**REPORT ON FRAUDULENT TRANSACTIONS IN THE PAST FEW YEARS**

**Abstract:**

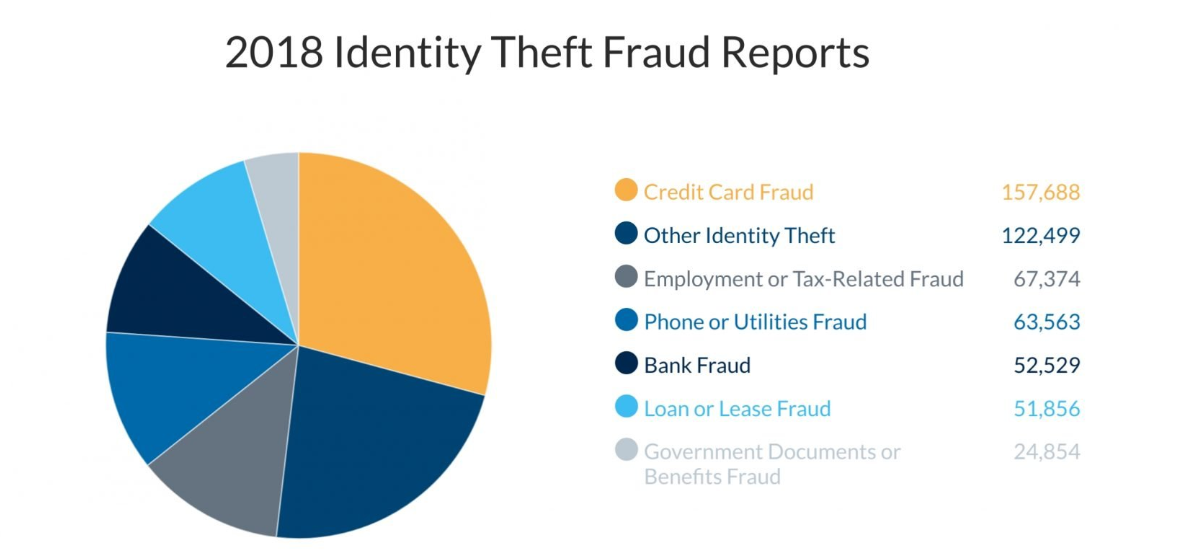
With the rapid advent in Technology, there also have been cons that many face each day, falling prey to the lure of innovations and advancements. The same road has also led people towards automating everything they use, so as to lessen the burden and hard work involved in it. Like they say, with greater power, comes greater responsibilities. In our case, with greater automation, comes a greater consequence. This report focuses on one such consequence, that we’ve all experienced at least once in our lives, a fraudulent bank transaction, or a fraudulent call trying to get to know important information from you for unimaginable and dangerous purposes. This report is a coalition of noteworthy statistics, news and predictions from trustworthy sites and organisations which one should be mindful and aware of while they continue to live in the world of automation.

**Types of Credit Card Fraud**:[**Source**: www.shiftprocessing.com]

Ways that someone can get your information to commit credit card fraud

* Stolen credit card
* Finding & Using a card that has been misplaced
* Account takeover
* **Counterfeit Cards:** Using a skimmer, thieves and criminals can make & use a duplicate card. EMV Technology (chip & PIN) has reduced this type of fraud
* **Intercepting Mailed Cards:** Cards taken from your mailbox
* **Fraudulent credit applications:** Using your taken information to apply for new credit in your name (**Identity Theft**)
* **Card-not-present fraud:** The physical card is not needed to commit fraud, just the number- increasing due to e-commerce.

**The statistics of Financial Frauds was studied from shiftprocessing.com where the below mentioned data was found:**



**$24.26 Billion was lost in 2018** due to payment card fraud worldwide.

According to statistic brain, 40% of all financial fraud is related to credit cards which amount to a total of $5.5 billion in credit card fraud worldwide.

**News Reports:**

1. Phishing attack using COVID-19 as bait expected to start today: Govt [Economic Times: June 21, 2020]

Government warned of a large-scale phishing attack expected to start from June 21, urging public to refrain from opening unsolicited e-mails, attachments and sharing private information. Attackers may use malicious e-mails under the pretext of government agencies working on COVID-19. They claim to have 20 lakh individual e-mail IDs and plan to send e-mails with subject - 'Free COVID-19 Testing'.

