

accenture

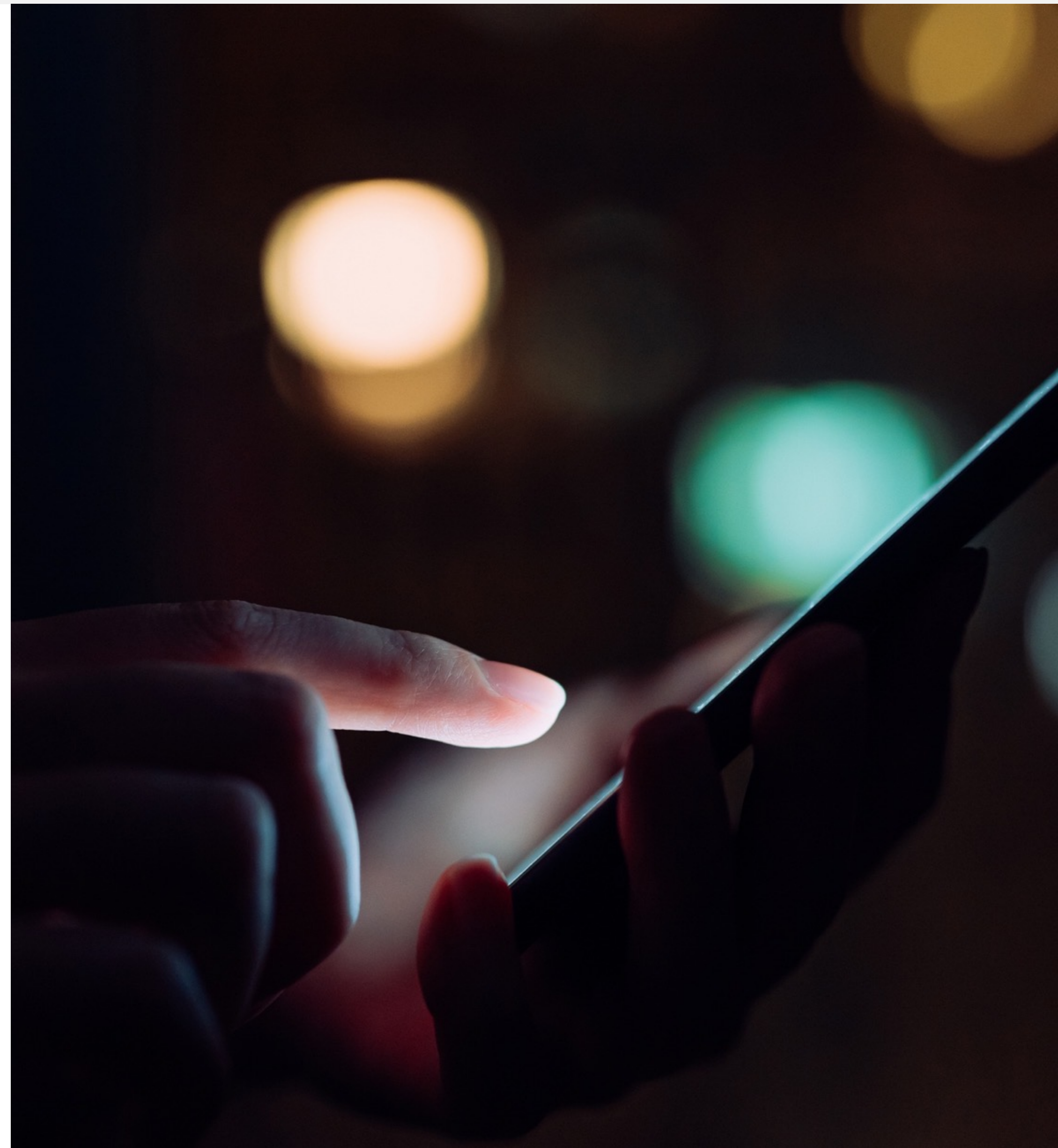
Cracking the code on consumer fraud

How public safety agencies can address
the growing challenge



Table of Contents

3	Executive summary
5	Consumer fraud: The “volume crime of our time”
10	Fraud will rise... but how fast and how high?
14	Barriers to change
17	Actions for public safety agencies
27	Reining in future consumer fraud
32	Appendix



Executive summary

A watershed moment for public safety agencies

Consumer fraud—fraud perpetrated against the public—has been growing steadily over the last decade. However, the pandemic supercharged its growth as remote work and a greater reliance on technology were spurred by lockdowns across the globe. The evolving nature and escalation of consumer fraud is impacting more victims and resulting in financial and psychological harm. It is also challenging the way public safety agencies operate today.

Public safety organizations understand the need to respond and are evolving their operations to keep pace with the fast-changing tactics of criminals engaged in consumer fraud. However, it's clear that this

threat is only likely to become more severe, and public safety agencies recognize the significant risks that could arise from a failure to combat its impact. It's a watershed moment.

The question is: What's the best way for public safety agencies to move forward? To help them respond, we developed four modeling scenarios, based on eight different countries, to forecast the growth of consumer fraud victims as well as direct and indirect costs to those victims. We also interviewed 14 leaders of public safety divisions, such as the Royal Canadian Mounted Police (RCMP), the US Federal Bureau of Investigation (FBI), and the UK's National Crime Agency (NCA), as well those from international agencies like Europol and Interpol, to inform about actions public safety agencies should take to keep up with the future of consumer fraud.



“Traditionally, law enforcement measures success on arrests and charges—but that's only one measure of success for cyber-enabled crime. The problem is so large, you can't arrest your way out of it. We need to change our thinking of success to include preventing and disrupting”

— Commander, Cybercrime Squad, State level, Australia

Based on our research, we identify four key pillars that pose significant barriers to change: ecosystem partners, citizen engagement, the public safety workforce and technology enablement. However, these pillars also reflect where opportunity for change can be found.

Indeed, there is real reason for optimism. Organizations are becoming more adept at preventing and disrupting consumer fraud and this, combined with greater public and political awareness and new technologies, offers a potential step-change in how law enforcement combats financial crime.

To achieve such advancement, agencies must approach consumer fraud in a new way, pursuing a more intelligence-led, proactive and collaborative path forward. Public engagement and awareness are key and while public safety agencies will do all that they can to stop fraudsters before crimes occur, attempts will get through.

Public awareness can reduce the likelihood of these attempts becoming successful. We identify three stages of operational response that public safety agencies participate in when combatting consumer fraud, and provide recommendations for change across them: **intelligence collection and analysis; prevention and disruption; and detection and investigation.**

As consumer fraud becomes more intrusive, sophisticated and cross border, it is increasingly evident that it can't be fought by a single entity. Combatting it requires a whole-of-government approach and, indeed, a whole-ecosystem approach in which government agencies and private sector organizations work together to innovate and deter fraud.

Our research shows there are many promising avenues to pursue in order to combat current trends in consumer fraud.

Doing so holds the promise of reducing the level of threat, risk and harm to the public, sustaining public trust and safeguarding economic prosperity.



“What does good look like...a person who has been victimized by fraud feels safe and educated...they feel safe afterwards and feel safe for the future”

— Temporary Director, National Economic Crime Centre, UK National Crime Agency

A close-up photograph of a man with dark hair and round glasses, wearing a black and white striped shirt. He is looking intently at a smartphone held in his left hand, with his right hand resting on his chin in a thoughtful pose. The scene is dimly lit with a blue and purple glow, suggesting a nighttime or indoor setting with artificial light. The background is blurred, focusing attention on the man and his device.

**Consumer fraud:
The “volume crime
of our time”**

Consumer fraud has been growing steadily...

The Credit Industry Fraud Avoidance System (CIFAS), a non-profit that manages the largest database of fraudulent activity in the UK, has described fraud against citizens as the “volume crime of our time.”¹ It is increasingly perpetrated digitally and often internationally, with funds sometimes crossing borders multiple times before becoming untraceable.

...but the pandemic turbocharged its growth

While consumer fraud has been rising for years, the pandemic dramatically accelerated its growth by creating optimum conditions for it to flourish (Figure 1). These include a major shift of workers and consumers to digital channels, negative economic conditions and a rise in household debt, as well as greater victim vulnerability as a result of stresses on their financial, physical and mental health. Consumer fraud has begun to hit record levels in terms of the number of victims and volume losses.²

Defining consumer fraud

In our study, we have used consumer fraud as a broad term to refer to any fraud that results in financial losses to a citizen. Some of the leading types of consumer fraud across geographies were noted as authorized push payment scams, credit/debit fraud, romance scams, mortgage scams, retail/e-commerce fraud and advance-fee fraud. Commercial fraud, targeting government agencies or private sector companies, is not included.

