VIEWPOINT

ARTHUR D LITTLE
2022

BETTER TOGETHER

FACING THE FRAUD INDUSTRY ON ITS OWN TERMS

Fraud is big business, costing the global economy an estimated US $5 trillion per annum, according to a report by Crowe and the Centre for Counter Fraud Studies. It is a problem no one can afford to ignore, as businesses and consumers struggle with the direct cost and associated disruption to economic life. Most worryingly, the incidence of fraud has increased as a result of mass digital adoption during COVID-19. This Viewpoint explains why a business-as-usual approach to managing fraud simply won't do.

AUTHORS

Juan González

Raimundo Cisneros

Salman Ali

Rocío Castedo

Juan Abascal

THE FRAUD THREAT

COVID-19 supercharged the shift to digital. Several observers have remarked that during the pandemic, businesses and consumers achieved in a single year what previously would have taken five years. A great deal of work became digital, turning office space into a liability. Shopper footfall vanished in high streets and malls because anything that could be delivered was available for delivery. The result has been an unexpected bonanza for product manufacturers, e-commerce platform providers, and delivery companies.

But while societies learned to do almost everything digitally, another bonanza emerged in parallel: fraud. Criminals saw the opportunity to use the same digital tools for nefarious means, finding and monetizing exploits to help themselves to other people's money. The US Federal Trade Commission (FTC) reported that 2021 showed a year-on-year increase of 70% in reported fraud losses. In reality, that figure is likely to be higher because reporting systems are only estimates and victims' losses are rarely reported to the authorities.

This Viewpoint provides context to decision makers on why businesses in general — and financial institutions in particular — cannot deal with the fraud challenge on their own. We also propose a course of action for initiating change.

FRAUD, CHARACTERIZED

We all have an intuitive understanding of fraudulent behaviors as those directed toward cheating somebody to get money or goods illegally. However, the scope of fraud is so broad that it allows for multiple interpretations. The very concept of fraud does not have a standardized definition among companies, much less across countries and sectors. Consequently, reporting is scarce and never homogeneous. Therefore, any study must begin by laying the grounds to which it is referring. In this Viewpoint we focus on three broad types of fraud:

> THE SCOPE OF FRAUD IS SO BROAD THAT IT ALLOWS FOR MULTIPLE INTERPRETATIONS

1. **Card fraud.** Unauthorized use of a debit or credit card to obtain a fraudulent benefit. It includes **card not present (CNP) fraud** (a criminal uses stolen card details to buy something on the Internet, over the phone, or through mail order), use of lost or stolen cards, and user ID theft, among others.
2. **Digital fraud.** Unauthorized use of digital channels, including:
   - **Account takeover.** Digital criminals compromise the online credentials of customer accounts to take over customer accounts and conduct fraudulent transactions in many types of schemes.
   - **Authorized push payment fraud (APP scams).** Victims are tricked into authorizing a payment from their own account to another account that is being controlled by a criminal.
   - **Application manipulation.** Malicious software modification aimed at changing the functionality of the system for fraudulent gain.
   - **CEO fraud.** A variant of cyberattack based on impersonating or deceiving high-level executives, achieving financial transactions outside of the customer's normal processes, with the aim of diverting funds to the fraudsters.
3. **Admission fraud.** Fraudulent applications using false or adulterated information for the subscription of credit products without meeting contractual payment obligations, including:

- **Account-opening fraud.** Criminals use stolen personal information to open new accounts for fraudulent activity such as borrowing money in another person's name.
- **Synthetic identity fraud.** Using a blend of fake information and real data to create brand new fake identities, expert-level criminals establish and build up an online credit history.

