transfers. Official studies indicate that authorized push payments (APP) volumes increased by 12 percent since 2022, while losses fell by 12 percent in the same period (The Payment Systems Regulator, 2024).[38] Industry studies further show that 77 percent of APP fraud in the first half of 2023 originated online, through fake websites and social media among other sources (UK Finance, 2024). Legislative reforms in response to fraud have included the Online Safety Bill, Financial Services and Markets Act, and Economic Crime and Corporate Transparency Bill. The UK is also considered the first jurisdiction in the world to have introduced a mandatory reimbursement scheme for authorized push payment fraud victims in certain circumstances (Braithwaite, 2024).

United States. Card and electronic payments are the major types of payment-related fraud that have been gradually growing (Figure 12, panel 5).[39] This trend reflects the findings from an earlier pioneering study by DeLiema et. al. (2017) for the United States, which found that the most common method of payments for financial fraud was by credit card. Official studies on payments fraud have also pointed to the increase in the aggregate fraud rate by value and number in the survey of depository institutions in 2012 and 2015 (Board of Governors of the Federal Reserve System, 2018). The study also highlighted that card fraud increased as a percentage of total fraud value, a shift from in-person fraud towards remote fraud, and increased use and acceptance of microchip-based cards and authenticated card payments. However, further issues on the increase of cardholders' card-present fraud loss rates, especially for dual-message networks, still needs to be addressed (Hayashi, 2025).[40] On a more aggregate level, losses from Internet crime continued to increase and reached USD 16.6 billion in 2024 (FBI, 2024) (Figure 12, panel 6). While not entirely payment-related fraud, there are implications with movement of funds between crypto assets and the traditional financial system (such as cash withdrawals at cryptocurrency exchanges or kiosks). Cyber-enabled fraud represents around 83 percent of all losses reported to the IC3 in 2024 with investments, particularly crypto investments, being the major type of crime while investment scams targeted at elders continued to be the costliest in terms of financial losses (FBI, 2023a; FBI, 2023b; FBI, 2024).

[35] See article.

[36] See RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds issued in April 2011. For detection of mule accounts, see article.

[37] See media report.

[38] UK authorities refer APP scams to a situation when a scammer tricks someone into sending a payment to an account outside of their control (The Payment Systems Regulator, 2024).

[39] See Board of Governors of the Federal Reserve System (2018) for a detailed study of payments fraud in the United States.

[40] See Hayashi et al., (2003). Dual-message networks send separate messages for transaction authorization and payment clearing, use the same infrastructure as credit card networks, and thus cardholders are traditionally authenticated with a signature. Single-message networks send a single message for both transaction authorization and payment clearing, originated from ATM networks, where cardholder authentication is traditionally done with a PIN.

Conclusion

This paper has reviewed and examined trends and developments in cyber events and digital fraud, focusing on the financial sector. The analysis uses public information, comprising a database of cyber events, official statistics of cyber-enabled and payment-related fraud, industry surveys, and media reports. The review found that cyber events in the financial sector have grown by tenfold and cyber-enabled fraud has nearly tripled in the past decade. The key observations drawn from the review is as follows.

On cyber events, the review found a marked increase in incidents targeting the financial sector over the past decade, largely driven by accelerated digitalization and a growing reliance on interconnected systems. The distribution of incidents reveals significant heterogeneity—both institutionally and geographically. Non-G-SIBs account for the majority of cases, highlighting possible gaps in cyber preparedness among smaller and less-resourced institutions (Ravikumar, 2025). At the regional level, advanced and highly digitalized economies report more incidents, likely reflecting greater exposure, digital integration, and stronger reporting mechanisms. Data breaches remain the most common outcome, particularly in sectors such as securities, insurance, and payments. In addition, geopolitical tensions are playing an increasingly prominent role in shaping attack motivations, with several incidents exhibiting characteristics of state-linked operations.

On digital fraud, the review identified several country-specific actions that have been taken to address the rise of digital fraud, including: (i) strengthening the legal basis and regulatory framework to further protect consumers with respect to data privacy, liability-sharing, and recovery of financial losses; (ii) formulating a ‘whole-of-society’ approach including a national strategy to fight digital fraud; (iii) formulating a fraud taxonomy; (iv) establishing fraud risk management frameworks across organizations; (v) identifying and eliminating mule accounts; (vi) strengthening measures against payment fraud; (vii) establishing an anti-scam center and/or central fraud registry to facilitate the reporting of cyber-enabled fraud by victims to authorities; and (viii) enabling cross-sectoral co-operation among public authorities and the private sector.