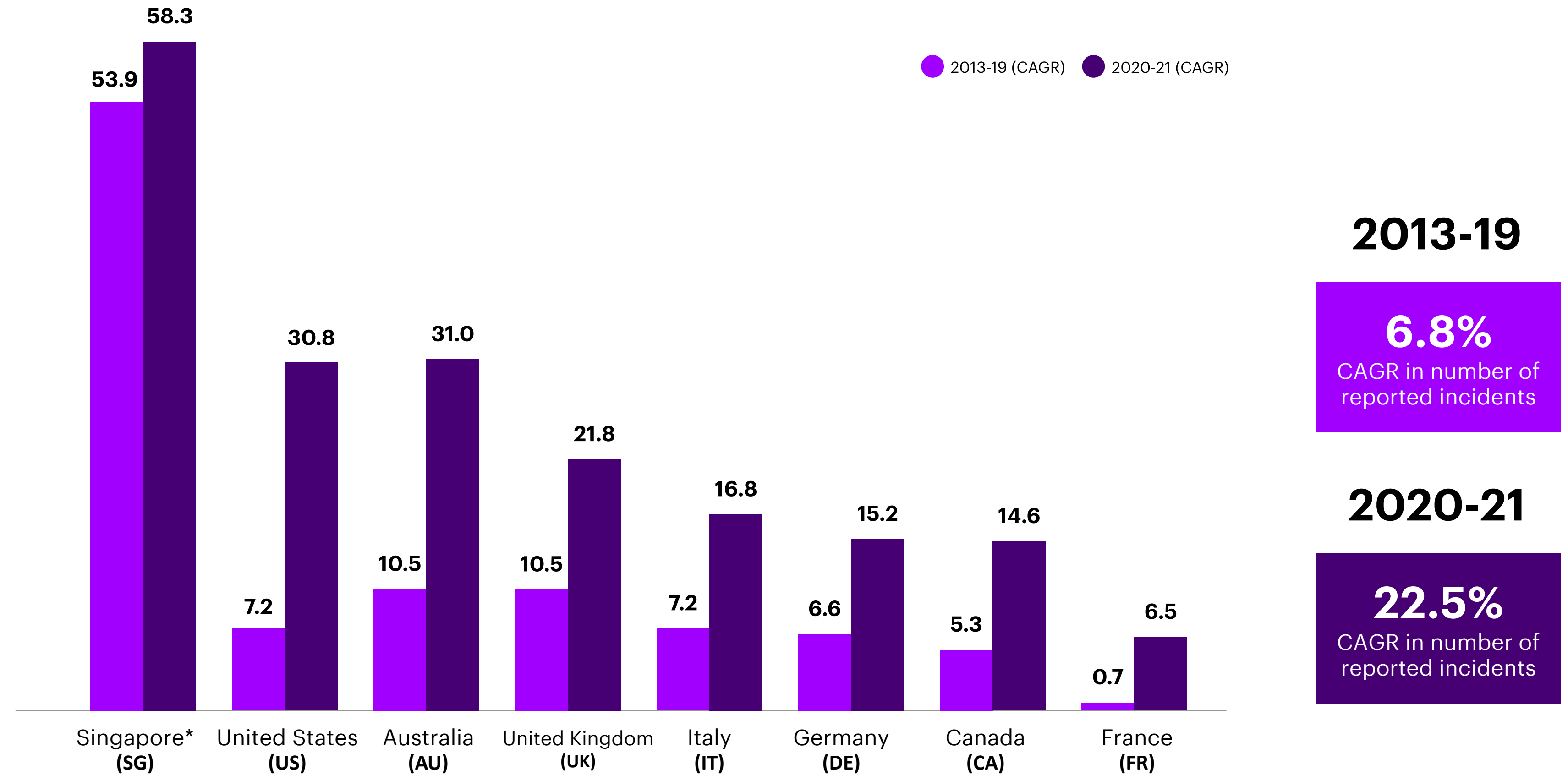
As consumer fraud is defined differently by different organizations and across different jurisdictions, there is some variability in reporting on consumer fraud between countries. For the purpose of this report, efforts have been made to make the data as comparable as possible between jurisdictions.



Based on eight countries in our study—Australia, Canada, France, Germany, Italy, Singapore, the UK and the US—we found that fraud incidents grew nearly 50% from 2013-2019, reaching US\$89B. However, the total cost of fraud in 2021 hit US\$143B, growing nearly 60% in just two years combined (see Appendix 1). Put simply, the growth in consumer fraud in 2020/2021 exceeded the total increase seen over the previous six years.

Figure 1: Annual compound growth of consumer fraud in 2013-2019 vs 2020-2021

(percent change in the number of reported cases for selected countries)



*Singapore's data releases on the extent of consumer fraud as a crime type began only in 2017. Prior, data tracking on consumer fraud was limited, and the definition has been broadened over the years for tracking purposes. Accordingly, the period pre-pandemic reflects a larger rate of growth than that of most other countries.

CAGR: Compound Annual Growth Rate

Impetus for action

Recently, there have been calls for new legislative proposals to tackle economic crime as a matter of priority across several jurisdictions, and the creation and adaption of public safety entities to tackle fraud continues at pace around the world. The reason for increased mobilization is clear: impacts are becoming more severe, public confidence is at risk and costs to government are rising in tandem with the rise in consumer fraud.

Impacts are becoming more severe

It is not just the overall incidence of fraud that's rising fast—average losses per victim are increasing too. The US Federal Trade Commission, for instance, reports average losses per victim in 2021 to be significantly higher across every fraud type compared to 2019.³ What's more, as this happens people are feeling more like victims, a trend that's likely to increase as banks become less willing to compensate for losses. If financial institutions become less likely to

compensate victims, expectations will likely mount for greater action from law enforcement. An example of this can be seen in the UK where authorized push payments (APP) have grown rapidly in recent years with the use of social engineering techniques. This type of fraud is of higher average value compared to many other fraud types and has lower customer refund rates by financial institutions. As a result, consumers are increasingly turning to law enforcement as they seek action and redress for APP fraud compared to traditional fraud methods, such as card fraud, which has close to a 100% refund rate by financial institutions in the UK.⁴

The nature of fraud is becoming more aggressive, intrusive and personal

As people spend more of their lives online, the personal details and sensitive information that they risk compromising also rises. Criminals are all too aware and are swift to take advantage, with increasingly sophisticated and ever-evolving tactics that harness advances in technology to exploit

vulnerabilities. And as the potential gains of consumer fraud increase with a perceived lower risk, this brings with it the interest of organized crime, which has the resources to develop consumer fraud operations on an even greater scale.^{5,6} As the Royal United Services Institute (RUSI) points out, “the very scale and nature of the most prevalent fraud typologies denote the involvement of organized crime groups, given either the sheer volume or the need for specialist skills to perpetrate the fraud.”⁷ The necessity to view consumer fraud in connection with serious and organized crime could help to close intelligence gaps and mitigate what is starting to be considered by some as a national security threat.

Securing trust

Governments are increasingly recognizing that fighting consumer fraud is critical to building and maintaining public trust and confidence. Today's reality is that citizens in many jurisdictions are more likely to fall victim to consumer fraud than to any other type of crime.

“[In Canada], the first nine months of 2021 was already a record year in terms of reporting and list value [compared to] 2020; and 2020 was a record year.”

— Director General of Anti-Fraud Center, National Police Service, Canada




In fact, national crime surveys from Australia, Canada, Singapore and the UK indicate that approximately every two years, 53-60% of consumers are targeted with attempted fraud.^{8,9,10,11,12} As the RUSI report points out: “failures in the response to date [by law enforcement] have the capacity to undermine public confidence... [and] public faith and trust in government.”¹³

Trust and confidence in policing have come into increasing focus in many parts of the world for a range of reasons. Making sure that crime is seen to have consequences and that policing can combat all crime types that impact communities is key to building and maintaining this trust. And as the incidences of consumer fraud and its impact on victims continue to grow, it is critical that public safety agencies are seen to be responding effectively. It is also important to acknowledge that many attempted frauds remain just that and the education and engagement of the public is key to helping ensure they are less likely to become victims.

Consumer fraud’s high costs for government

Many countries are now recognizing that preventing consumer fraud costs less than resolving it. In the UK, for instance, a 2018 report by the Home Office showed that costs incurred by the criminal justice system in response to fraud were £10 higher per incident than those incurred in anticipating and preventing it.¹⁴ In addition, some agencies have been able to put a unit cost to working on a single fraud case, providing insight into the anticipated cost burden of any incremental increase in fraud.

It’s clear that consumer fraud is a growing threat for citizens and governments. But what is likely to happen in the future? To predict the future growth of consumer fraud we used publicly available data to identify some possible scenarios.

A hand is shown interacting with a large digital screen. The screen displays a world map with various data visualizations, including a grid of blue and white squares, a keyboard layout, and the text 'WORLD CONNECTION'. The background is a dark blue with a grid pattern. The hand is positioned over the map, suggesting a focus on global connectivity and data analysis.

**Fraud will rise...
but how fast and
how high?**

Victims and losses set to grow

Given the rate of fraud increase that we've already seen, looking into the future means it's no longer a question of 'will fraud continue to rise?', but rather 'how fast and how high?' The four scenarios we created based on historical trend data¹⁵ all highlight a substantial growth in fraud over the coming five years.

An increase in victims is anticipated no matter the scenario...

Our analysis shows that fraud will continue to affect a higher share of the population. Our most optimistic scenario shows fraud impacting 17% of the total population of countries we surveyed by 2027. In contrast, our pessimistic scenario forecasts this rise to reach 24% of the population over the same period (Figure 2). To put this in greater context—these increases compare to 7% of the population being affected by fraud during 2013-2019.