1. Microsoft says its digital crimes unit thwarted a massive COVID-19 phishing scam [Abaction News: July 16, 2020]

A massive scam related to COVID-19 that targeted millions of Office 365 users in 62 countries were stopped by Microsoft's digital crimes unit. One of the recent lures was a "cure for coronavirus" or "COVID-19 safety tips" from the Red Cross. The hackers were hoping Officer 365 users would take the bait and click.

1. [Cybercrooks see the coronavirus as an opportunity to steal from you](https://www.fastcompany.com/90476868/cybercrooks-see-the-coronavirus-as-an-opportunity-to-steal-your-data)

[Fast Company: March 12, 2020]

Security firms have been tracking scam emails from numerous hackers offering a fully functioning replica of the Johns Hopkins interactive map. When a user takes the bait and opens the attachment, malware is installed on their computer that’s designed to steal passwords, credit card numbers, and other sensitive information.

1. Hackers taking advantage of COVID-19 to spread malware

[Modern Healthcare: March 16, 2020]

Security researchers at IBM discovered one of the first email scams tied to coronavirus, in which a cyberattacker urged recipients to download a malware-infected email attachment by claiming it was a Word document containing infection-prevention measures.

**Credit Card Fraud Cases in India:** [**Source**: Times of India]

1) Delhi: Two nabbed for cloning ATM cards [July 13, 2020]

2) Pune techie loses Rs 3.3 lakh in credit card cloning fraud [Feb 1, 2020]

3) Ludhiana: Man uses else’s credit card to do shopping worth Rs. 1 lakh

[Feb 21, 2020]

4) Pune: Private firm staffer loses Rs 2.13 lakh in online fraud [June 11, 2020]

5) Fruit vendor loses Rs 14.49 lakh to debit card update fraud [July 10, 2020]

6) Delhi: Former bank employees held for credit card fraud [April 11, 2019]

7) Instances of cloned ATM cards in Delhi; affected customers to get refund: SBI [May 12, 2020]  
**Key Statistics** [**Source:** www.fool.com]

* There were 650,572 cases of identity theft in 2019.
* Those aged 30 to 39 reported the most cases of identity theft last year.
* Georgia, Nevada, and California were the top three states for identity theft by population.
* With over 270,000 reports, credit card fraud was the most common type of identity theft last year and more than doubled from 2017 to 2019.
* Almost 165 million records containing personal data were exposed through data breaches in 2019.
* The Capital One cyber incident was the biggest data breach of 2019, as it exposed the personal data of approximately 100 million consumers in the United States.
* Unauthorized access is on the rise and is the leading cause of exposed records with personal information in data breaches.

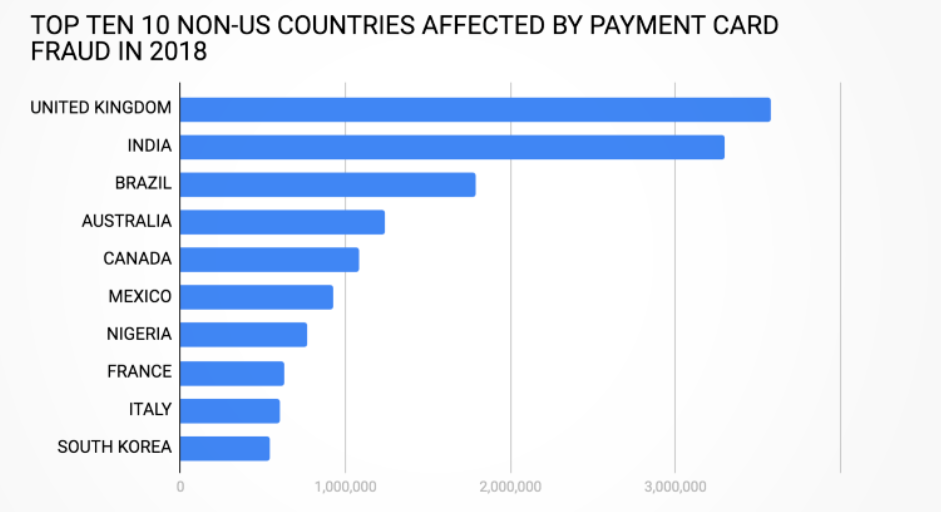
**Since the Beginning of COVID-19 Pandemic** [**Source:** Socure Research Report]