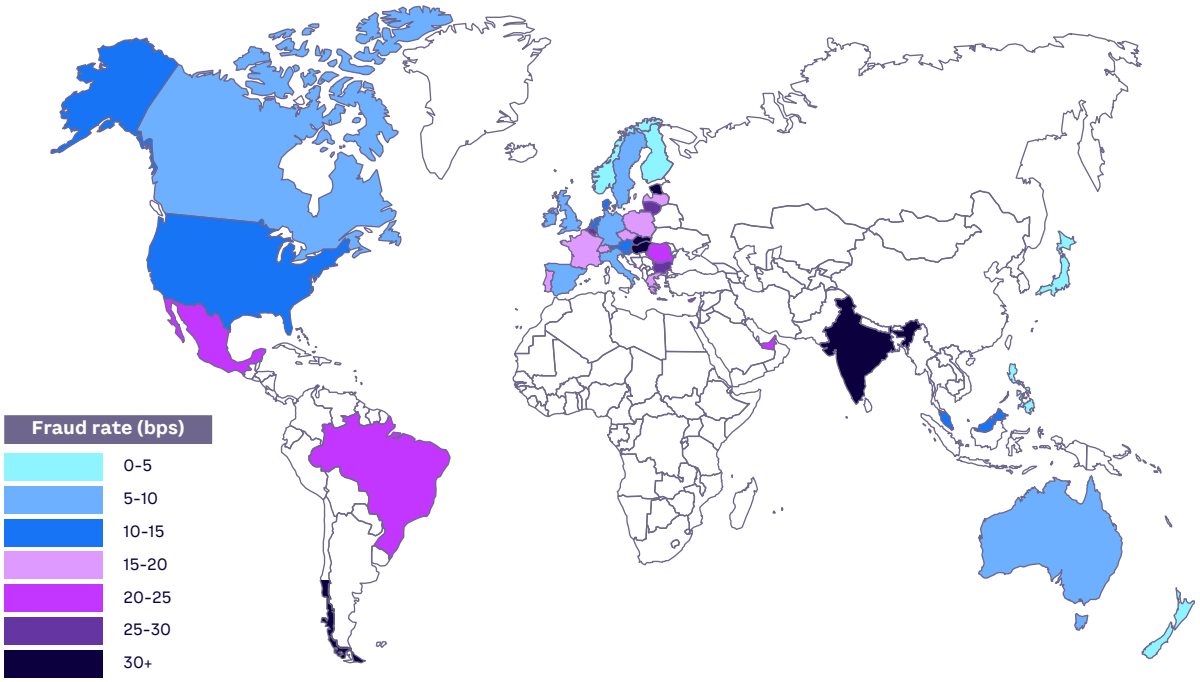
The relevance and impact of each type of fraud varies considerably by geography, as shown in the "Online Fraud Trends and Behavior" report from Stripe (see Figure 1).

In countries that use relatively weaker identity systems (as in the case of Mexico and Brazil, but also in the US as compared to other European countries) fraud impact is much more relevant. In the case of the US, fraud is ranked as the third concern for financial entities, according to Engageware.

THE RELEVANCE AND IMPACT OF EACH TYPE OF FRAUD VARIES CONSIDERABLY BY GEOGRAPHY

In markets where the economy has accelerated its shift to digital, fraud in digital channels is at the top of the list of fraud typologies. In these markets, the most common fraud attack businesses encounter are APP scams, followed by account takeover fraud. Admission fraud, including account-opening fraud and synthetic identity fraud, are the next categories in the ranking according to Experian, although their financial impact is more commonly reported as loan defaults than as fraud.

Figure 1. Country-level fraud rates



Source: "Online Fraud Trends and Behavior." Stripe, 2017 (used with permission)
Note: Radar helps detect and block fraud for any type of business using machine learning

Fraud is inextricably linked to identity. Fraudsters succeed when they can impersonate one of the participants in a transaction. Reinforcing identity management is an essential step to reduce fraud. Traditional approaches to identity management focus on on-boarding controls (to limit the risk of granting credentials to unlawful applicants) and sophisticated validation and verification rules such as those used to accept transactions involving bank customers. Big tech players have shown the value of adopting a broader view to validate identity, considering attributes describing the customer context (e.g., residential address, email, phone number) and attributes accumulated over time by the customer (e.g., transactional history, search and typing behavior, and preferences) to enrich core digital identity. Tracking patterns of changes in customer context or behavior facilitates better protection against fraud.

FRAUDSTERS CAN LEVERAGE PEOPLE'S WILLINGNESS TO SHARE PERSONAL INFORMATION IN INCREASINGLY INSIDIOUS WAYS

A GLOBAL, GROWING, INCREASINGLY SOPHISTICATED INDUSTRY

Most digital criminals are neither isolated amateurs nor local groupings of enterprises. More commonly, they are defacto transnational networks run by criminals to engage in illegal activity for profit, just like other branches of organized crime. While some digital crime is highly structured in criminal hierarchies or syndicates, most criminal activity is not organized within coherent groups. Rather, they are specialized teams in one or more aspects of fraud, conducting a set of specific activities to achieve particular outcomes.