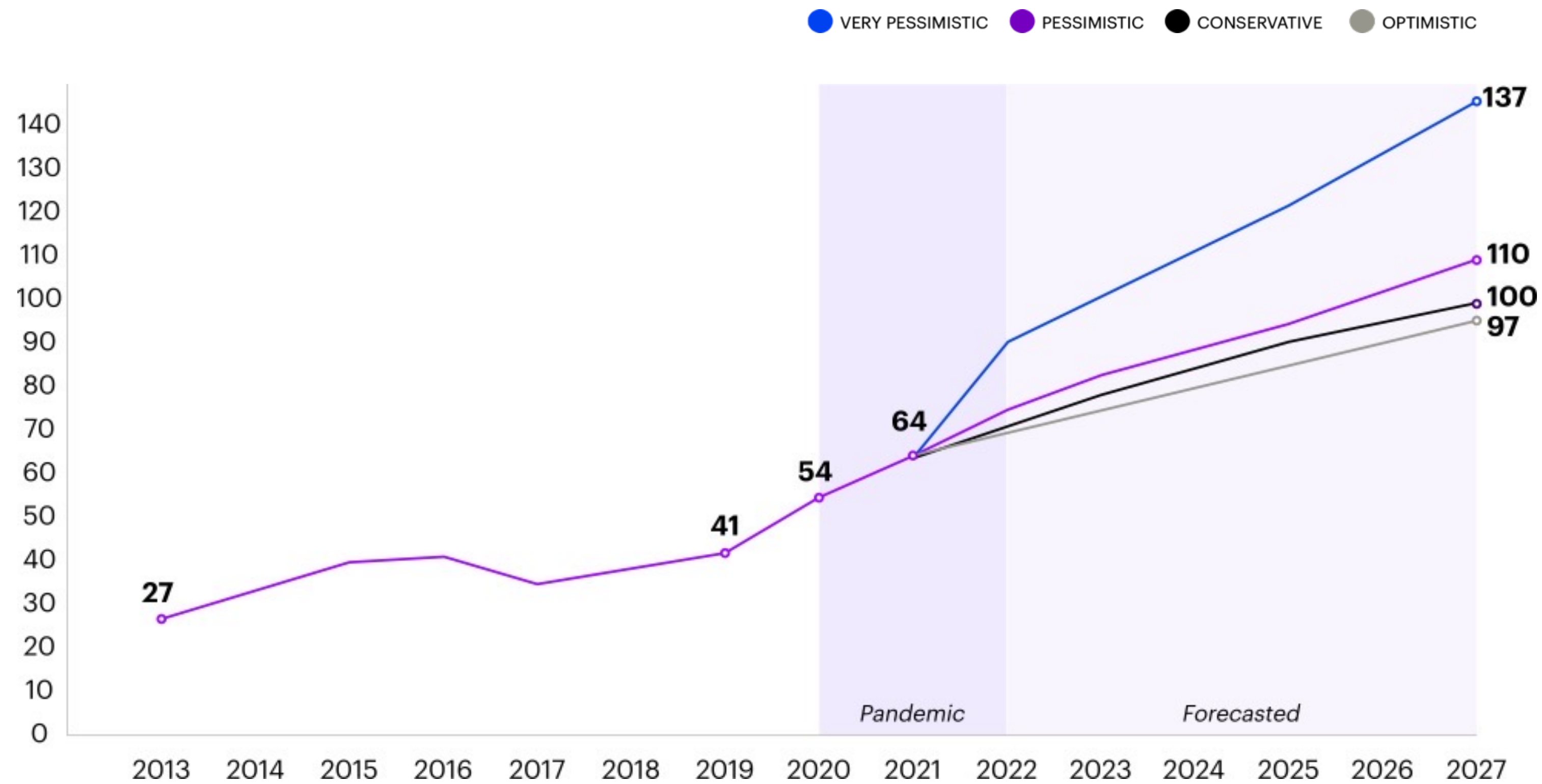
...along with a rise in direct financial losses

It follows that direct financial losses from consumer fraud are also expected to rise. Our optimistic scenario points to losses rising to US\$94B in 2027; the pessimistic case anticipates this total to reach US\$157B by 2027. That translates to the burden of fraud, as a percentage of GDP, growing by between 2.4x-3.9x its share compared with 2013.



Figure 2: Four scenarios on the future number of consumer fraud victims over the next five years

Number of victims of fraud
In millions, 2013-2027



2013-19

+50%
in the number
of victims

7.3%
of total population
in 2019

2020-22

Up to
+84%
in the number
of victims

Up to
13.2%
of total population
in 2022

2023-27

Up to
+83%
in the number
of victims

Up to
23.6%
of total population
in 2027

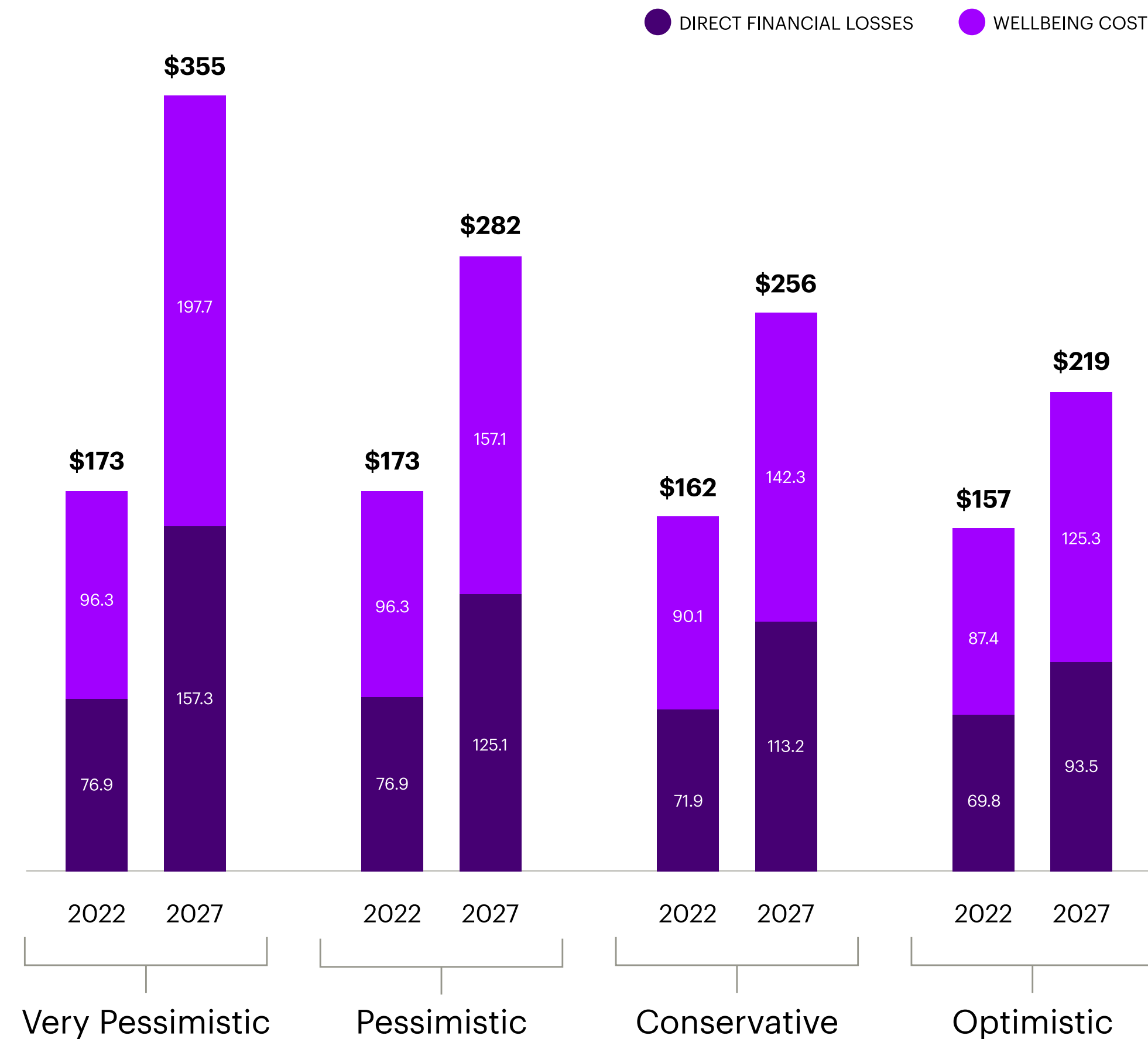
Well-being costs likely to rise too

Typically, it's financial losses that come to mind when we think of consumer fraud. However, victims of fraud also often experience significant negative effects on their emotional wellbeing. A 2020 survey by the European Commission, for example, found that nearly 80% of victims report experiencing some form of emotional harm.¹⁶

Leveraging research from UK Consumer group 'Which?', our analysis shows that wellbeing costs to victims across the eight countries in scope are just as significant as direct financial losses. Indeed, we estimate that wellbeing costs represented US\$79B in 2021 and calculate that these will rise alongside the growth of fraud to US\$125B-\$198B by 2027 (see Appendix 1). At a broader level, we anticipate direct financial losses together with wellbeing costs to reach between \$219M-\$355M within the next five years (Figure 3).

Figure 3: Four scenarios for future direct financial losses and wellbeing costs to victims of fraud in select countries

In US\$ billion, 2022 vs 2027



Barriers to change



To contend with the continuous rise of consumer fraud and its growing sophistication, public safety agencies are developing and adopting new processes, tactics, technologies and ways of operating that combat the growing and evolving threat—especially in the digital world. However, major barriers to change persist. We identify four pillars that must guide the evolution of approaches and processes. The next page highlights specific challenges across each of these.

Four pillars that hold both challenge and opportunity:

Partners: Ecosystem partners include other public safety and government agencies at the local, state and international level as well as private sector companies, such as financial institutions, telecommunications companies

and technology companies (e.g. Meta, Google, Twitter, etc.) and third-sector organizations.

Citizens: Engagement of citizens both from the perspective of informing and educating the public to reduce the likelihood of them becoming victims, as well as supporting and reassuring victims and helping them to feel safe and educated.