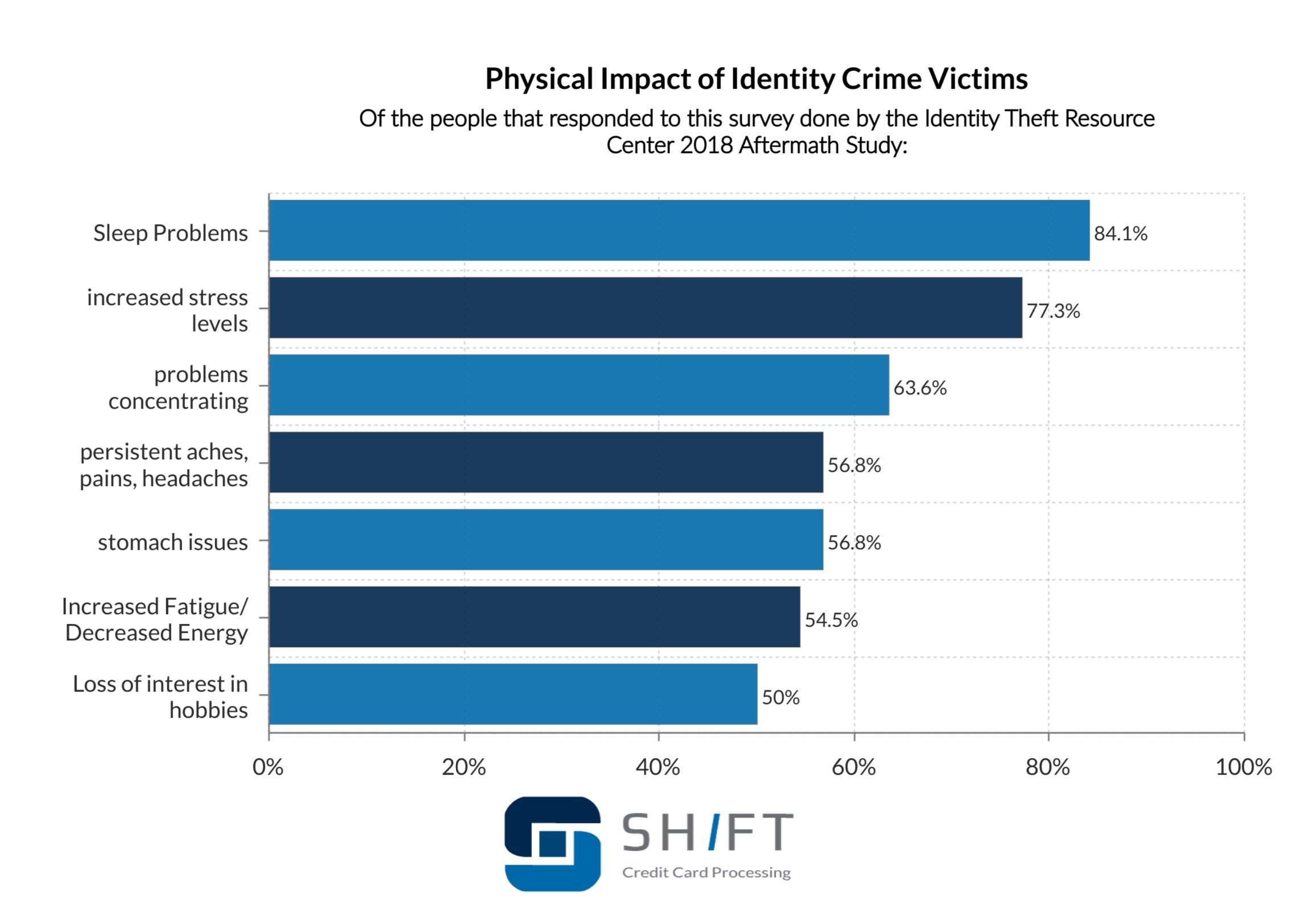
There has been a drastic increase in credit card fraudulent cases since the outbreak of COVID-19. Socure Research shows the statistics of credit card frauds since the lockdown:

**Highlights of the findings include:**

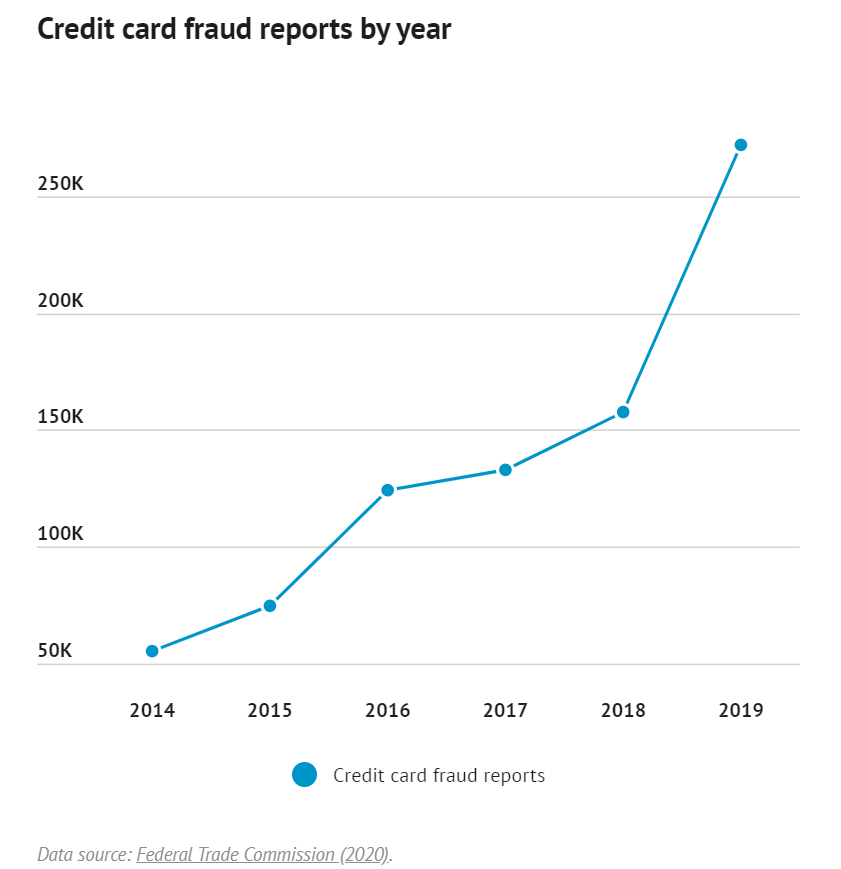
* Fraudulent credit card applications soared during the peak unemployment time to 93%
* Challenger banks experienced a 200% increase in attempted DDA fraud between March and June.
* Money transfer attempted fraud was up 43%
* Government funding of the Paycheck Protection Program led to a 65% increase in attempted fraud.
* According to research conducted by Barracuda Networks, COVID-19 related spear **phishing attacks increased by an alarming 667%** between the end of February and March 23rd – a number that has likely surged even higher since this time.
* Google saw more than 18 million daily malware and phishing emails related to COVID-19 during April.

**Important Statistics:**

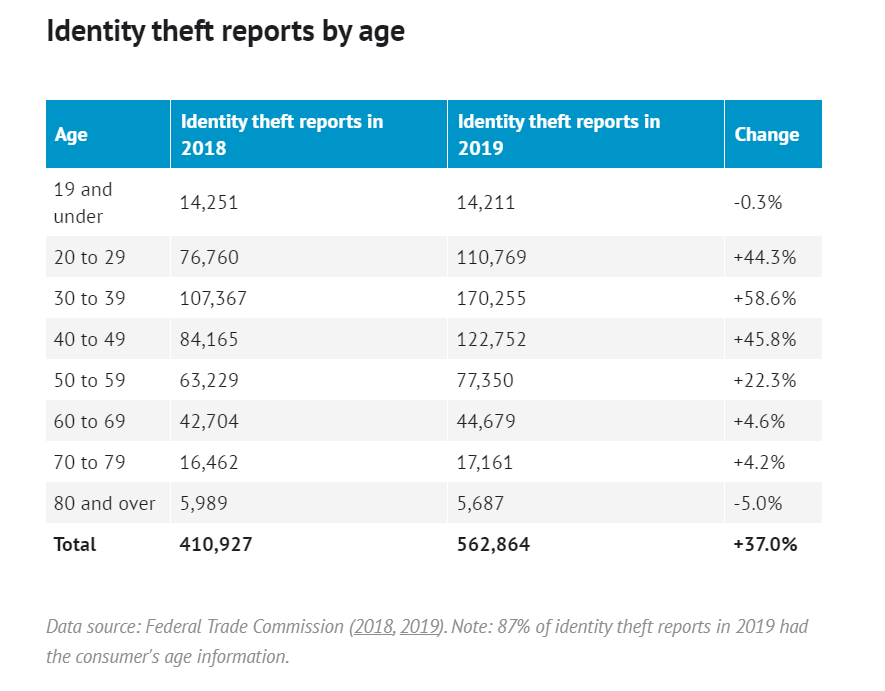
**Top Ten Non-US Countries Affected by Payment Card Fraud in 2018**