As with every other global industry, digital criminals have benefited from the proliferation of new technologies, the Internet and the massive adoption of e-commerce. Increased loss of control over personal information allows for the industrialized invasion of privacy, leading to identity theft at scale through sophisticated attacks and systematic massive attacks, targeting both individuals and enterprises, including banks.

Fraudsters can leverage people's willingness to share personal information in increasingly insidious ways. For example, social engineering is a new attack vector in which a user is deceived by a fraudster through scam techniques that rely on fake intimacy and can lead to emotional blackmailing, harassment, and cyberstalking.

As criminal activity becomes more sophisticated and global, attempted fraud is growing annually at double digits in most geographies. In addition to the FTC's reported year-on-year increase of 70% in fraud losses, UK Finance indicated that in the first half of 2021, fraud increased more than 30% over the first half of 2020. For its part, Mexico reported a 52% increase of fraud claims in 2021, according to *Forbes* Mexico.

FRAUD-RELATED CUSTOMER LOSSES CONSTITUTE A SOCIAL PROBLEM

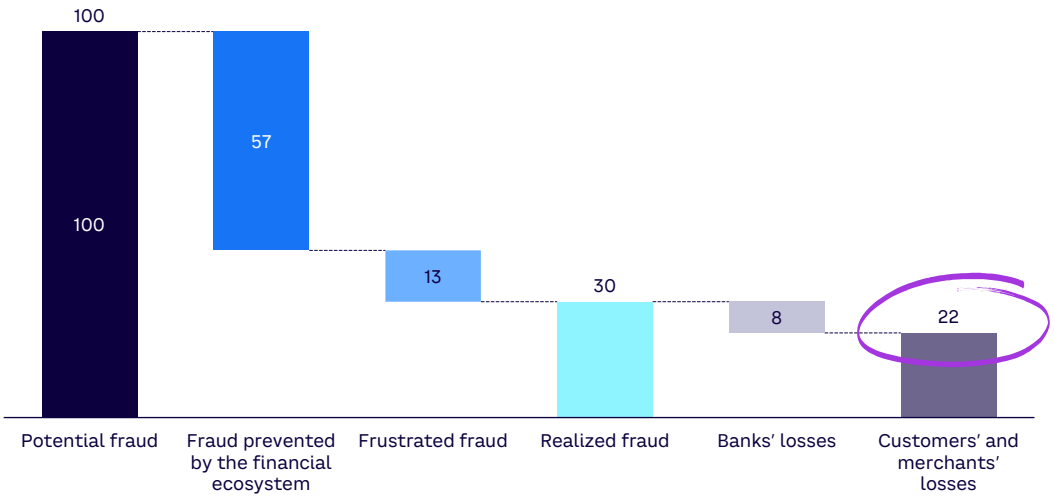
FRAUD'S IMPACT ON SOCIETY

Financial services providers can prevent almost 70% of all attempted fraud attempts. According to recent Arthur D. Little (ADL) project experience, the burden of realized fraud (the non-prevented 30%) is split into a third that is assumed by banks and two-thirds by end customers and merchants (for an international bank, see example in Figure 2).

Fraud-related customer losses constitute a social problem. People who have been attacked by a fraudster not only suffer financial harm, but in most cases also need to invest time and resources to clean up the mess. Beyond that, they must deal with feelings of vulnerability the deception has caused. Those who have been defrauded also lose trust in financial institutions, believing that their financial services provider could have been more diligent.

Figure 2. Total potential fraud breakdown

Figures indexed to 100[1]



Source: Arthur D. Little, built on ADL casework for an international bank
Notes: 1) There are loss recoveries received from insurance policies taken out by the banks themselves

Society should be made aware of the aggregated magnitude of the problem as well as the primary forms of fraud and patterns used in each region. In most geographies, the public lacks insight into the volumes and types of fraud. Banks are reluctant to show their fraud losses, and few regulators are making efforts to generate reports that unify fraud definitions and criteria across the financial sector, but they do now include a measure of the monetary impact of fraud. The UK is the only country that reports this type of information at aggregate level.