Workforce: The way in which public safety officers and staff are recruited, retained, trained and supported to best fight consumer fraud.

Technology: How digital capabilities and new emerging technologies can be best leveraged to address consumer fraud.



Barriers to advancing the fight against consumer fraud



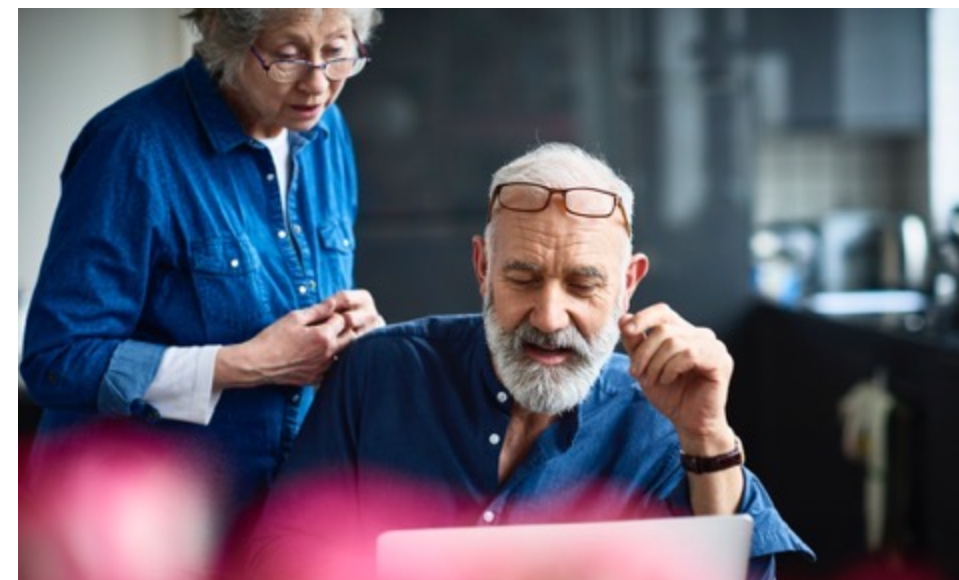
Partners

Operating Models: Models largely pre-date cross-border and high-volume/low-cost consumer fraud

Communications Framework:

Communications are largely based on existing relationships rather than formalized local and international contact points

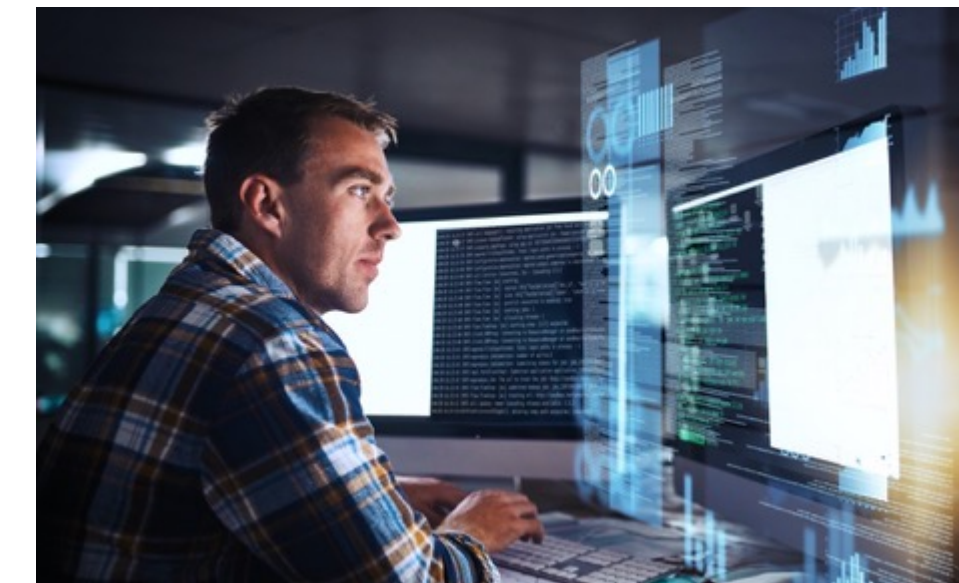
Alignment of Priorities: Organizational incentives and priorities do not lend themselves to a collaborative response by partners



Citizens

Citizen Outreach: Education and awareness programs are often conducted separately from partners and are hampered by capacity constraints

Public Trust: Challenges to respond to victims in a timely manner or progress cases from report to justice outcomes can result in an erosion of public trust



Workforce

Capacity: Capacity constraints inhibit dealing with high volumes of fraud and increasingly complex cross-border incidents

Culture: Cultural mindsets impede sharing fraud data and preclude recognition of fraud as an increasingly important crime type

Skills Gaps: Skill deficits—especially across local and state field offices—persist when it comes to financial crime analysis, intelligence gathering and cyber skills



Technology

Legacy Technology: Systems require a high level of manual processing, are not interoperable with those of other law enforcement or partner organizations, and lack capabilities for strong analytics

Data Quality: Sub-optimal data quality or sub-optimal capabilities to share data strategically or at scale (often heavily influenced by legislation and organizational policies)

Actions for public safety agencies

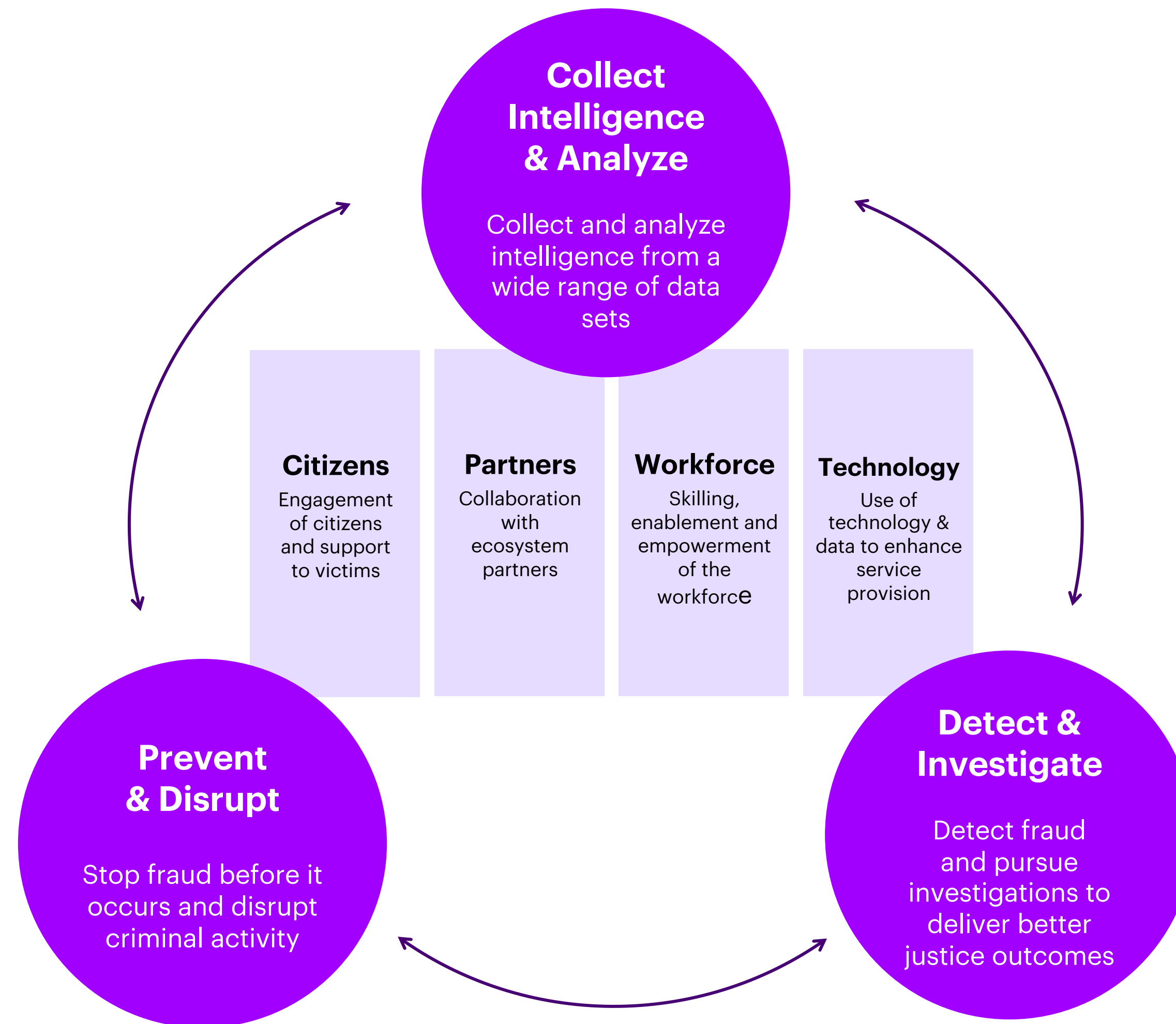


Actions for public safety agencies

While there are clear actions that public safety agencies can begin to take today to combat consumer fraud, there are unfortunately no one-size-fits-all solutions. The reason? Different agencies are at different levels of maturity owing to their level of oversight (local vs. national), their operating model (federated vs. centralized), the depth and breadth of partnerships, the nature of their technology capabilities and the policies within their jurisdiction.

However, there is the potential for a range of activities to fight consumer fraud. For each of our four pillars, we outline potential solutions for public safety agencies to take across three areas of operational response: collect intelligence and analyze, prevent and disrupt, and detect and investigate.