The financial stability implications from digital fraud could include financial losses to banks and reputational risks to banks and supervisors (BCBS, 2023). With the rapid growth of digital payments and cryptoassets, along with the movement of funds across borders and between the traditional and non-traditional (crypto-assets) parts of the financial system, the impact on the occurrence and trends of future cyber events and digital fraud should be closely monitored to address the evolving risks in the threat landscape.

References

Basel Committee on Banking Supervision (2023). Digital Fraud and Banking: Supervisory and Financial Stability Implications, Discussion Paper, November.

Board of Governors of the Federal Reserve System (2018). Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study, October.

Braithwaite, J (2024). Authorized Push Payment Bank Fraud: What Does an Effective Regulatory Response Look Like? Journal of Financial Regulation, Vol. 10, No. 2, pp.174-193.

Canadian Anti-Fraud Centre (CAFC) (2023). Annual Report 2022.

Chainalysis (2024). Funds Stolen from Crypto Platforms Fall more than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises, January 24.

Committee on Payments and Market Infrastructures (CPMI) (2018). Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security, May.

CPMI (2019). Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security: A Toolkit, October.

DeLiema, M., G. Mottola., and M. Deevy (2017). Findings from a Pilot Study to Measure Financial Fraud in the United States, Stanford Center on Longevity and FINRA Investor Education Foundation, February.

De Ruijter, M (2025). Effectiveness of Fraud Interventions: Combining Systemic and Individual Interventions, Journal of Payments Strategy & Systems, Vol. 19, No. 4, pp. 356-363.

Doerr, S., L. Gambacorta., T. Leach., B. Legros., and D. Whyte (2022). Cyber Risk in Central Banking (BIS Working Paper No. 1039). Bank for International Settlements.

European Banking Authority (EBA) (2024). EBA Opinion on New Types of Payment Fraud and Possible Mitigants, 29 April.

European Banking Authority (EBA) and European Central Bank (ECB) (2024). 2024 Report on Payment Fraud.

EBA and ECB (2025). 2025 Report on Payment Fraud.

European Payments Council (EPC) (2024). 2024 Payment Threats and Fraud Trends Report, 22 November.

European Union Agency for Cybersecurity (ENISA) (2024). ENISA Threat Landscape: Finance Sector, January 2023 to June 2024.

Europol (2024). Internet Organized Crime Threat Assessment (IOCTA) (2024). Publications Office of the European Union, Luxembourg.

Executive Office of the President (2022). North American Industry Classification System, Office of Management and Budget, United States.

Federal Bureau of Investigation (FBI) (2013). Internet Crime Report 2013, Internet Crime Complaint Center.

FBI (2018). Internet Crime Report 2018, Internet Crime Complaint Center.

FBI (2023a). Cryptocurrency Fraud Report 2023, Internet Crime Complaint Center.

FBI (2023b). Elder Fraud Report 2023, Internet Crime Complaint Center.

FBI (2024). Internet Crime Report 2024, Internet Crime Complaint Center.

Financial Action Task Force (FATF)—Interpol—Egmont Group (2023). Illicit Financial Flows from Cyber-Enabled Fraud, FATF, Paris, France.

FATF (2025). Cyber-Enabled Fraud—Digitalization and Money Laundering, Terrorist Financing and Proliferation Financing Risks, February.

Financial Stability Board (2023). Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities, December.

Gaidosch, T., E. Islam., T. Khiaonarong., R. Ravikumar., and C. Wilson (2026). Good Practices in Cyber Risk Regulation and Supervision. Departmental Paper, Monetary and Capital Markets Department, International Monetary Fund.

Global Anti-Scam Alliance (GASA) (2024a). Global State of Scams Report 2024.

GASA (2024b). Asia Scam Report 2024.

GASA (2024c). The State of Scams in Singapore 2024.

Harry, C. and N. Gallagher (2018). Classifying Cyber Events. Journal of Information Warfare, 17(3), 17-31.

Harry, C., N. Gallagher., and L. Samuelson (2023). Cyber Events Database Codebook. Center for International and Security Studies at Maryland, School of Public Policy, University of Maryland, March.