On the other hand, while there is a perception that online fraud primarily affects the elderly and vulnerable, young people are increasingly likely to fall victim. Social media plays a significant role in online scams, and further education is needed to make young people aware of the dangers of sharing personal information online. Young people may also be more vulnerable to fraud than older generations because they have a quite different approach to personal information. For example, some young people have been known to share pictures of their passports and driver's licenses on social media, putting them at increased risk of identity theft and fraud. Awareness of best practices to stay safe online remains low.

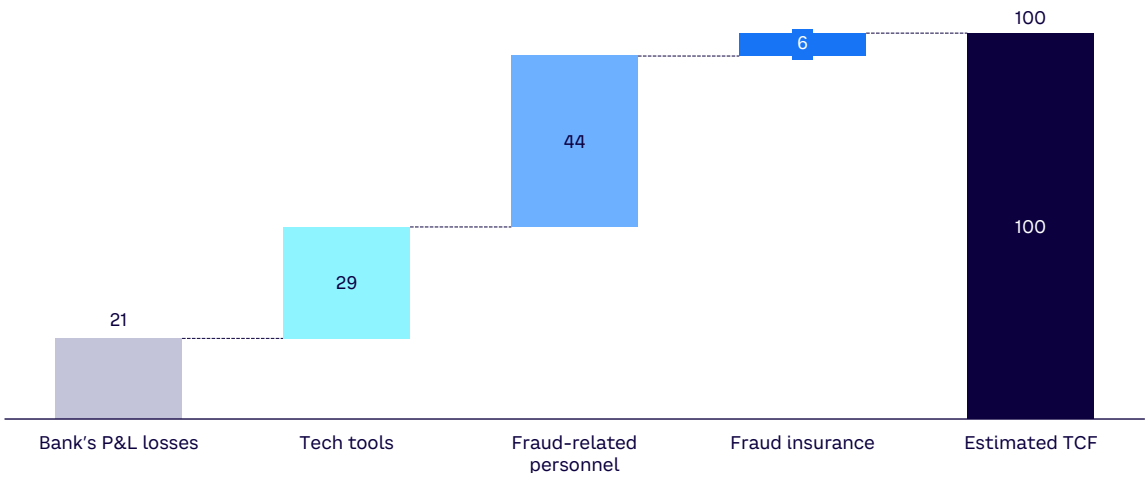
AWARENESS OF BEST PRACTICES TO STAY SAFE ONLINE REMAINS LOW

FRAUD'S IMPACT ON BANKS

The impact of fraud on banks goes beyond any monetary losses incurred during an attack (see Figure 3). ADL estimates that the total cost of fraud for banks could reach €2-€4 per customer. Banks invest heavily to protect themselves and their customers from fraud. Almost 80% of total fraud-related costs include technology for monitoring and detecting fraud, personnel to perform investigations, and case management and insurance to protect the bank from the financial damages resulting from fraud. And we expect technology and resources budgets to increase to respond to expected additional regulatory requirements. As an example, regulatory initiatives are currently being considered to force all UK banks to reimburse victims of APP scams, marking a landmark win for victims.

Figure 3. Total potential fraud breakdown for an international bank

Figures indexed to 100



Source: Arthur D. Little

Fraudulent behavior performed by professionals is notoriously difficult to detect amid the enormous number of legitimate transactions a financial institution carries out every day. Fraud is the quintessential needle-in-a-haystack problem.

Historically, to identify fraud attempts, banks have relied on heuristics and expert judgment. Rules have been developed from an extremely limited amount of fraud cases. Moreover, banks have sought patterns within data associated with financial transactions with limited access to context and behavioral data.

Machine learning and artificial intelligence change the playbook. Banks are now able to implement behavior analysis along the overall customer journey, from onboarding and identification to transaction execution or even other requests (i.e., change of address) to detect any anomaly before it happens. Investments bring significant payoffs. Adding behavioral analytics to the monitoring of the customer transactional history can improve fraud detection rates by 25%, according to ADL project experience. The new tools can also bring cost savings, as they deliver information in a form that does not require data scientists to interpret it.

When considering technology platform alternatives to fight fraud, a financial institution has no best alternative a priori. The options include development of a new shared bank-bancassurer platform, migration to one of the available platforms, or coexistence and communication between existing platforms. Decision makers should study each case, considering the circumstances and strategies of the stakeholders.