A framework for evolving the prevention and detection of fraud



01

Collect intelligence and analyze:

Building the intelligence picture

Maximizing the intelligence available to understand and help identify and predict patterns of consumer fraud is critical. Additionally, as the volume and impact of consumer fraud grows, meeting the challenge of collecting and analyzing ever-larger volumes of data to disrupt and detect fraud will remain a key to success.

Citizens: Help the public report fraud through their channel of choice, assess vulnerability, and provide advice to reduce harm and protect victims from repeat victimization at the earliest opportunity. For leading agencies, the public should be able to report fraud only once, through a single point of contact which reaches both public safety agencies and relevant partner organizations, such as any relevant financial institutions or victim support organizations.

Partners: Pursue more connected models for intelligence gathering at a national and international level to improve understanding of the threat landscape—both with other public safety institutions and with private sector organizations. As criminals will always exploit the weakest links, it is critical for multilateral organizations, such as Interpol, to provide intelligence and support capabilities to members whose abilities to detect fraud offences are limited. Once the foundations have been built, agencies should have a framework in place to both share and receive intelligence between partners within the parameters of government legislation.

Workforce: Utilize automation and advanced analytics to reduce the burden of repetitive, high-volume, administrative tasks. This will enable staff to analyze large

volumes of data using a range of visualizations, improving employee experience and increasing engagement. Provide enhanced digital tools and creative training approaches and resources, such as open-source training platforms, to help upskill. Recognize and reward workers for building skills and acquiring accreditations.

In the Netherlands, the National Internet Fraud Reporting Portal (LMIO) employs a digital reporting form where which victims can easily report consumer fraud incidents online. Victims are actively informed by the LMIO about their reports and follow-up. LMIO is a public private partnership. Over the years, the reporting portal has gone through several iterations. For example, a smart decision-aid based on AI has been added so that reports that do not involve a criminal offence are filtered out. In cases of no criminal offence, civilians are referred to other parties for help. Data of the reports are used for analysis and intelligence purposes as well as for criminal detection and prosecution.

“I think we’ve gone too far to one side with regards to data Protection... [there needs to be] a change in internal policies. It needs somebody with courage in organizations not to be afraid of the consequences to be able to do things for the greater good. We’re all overly cautious [in sharing data] and to our detriment.”

*–Criminal Intelligence Officer,
Interpol*

Technology: Apply new and emerging technologies to advance intelligence and analysis—including interoperability of platforms—that can inform both the tactical and strategic intelligence picture. The use of AI and advanced analytics, enabled by the power and flexibility of the cloud, will help agencies keep up with threats across all parts of the digital world, including the dark web. These

capabilities should ideally link reports and match entities across databases and organizations to inform the development of high-quality intelligence packages.

Investments in intelligence platforms should be made on the basis that they can be evolved over time to keep pace with the changing threat landscape.

Europol, together with Eurojust and the European Banking Association, recently completed its seventh operation of the European Money Mule Action (EMMA). Established in 2016, it is the largest international operation of its kind, with approximately 400 banks and financial institutions engaged. By sharing intelligence on potential money mules, law enforcement can develop intelligence insights and then decide on what action to take. Europol supports these activities by connecting law enforcement and private sector partners and facilitating information exchange between them. In the operational phase, Europol provides analytical support that connects transnational cases with the money-muling networks behind them. The results last year included the identification of 18,000 money mules, arrests of 1,800 individuals, and preventing total losses estimated at nearly €70M.¹⁷





The National Cyber-Forensics Training Alliance (NCFTA)

The NCFTA was established in 2002 to bring private sector organizations, government and academia together to mitigate and disrupt cybercrime. As cyber-enabled fraud has grown over recent years, the organization has gained increasing importance in helping to combat consumer fraud. By sharing data, learning collaboratively from its members, and pursuing outcome-driven intelligence, the Alliance has prevented over US\$2B in losses while also identifying critical threats to private sector industries. The organization enables field agents and other law enforcement investigators to co-locate with analysts and risk managers from banks and other private sector companies to identify cyberthreats and work on cases together. Teaming up off-site in non-government buildings makes it easier for employees to share information without worrying about classification levels or national-security clearances—an approach that law enforcement attributes to being key to uncovering large schemes and cracking big cases.^{18,19}

02

Prevent and disrupt:

Stopping consumer fraud before it happens

The complexity, speed and often global nature of consumer fraud means that an even greater degree of effort and focus should be placed on prevention and disruption.

Citizens: Develop a coordinated approach to campaigns and online training with partners to educate the public about fraud risks, scam tactics and emerging trends. As the majority of consumer fraud today is enabled through technology, developing more campaigns online and on mobile could bolster prevention efforts that are viewed by wider audiences. Select education and awareness campaigns should also be tailored to citizens who are at increased risk for being victims of specific scams. To continuously improve education and awareness, law enforcement should take a data-driven approach to track and monitor the effectiveness of their prevention activities. They should also conduct

research to increase understanding of the types of citizen engagement activities that have the strongest preventative impact.

Partners: Coordinate efforts between partners using creative models to fund joint activity and incentivize parties to share data. For example, partners could re-examine internal policies to allow for greater sharing of data within legislative limits. Public safety agencies can identify ways to enhance their value proposition to private sector partners so that all sides recognize benefits to data sharing. Creating new roles and functions within public safety agencies which are designed to explicitly forge relationships and work with social media, telecommunications and financial institutions is also key to preventing and disrupting fraud. A strong model can be seen with the FBI's Internet Crime Complaint Center (IC3). In 2018, the IC3 created a Recovery Asset Team to streamline

communications with financial institutions and FBI field offices in order to stop fraudulent transactions faster. Instead of relying on makeshift relationships across organizations, IC3's formalized channels of communication paid off—within one year, the team successfully recovered more than US\$300M for victims.²⁰

“We believe prevention is always a core pillar of policing, but we really believe fraud is the one [area] where you can have the most gains if people can educate themselves and have [greater] awareness”

–Director General of Anti-Fraud Center, National Police Service, Canada

The Canadian Anti-Fraud Centre (CAFC), which is a joint partnership of the Royal Canadian Mounted Police (RCMP), the Ontario Provincial Police and Canada's Competition Bureau provides a strong example of how education programs can be tailored to specific victim groups. Understanding that stories from peer groups often resonate more strongly with individuals, they established a Senior support unit, in which senior citizen volunteers receive basic training from the CAFC in order to conduct education sessions about consumer fraud with seniors in the community via retirement associations and across senior residences. Fraud types, such as romance scams, which have higher prevalence rates among seniors than others, are often a main focus for these education campaigns.

Workforce: Work with partners and international law enforcement agencies to upskill and build capacity. For example, embedding police officers in private sector organizations to work side-by-side with partners can help to advance prevention and disruption activities that benefit both parties. Additionally, taking full advantage of services offered by organizations such as Interpol and Europol to train local public safety officials can help to advance fraud disruption and build critical relationships internationally.

Technology: Provide digital tools to empower citizens to prevent themselves from falling victim to fraud. Additionally, enhance automation and interoperability of technology systems to freeze accounts at the point of report receipt to prevent financial losses to victims. Finally, for public safety agencies further along the maturity scale, use advanced AI and analytics to identify fraudsters trolling social media platforms and disrupt the recruitment of money mules on those platforms.

In the Netherlands, citizens and companies can monitor the safety of their intended online purchases by conducting a simple background check of a vendor or individual on the country's police website, <https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html>. By entering data such as the individual's telephone number, URL of their website, e-mail address or bank account number of the selling party, they can verify if the individual is known to police. This check function has been highly successful in preventing fraud, as evidenced by more than 160,000 monthly checks, with approximate 6% of queries involving potential fraudsters.





Credit Industry Fraud Avoidance System (CIFAS)

CIFAS is a not-for-profit fraud prevention organization based in the UK. Close to 600 member organizations—including 27 local police authorities—from across sectors share their fraud risk data and intelligence through CIFAS' databases—the largest database of fraud incidents in the country. In 2020, CIFAS members prevented fraud totaling £1.4B, providing members with an average return of £169 for every £1 spent on membership.

In addition to supporting the private sector, CIFAS is also deeply engaged with the public sector. Last year, they extended support to local authorities by allowing them to conduct fraud checks for grant applications against CIFAS' National Fraud Database. Local authorities completed over 67,000 searches, resulting in 411 matches—with 62% of these relating to identity fraud.²¹

03

Detect and investigate:

Detect fraud and pursue investigations to deliver better justice outcomes

While often complex and time consuming, the detection, investigation and prosecution of fraudsters is imperative to deter them and build public confidence, by showing that consumer fraud is a crime which has consequences.

Citizens: Use victims' preferred channels to communicate with them throughout the investigation, not only giving them updates about how their case is progressing and the outcomes that have been achieved, but also reassuring them and educating them so that they feel safe and secure.

Partners: Conduct connected policing investigations to maximize available collective resources and to effectively coordinate cross-border investigations. Maximize use of memberships with international organizations, such as Europol and Interpol, as well as relationships with private sector partners through joint apprenticeships and work-exchange programs. Additionally, explore alternative settlement options to create greater accountability and improved outcomes for victims.

Workforce: Provide continuous skilling opportunities in fraud investigations to attract and maintain talent, while also improving investigation quality and delivering better justice outcomes. Separately, consider the engagement of civilians through different types of employment models to augment police resources for specialist capabilities and to support investigations.