Hayashi, F., R. J. Sullivan., and S. E. Weiner (2003). A Guide to the ATM and Debit Card Industry, Federal Reserve Bank of Kansas City.

Hayashi, F. (2025). Did Card-Present Fraud Rates Decline in the United States After the Migration to Chip Cards? Federal Reserve Bank of Kansas City, Payment Systems Research Briefing, February 12.

HM Government (2023). Fraud Strategy: Stopping Scams and Protecting the Public, Presented to Parliament by the Secretary of State for the Home Department by Command of His Majesty, May.

Houtti, M., A. Roy., V. N. R. Gangula., and A. M. Walker. (2024). A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries, Journal of Online Trust and Safety, July, pp. 1-26.

International Monetary Fund (IMF) (2024). Global Financial Stability Report: The Last Mile—Financial Vulnerabilities and Risks, Chapter 3: Cyber Risk: A Growing Concern for Macrofinancial Stability.

International Organization of Securities Commissions (2016). Cyber Security in Securities Markets – An International Perspective (FR02/2016). IOSCO.

Interpol (2024). Interpol Global Financial Fraud Assessment, Interpol General Secretariat, France.

Mendez-Barreira, V., and J. E. Popowicz (2022). Risk Management Benchmarks 2022 Report—Assuming New Responsibilities. Central Banking Institute, February.

McDougall, M., N. Asgari., and A. Livsey (2025). Pension funds dabble in crypto after massive bitcoin rally. Financial Times, January 16.

Nadrag, P. (2021) Stolen Patient Records a Hot Commodity on the Dark Web, February 3.

National Crime Agency (2024) National Economic Crime Center Annual Report 2023-2024.

National Crime Records Bureau (2022). Crime in India 2022, Statistics Volume II, Ministry of Home Affairs, Government of India, New Delhi.

National Crime Records Bureau (2016). Crime in India 2016, Statistics, Ministry of Home Affairs, Government of India, New Delhi.

Nordic Financial CERT (2024). Cyber Threat Landscape for the Nordic Financial Sector 2024.

PYMNTS (2016, May 9). Another Central Bank Hacked—Anonymous to Blame?

Ravikumar, R (2025). Strengthening Cybersecurity: Lessons from the Cybersecurity Survey, IMF Technical Notes and Manuals, TNM/2025/06.

Reserve Bank of India (2024). Report on Trend and Progress of Banking in India 2023—24.

Reserve Bank of India (2025). Report on Trend and Progress of Banking in India 2024—25.

Singapore Police Force (2024). Mid-Year Scams and Cybercrime Brief 2024.

Singapore Police Force (2025). Annual Scam and Cybercrime Brief 2025.

S&P Global Ratings. (2025). Technology Is Delivering for Banks and Societies. Financial Inclusion in Emerging and Frontier Markets. April 8, 2025.

Sum and Substance Ltd (UK) (2024). Identity Fraud Report.

The Payment Systems Regulator (2024). Authorized Push Payment (APP) Scams Performance Report, July.

UK Finance (2023). 2023 Half Year Fraud Update.

United Nations Office on Drugs and Crime (UNODC) (2023). Measuring Cybercrime through the ICCS Lens, ICCS Advocacy Brief #2, July.

UNODC (2024). Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape, Technical Policy Brief, October.

UNODC (2024). UNODC Research - Data Portal – Corruption and Economic Crime.

UNODC (2025). Inflection Point: Global Implications of Scam Centers, Underground Banking and Illicit Online Marketplaces in Southeast Asia, Technical Policy Brief, April.

Van Praag, E. (2025). The Future of European Payments: Faster, Cheaper, More Digital and More European: With No One Left Behind, Journal of Payments Strategy & Systems, Vol. 18, No. 4, pp. 327-341.

Wall Street Journal. (2024). IMF Warns of Cyber Risks to Financial Sector, April 18.

World Bank. (2023). “Hacking” the Cybersecurity Skills Gap in Developing Countries, Practitioner Note, November.

World Bank. (2025). Cyber Risks in Fast Payment Systems. World Bank Group, February.

Annex I. North American Industrial Classification System

Background

The NAICS is an industry classification system that groups establishments into industries based on the similarity of their production processes. It is a comprehensive system covering all economic activities. There are 20 sectors and 1,012 industries in 2022 NAICS United States.