The selection of one option involves the relationship between entities. One stakeholder might be a subsidiary of another and, thus, its platform might be embedded in the parent environment. The chosen alternative must ensure that non-related areas are not impacted and their regular operation is preserved.

Other key analyses are related to security and access control issues. IT security as well as the legal department should thoroughly examine these issues. Additionally, decision makers should consider the platform's evolution roadmap, as it might affect the usage of specific software and economy-of-scale opportunities.

CAN WE DO BETTER?

Despite these efforts, non-prevented fraud continues to grow at double-digit rates. Governments and banks must act and be certain not to underestimate the problem.

First, governments and banks should provide greater consistency and transparency on fraud figures to ensure that those potential vulnerabilities in the system are addressed as a priority. Society and the banking industry will benefit from seeing where patterns are emerging at the aggregate level.

Providing more transparency into fraud could also make the public more aware of the magnitude and nature of the problem. Awareness campaigns are key in helping people to avoid becoming victims. But public involvement should go further. Particularly regarding schemes in which customers are tricked into facilitating their payment credentials, customers should have a more active role in signaling the issue in order to accelerate an effective response.

Banks also need to improve the way they work together in responding to fraud. Today, each bank has its own fraud-fighting team, with its own process, along with custom platforms that support the process flow and accompanying decision making. This makes them collectively disorganized and hence vulnerable to attack, making it hard to police everything from data to security.

It is not enough for each entity to adopt its own cutting-edge technologies (such as continuous auditing, big data analysis, and profiling) that are available today. As the process becomes increasingly data-driven, access to larger, more time-relevant sets of data becomes essential. The value of collective protection against fraud is higher than the sum of the individual initiatives. Banks will need to cooperate with competitors to build a robust fraud-protection scheme.

As a start, competing banks could share best practices. They could also establish means to share information and add increased joint levels of scrutiny to suspicious transactions. Finally, they could build a better common toolbox for fraud-detection algorithms trained over the whole system and not only on local cases.

Cifas, the UK's fraud-prevention community, provides a good example of the value of cooperation. Cifas leads the fight against fraud by sharing data, intelligence, and learning. It was founded as a not-for-profit company by seven retail credit providers. All Cifas members (currently 600), coming from all industries affected by fraud, record instances of actual and attempted fraud, enabling other members to search and learn from the data.

THERE IS OPPORTUNITY TO REDUCE FRAUD THROUGH GLOBAL COLLABORATION AMONG FINANCIAL ENTITIES

Banks, as heavily regulated and trusted companies with a large base of customers and robust identity-verification processes, are the right candidates to lead on digital identity. An industry-wide banking identity platform, assuring the quality and strength that banks require, could be open to third parties and enrich customer behavior information to further reduce the impact of fraud. For example, the Norwegian banking sector has been working since 2000 on developing a joint identity infrastructure and today, BankID offers secure authentication and signing to digitally recognize 4 million Norwegians. The tool is being used by all of the country's banks and public digital services. With strong enough identity models, banks could even protect third parties against fraud and insure their payments against fraud attacks.

There is an opportunity to reduce fraud and its associated costs through a global collaboration initiative among financial entities. Such an approach makes economic sense for the banking industry as well as doing the right thing to protect consumers.

CONCLUSION

TACKLING THE FRAUD THREAT

GOVERNMENTS AND BANKS ARE NOT DOING ENOUGH TO TACKLE ONLINE FRAUD

Tackling fraud should not be an individual fight. Fraud is a social problem, and that's why financial institutions and governmental organizations should join forces. Some points to consider in the fight include:

1. Fraud is a global phenomenon with great economic impact; however, the response of the financial entities is almost always local and lacks coordination.
2. The victims of fraud are mostly consumers, although financial institutions are also heavily affected, both in terms of losses and the indirect costs associated with fraud.
3. Strong identity verification is already playing a significant role in terms of detecting fraud.
4. Governments and banks are not doing enough to tackle online fraud, and their response has not been proportional to the scale of the problem.
5. Governments and other bodies must provide transparency on the scale and forms of fraud while leading awareness campaigns.
6. Financial institutions must take more responsibility and work together to tackle the problem of fraud head-on.


F2
F3
F4
F5
F6
F7
£
3
$
4
%
5
^
6
&
7
E
R

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.