Technology: Employ advanced AI and machine learning technologies to automate case prioritization and triage, as well as to identify viable lines of inquiry to improve the quality and speed of investigations. Use common data models, cloud and APIs to enable interoperability across systems, effectively connect investigations and facilitate rapid sharing of insights and developments with partners.

"I think [agencies and partners] needs to have a good understanding of the information-sharing legislation...and the mindset has to move from protecting information to actually utilizing that information for the benefit of law enforcement where appropriate...it requires a bit of courage to make the decision to actually facilitate important information sharing

–Head, District Financial Crimes Unit, New Zealand

This year, Interpol conducted an operation to tackle cyber-enabled financial crime. The first such initiative from Interpol to be truly global in scope, it included specialized police units from 20 member countries, touching every continent. Codenamed HAECHI-II, its purpose was to target specific types of online fraud, such as romance scams, investment fraud and money laundering associated with illegal online gambling. It resulted in the arrests of more than 1,000 individuals and intercepted almost US\$27M of illicit funds. It also helped investigators to close over 1,600 cases and blocked over 2,000 bank accounts linked to online financial crime. A new global stop-payment mechanism—the Anti-Money Laundering Rapid Response Protocol (ARRP)—proved critical to successfully intercepting the illicit funds. Interpol's Secretary General, Jürgen Stock noted that "Only through this level of global cooperation and coordination can national law enforcement effectively tackle what is a parallel cybercrime pandemic."^{22,23}



Singapore's Anti-Scam Center (ASC)

The Singapore Police Force's Anti-Scam Centre (ASC) was founded in 2019 and is charged with investigating scam-related crimes and disrupting operations to mitigate victims' losses. A resource from Singapore's leading consumer bank provided guidance to ASC's establishment and ensured alignment between police and private sector partners. In its first year, ASC recovered more than S\$21M, equating to ~40% of the total amount scammed in reports that the ASC received.

The organization collaborates with 12 banks in Singapore, along with fintech companies, remittance agencies, telecommunications companies and online marketplaces. Based on these new partnerships, funds tracing, which previously took up to two months, can now be

processed almost immediately. The organization also works to effectively terminate mobile lines used for scams. By conducting screening and sense-making of local mobile numbers used in reported scams, more than 1,500 local mobile lines were terminated from January-June in 2020.²⁴

Reining in future consumer fraud



Consumer fraud presents a fast-growing challenge. The number of victims is increasing all the time, as are the losses and impacts on people's wellbeing. While there have been calls for new legislation to tackle economic crime as a matter of priority, it's clear that legislation alone can't solve this challenge.

There's an urgent need to address consumer fraud holistically and that means working to overcome the current barriers and developing new approaches built around the four pillars of citizens, partners, workforce and technology. Additionally, as consumer fraud is increasingly conducted across borders, ensuring that public safety agencies internationally raise their standards to a level of 'best in class' is critical to combat global consumer fraud collectively.

Crucially too, a challenge of this scope and complexity requires a whole-of-government approach. Responding to consumer fraud cannot be achieved successfully by public safety agencies alone, but rather requires the collaboration of the intelligence and law

enforcement communities as well as support from government leaders. It also requires a whole-ecosystem approach reaching across government to the private sector, and critically to the public themselves.

We urge public safety agencies and their partners to continue to invest in fighting consumer fraud before it becomes an even greater threat to citizens' wallets and wellbeing, to trust in public safety agencies, and ultimately to economic and national security.

"Everyone has a role and everyone has different roles... it requires law enforcement, public and private sector to work towards a common goal... the whole of society will need to stand up to combat it together."

—Temporary Director, National Economic Crime Centre, UK National Crime Agency



Authors



James Slessor

Managing Director – Consulting,
Public Safety Lead
james.w.slessor@accenture.com

James is a Managing Director leading Accenture's Global Public Safety practice, focusing on policing, law enforcement, justice, prisons and rehabilitation and national security. He brings more than 20 years of industry experience to his role helping public safety organizations enhance operational performance, increase efficiency and deliver improved outcomes to the public.

A recognized expert in his field, James has spoken and written extensively in leading industry publications on a range of public safety topics including the use of social media, information management, analytics, digital disruption and most recently the impact of COVID-19.



Sarah Berger

Manager – Accenture Research,
Public Service
sarah.g.berger@accenture.com

Sarah is part of the Accenture Research public service team. Formerly, she held positions as the North American lead for workforce research and was also research manager of the office of Accenture's CEO. In these roles, she has partnered with the G20, Harvard Business School and Amazon on various research projects. Previously, Sarah worked for 10 years as a strategy consultant with a focus on health and public sector organizations, including a position with the United Nations World Food Programme in Italy.



Lily Robinson

Manager – Strategy & Consulting,
Public Service, United Kingdom
lily.robinson@accenture.com

Lily is a Manager in Accenture's Global Public Safety practice, focusing on policing, law enforcement and justice. She is a CIPFA Accredited Counter Fraud Specialist and is passionate about transformation in fraud and economic crime. Lily has advised Accenture's public safety and central government clients on fraud risk management, fraud policy and digital justice. Prior to Accenture, Lily worked at the UK Ministry of Justice and Crown Prosecution Service.

Special acknowledgements

Accenture Contributors

David Armond (United Kingdom)

Nicholas Cheng Kiat Chua
(Singapore)

Pierre Dupont (Canada)

Tim Godwin (United Kingdom)

Darren Harrison (United Kingdom)

Peter Henschel (Canada)

Howard Marshall (United States)

Keiran Miller (Australia)

Jacqueline Morley (United Kingdom)

Helen Short (United Kingdom)

Morna Spence (United Kingdom)

Emily Sutton (United Kingdom)

Ezequiel Tacsir (Argentina)

Jody Weis (United States)

External Contributors

We would like to thank the following business leaders, experts and practitioners for their insights:

Matthew Craft, Detective Superintendent, Commander Cybercrime
Squad New South Wales, Australia

Chris Lynam, Director General, National Cybercrime Coordination
Unit and Canadian Anti-Fraud Centre, Royal Canadian Mounted
Police, Canada

Guy Paul Larocque, Sergeant/Acting Officer in Charge, Canadian
Anti-Fraud Centre, Royal Canadian Mounted Police, Canada

Mike Creedon, Former Chief Constable, Derbyshire, United Kingdom

Chris Allan, Head, Financial Crime Unit, Auckland City District Police,
New Zealand

Mark Cheeseman, Director of Government Counter Fraud Function
and Chief Operating Officer for Fraud, Errors, Debt, and Grants, UK
Cabinet Office, United Kingdom

Ian Pemberton, Coordinator for Anti-Money Laundering and Asset
Recovery at the INTERPOL Financial Crime & Anti-Corruption
Centre, France

Eric Shiffman, Assistant Special Agent in Charge, Federal Bureau
of Investigation, United States

Brian Swain, Special Agent In Charge, U.S. Secret Service,
United States

Matthew Long, Temporary Director National Economic Crime
Centre, National Crime Agency, United Kingdom

Sandra Peaston, Director of Research & Development, Cifas,
United Kingdom

Peter Hagenaaars, Renewer in combatting digital crime on behalf
of the Dutch National Police; Owner of Top Management
Consult, The Netherlands

Burkhard Muehl, Head of Department, European Financial &
Economic Crime Centre, Europol, The Netherlands

Sebastian Bley, Head of Economic Crime Team, Europol, The
Netherlands

About

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com

Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

Copyright ©2022 Accenture. All rights reserved. Accenture and its logo are registered trademarks of Accenture.

This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.

About Accenture Research

Accenture Research shapes trends and creates data-driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients’ industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients.

Appendix



We developed four different scenarios to forecast the future evolution of fraud. These scenarios are based on extrapolating past trends and applying different rates of growth based on reported incidents of consumer fraud across eight geographies. Since fraud is heavily underreported, we estimated a measure of total incidents based on fraud reported in national crime surveys and applied a rate of growth of reported incidents to law enforcement. These numbers were re-scaled from adult populations to total population numbers to obtain an incidence rate of consumer fraud for the total population across countries in scope.

In the first three scenarios, we assumed that there were no changes in terms of prevention capabilities or in terms of the financial loss trends. The fourth scenario includes an assumption that the prevention rates of fraud return to pre-pandemic

levels., with average financial losses and wellbeing costs also reverting to pre-pandemic rates.

The four scenarios we outline are categorized as follows:

1. Very pessimistic. “Fraud is part of the new normal:”

2022 fraud rates will grow as they did in 2021 and, from 2023 onwards, they will grow at the same CAGR observed from 2013-20.

2. Pessimistic. “After a 2022 with pandemic effects, fraud gets back to pre-pandemic rates:”

2022 consumer fraud rates will grow at the same rate as in 2021, but from 2023 onwards they will grow as it did pre- pandemic.

3. Conservative. “Fraud get back to pre-pandemic rates:”

2022 exhibits a slower

rate of growth, converging to pre-pandemic rates from 2023 onwards.

4. Optimistic. “After the pandemic, prevention efforts curb the growth in affected people and those who suffer financial losses:”

With growth rates similar to pre-pandemic levels, prevention rates cause the number of victims and subsequent financial losses and wellbeing costs to slowly return to rates observed pre-pandemic.