NAICS was initially developed and subsequently revised by Mexico's INEGI, Statistics Canada, and the U.S. ECPC (the latter acting on behalf of OMB) to provide common industry definitions for Canada, Mexico, and the United States that will facilitate economic analyses of the economies of the three North American countries. The statistical agencies in the three countries produce information on inputs and outputs, industrial performance, productivity, unit labor costs, and employment. NAICS, which is based on a production-oriented concept, ensures maximum usefulness of industrial statistics for these and similar purposes.

NAICS United States is used by U.S. statistical agencies to facilitate the collection, tabulation, presentation, and analysis of data relating to establishments; and to provide uniformity and comparability in the presentation of statistical data describing the U.S. economy. NAICS United States is designed for statistical purposes. Although the classification also may be used for various administrative, regulatory, and taxation purposes, the requirements of government agencies that use it for nonstatistical purposes played no role in its development or subsequent revision.

Organization of Subsectors in the Financial Sector

The Finance and Insurance sector comprises establishments primarily engaged in financial transactions (transactions involving the creation, liquidation, or change in ownership of financial assets) and/or in facilitating financial transactions. Three principal types of activities are identified:

- Raising funds by taking deposits and/or issuing securities and, in the process, incurring liabilities. Establishments engaged in this activity use raised funds to acquire financial assets by making loans and/or purchasing securities. Putting themselves at risk, they channel funds from lenders to borrowers and transform or repackage the funds with respect to maturity, scale, and risk. This activity is known as financial intermediation.
- Pooling of risk by underwriting insurance and annuities. Establishments engaged in this activity collect fees, insurance premiums, or annuity considerations; build up reserves; invest those reserves; and make contractual payments. Fees are based on the expected incidence of the insured risk and the expected return on investment.
- Providing specialized services facilitating or supporting financial intermediation, insurance, and employee benefit programs.

In addition, monetary authorities charged with monetary control are included in this sector.

NAICS assigns codes and defines each subsector as follows:

- **521 Monetary Authorities-Central Bank.** The Monetary Authorities-Central Bank subsector groups establishments that engage in performing central banking functions, such as issuing currency, managing the Nation's money supply and international reserves, holding deposits that represent the reserves of other banks and other central banks, and acting as a fiscal agent for the central government.
- **522 Credit Intermediation and Related Activities.** Industries in the Credit Intermediation and Related Activities subsector group establishments that (1) lend funds raised from depositors; (2) lend funds raised from credit market borrowing; or (3) facilitate the lending of funds or issuance of credit by engaging in such activities as mortgage and loan brokerage, clearinghouse and reserve services, and check cashing services.
- **523 Securities, Commodity Contracts, and Other Financial Investments and Related Activities.** Industries in the Securities, Commodity Contracts, and Other Financial Investments and Related Activities subsector group establishments that are primarily engaged in one of the following: (1) underwriting securities issues and/or making markets for securities and commodities; (2) acting as agents (i.e., brokers) between buyers and sellers of securities and commodities; (3) providing securities and commodity exchange services; and (4) providing other services, such as managing portfolios of assets; providing investment advice; and trust, fiduciary, and custody services. This subsector includes establishments primarily engaged in operating commodity or securities exchange clearinghouses (including virtual currency trading exchange clearinghouses—Code 523160).
- **524 Insurance Carriers and Related Activities.** Industries in the Insurance Carriers and Related Activities subsector group establishments that are primarily engaged in one of the following: (1) underwriting (assuming the risk, assigning premiums, and so forth) annuities and insurance policies or (2) facilitating such underwriting by selling insurance policies and by providing other insurance and employee benefit related services.
- **525 Funds, Trusts, and Other Financial Vehicles.** Industries in the Funds, Trusts, and Other Financial Vehicles subsector group legal entities (i.e., funds, plans, and/or programs) organized to pool securities or other assets on behalf of shareholders or beneficiaries of employee benefit or other trust funds. The portfolios are customized to achieve specific investment characteristics, such as diversification, risk, rate of return, and price volatility. These entities earn interest, dividends, and other investment income, but have little or no employment and no revenue from the sale of services.

Source: Executive Office of the President.

PUBLICATIONS

The Rise of Cyber Events and Digital Fraud in the Financial Sector

Working Paper No. WP/2026/062