**Physical Impact of Identity Crime Victims **

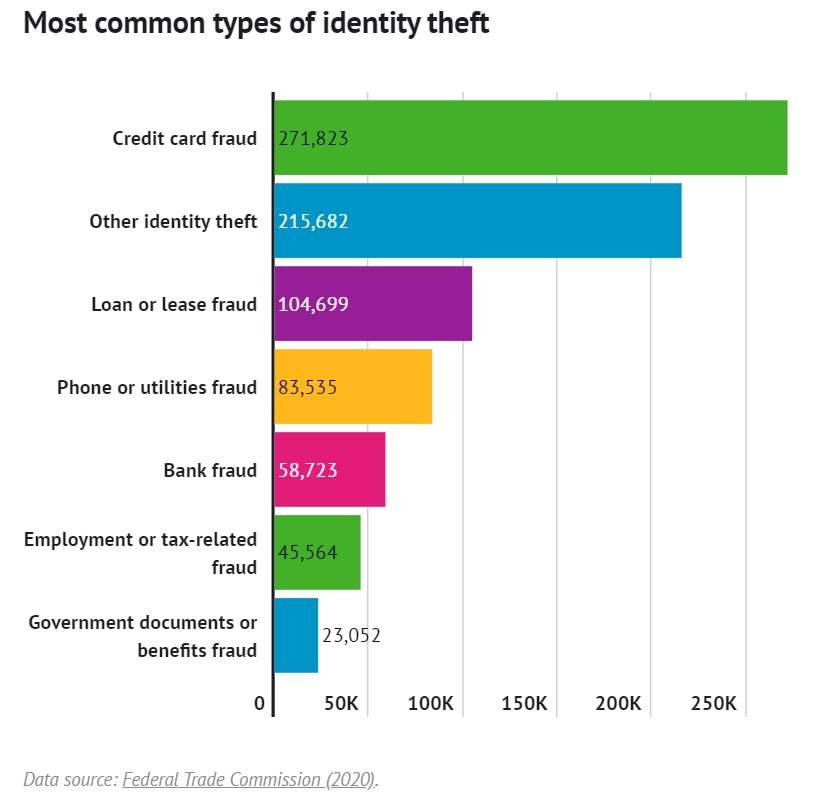
**Credit card fraud reports by year:**



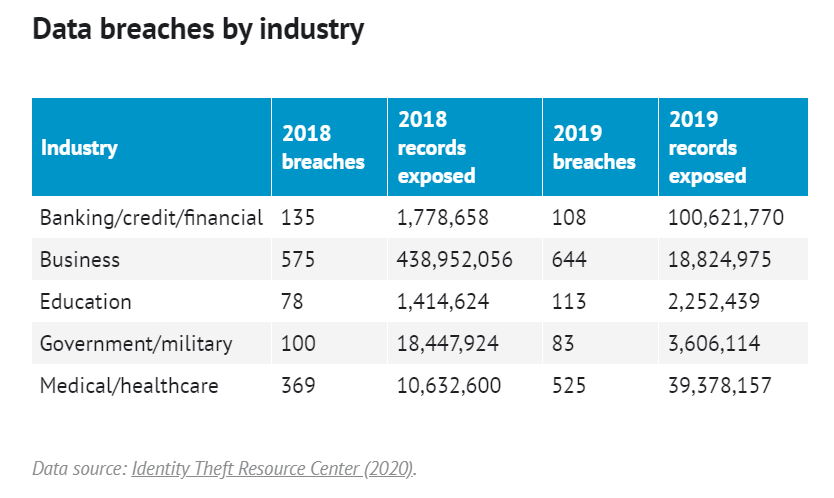
**Identity theft reports by age:**



**Most common types of identity theft:**



**Data breaches by industry:**



**Conclusion:**

The more we advance towards automation and technology, the more we end up witnessing frauds and breaches. Any data is sensitive, if fallen into wrong hands, the effect and consequences can be disastrous. These frauds and malicious attacks call for a **ground-breaking innovation** which can help little by little to help everything fall into the right place. We believe that **Card Pay** holds the potential to make one feel safe and secure while enabling one to experience a seamless transaction.