Using national surveys that show the proportion of victims by band of losses, we use the implied mean loss for victims in each band. Based on these estimates and based on the information and forecasts of price indices and exchange rates, we obtain a measure for the direct financial losses for each country for each year.²⁵

Our scenarios also include quantifying the wellbeing costs of being a victim of fraud. UK Consumer organization, which estimated that the costs of the emotional trauma linked to fraud are equivalent to £2,500 (US\$3,300), based on change in life satisfaction reported by victims of fraud, with the monetary cost then calculated using central values approved by the UK Government's HM Treasury. We adapted their conservative estimate, equivalent to £786 (US\$1,050)/victim. Estimates are

extrapolated to the other countries based on their respective per capita income. For both wellbeing costs and direct financial losses, we use the information and forecasts of price indices and exchange rates to obtain a measure in current US dollars.^{26,27,28} A detailed view of each of the four scenarios can be viewed below:

Further details of the four scenarios can be viewed on the following pages.

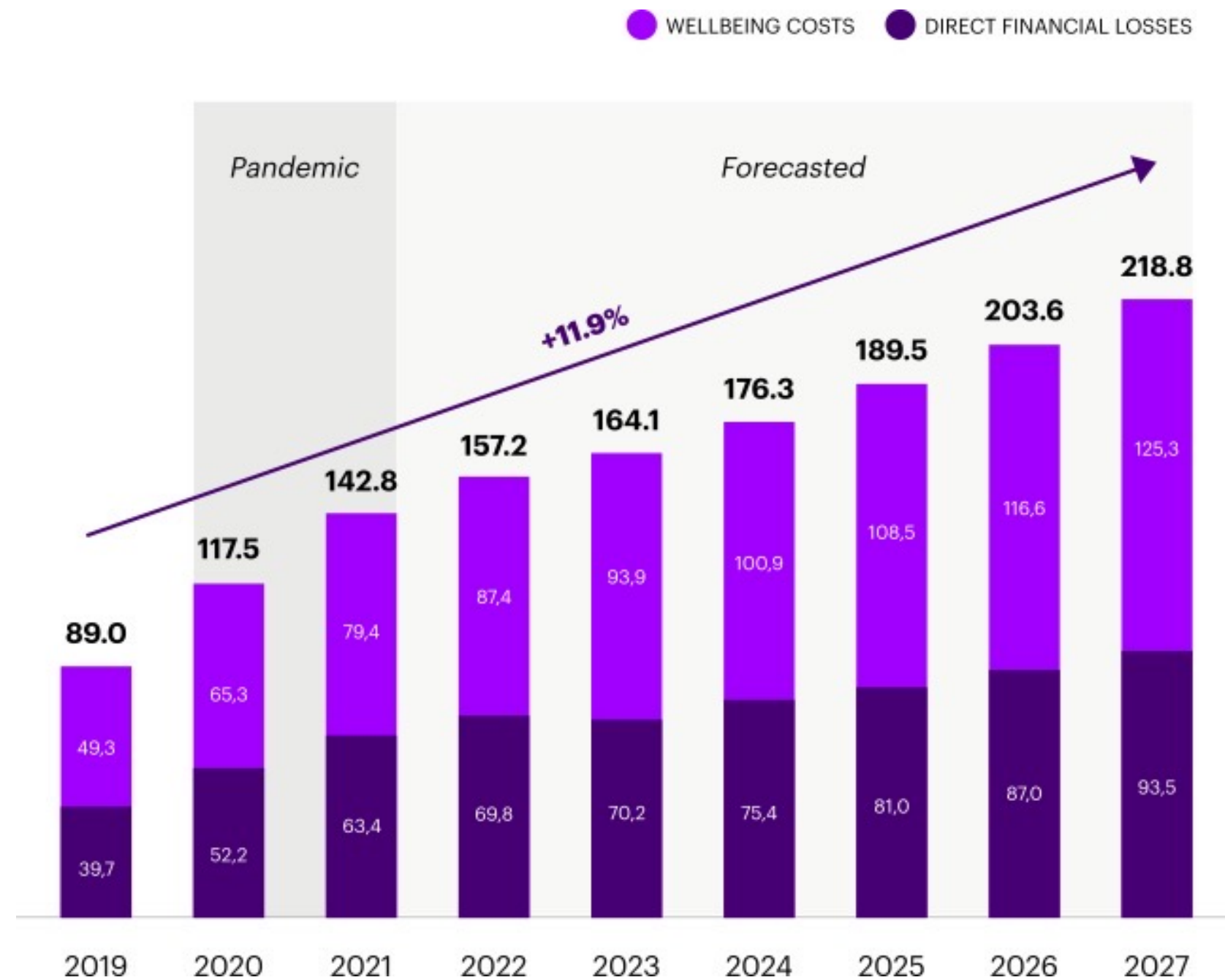
	2013-19	2020-22	2023-27			
Victims CAGR	6.8%	22.5%	Very pessimistic 12.9%	Pessimistic 7.9%	Conservative 7.2%	Optimistic 7.1%

Based on estimates for the US, UK, France, Germany, Italy, Canada, Australia, and Singapore.

A detailed view of each of our four scenarios (1/2)

“Optimistic” scenario: fraud costs US \$219b by 2027 or 0.41% of GDP

Direct financial losses and wellbeing costs in selected countries
In US \$ billion, 2019-2027



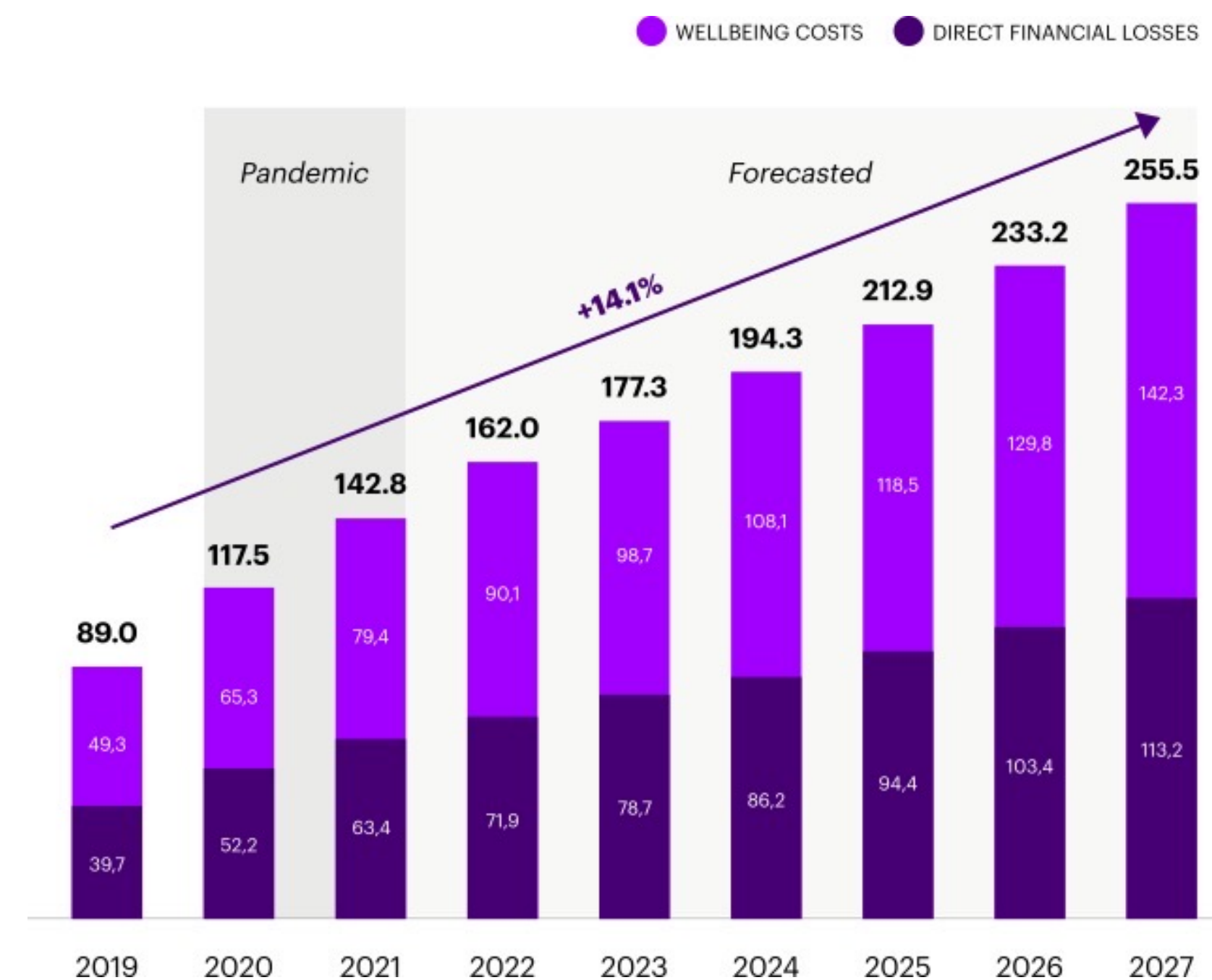
2.4X
in terms of GDP in between 2013 and 2027

16.6%
of total population affected by fraud in 2027

10.8%
of total population will suffer a financial loss due to fraud by 2027

“Conservative” scenario: fraud costs US \$256b by 2027 or 0.48% of GDP

Direct financial losses and wellbeing costs in selected countries
In US \$ billion, 2019-2027



2.8X
in terms of GDP in between 2013 and 2027

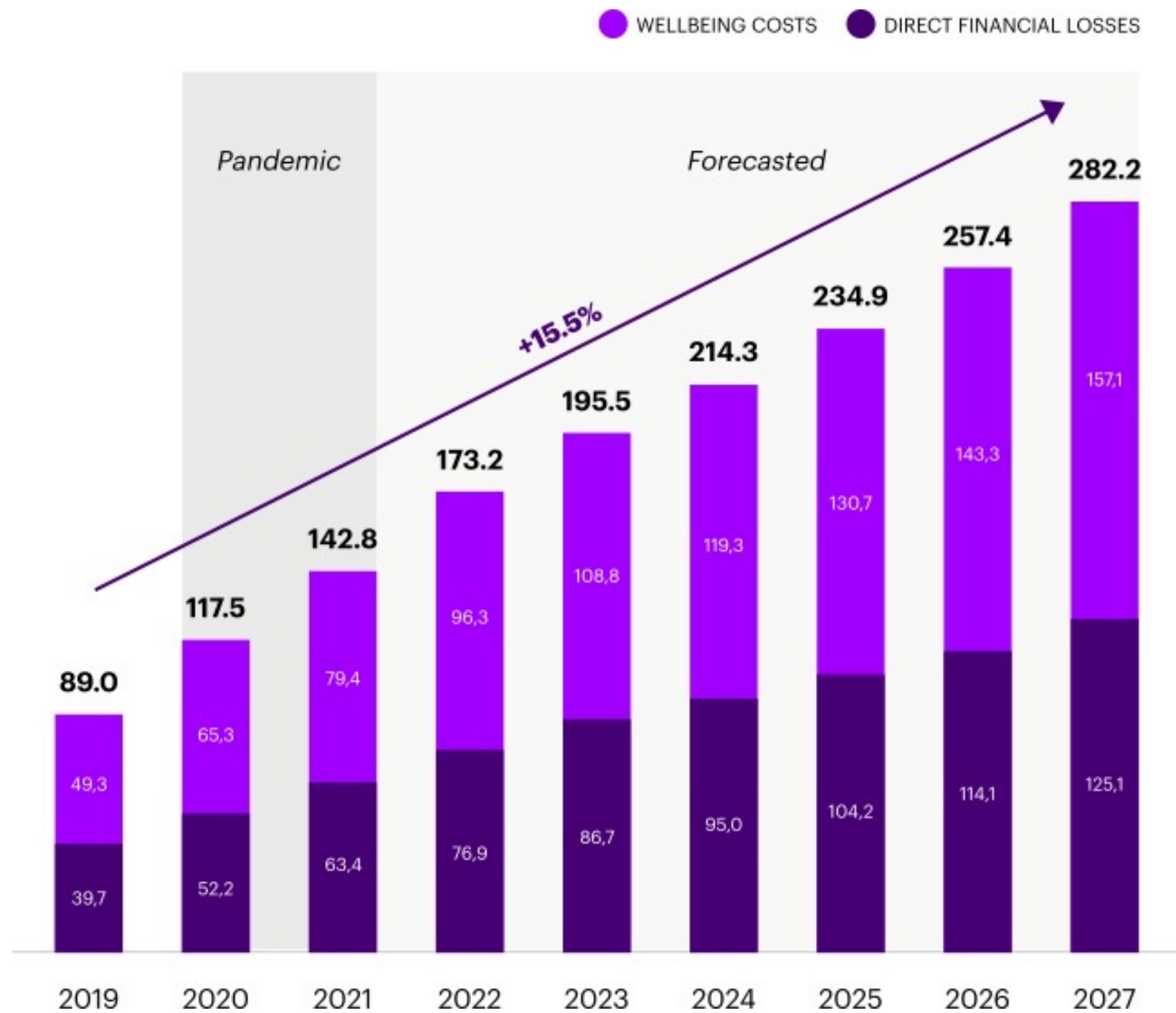
17.1%
of total population affected by fraud in 2027

12.1%
of total population will suffer a financial loss due to fraud by 2027

A detailed view of each of our four scenarios (2/2)

“Pessimistic” scenario: fraud costs US \$282b by 2027 or 0.54% of GDP

Direct financial losses and wellbeing costs in selected countries
In US \$ billion, 2019-2027



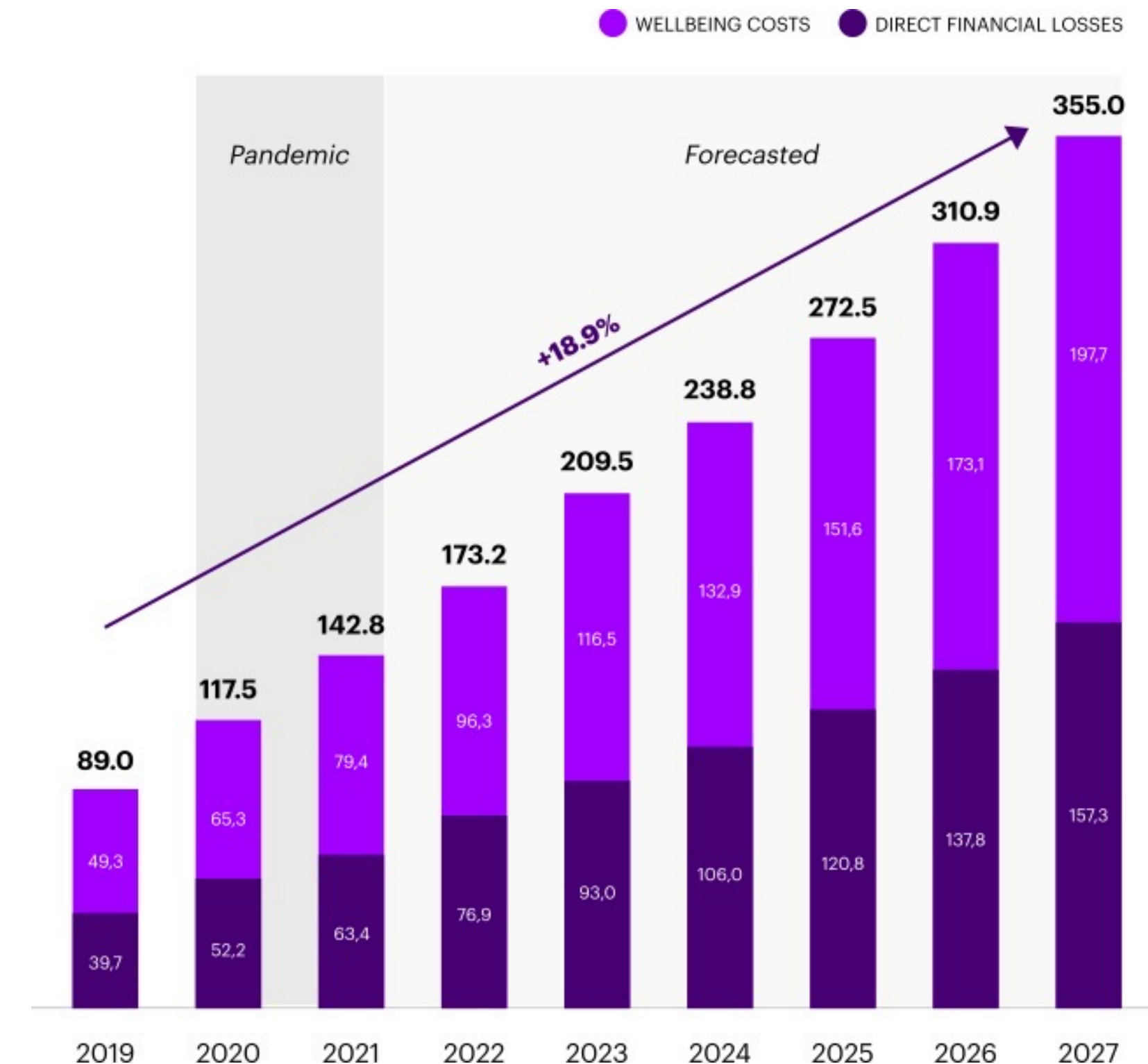
3.1X
in terms of GDP in between 2013 and 2027

18.8%
of total population affected by fraud in 2027

13.3%
of total population will suffer a financial loss due to fraud by 2027

“Very pessimistic” scenario: fraud costs US \$355b by 2027 or 0.66% of GDP

Direct financial losses and wellbeing costs in selected countries
In US \$ billion, 2019-2027



3.9X
in terms of GDP in between 2013 and 2027

23.6%
of total population affected by fraud in 2027

16.7%
of total population will suffer a financial loss due to fraud by 2027

References

- 1 Fraudscape, CIFAS, 2019. <https://www.cifas.org.uk/insight/reports-trends/fraudscape-2019>
- 2 Internet Crime Report, FBI, 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- 3 Fraud Reports, Federal Trade Commission, 2021. <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>
- 4 Half Year Fraud Update, UK Finance, 2021. <https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf>
- 5 EU Policy Cycle – EMPACT, Europol, 2022. <https://www.europol.europa.eu/crime-areas-and-statistics/empact>
- 6 ‘Organized crime knows fraud is the way to go’: former RCMP financial crime expert, Global News Canada, 2019. <https://globalnews.ca/news/5463766/organized-crime-knows-fraud-is-the-way-to-go-former-rcmp-financial-crime-expert/>
- 7 The Silent Threat - The Impact of Fraud on UK National Security, Royal United Services Institute, 2021. https://static.rusi.org/the_silent_threat_web_version.pdf
- 8 Note: The range is dependent on location and the definition of attempts of fraud used in those locations
- 9 2019 Annual Fraud Study, CPA Canada, 2019. <https://www.cpacanada.ca/en/news/canada/2019-03-07-cpa-canada-fraud-survey>
- 10 2014-15 Personal Fraud Statistics, Australian Bureau of Statistics, 2015. <https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release>
- 11 National Prevalence of Survey Scams, Behavioural Sciences Collective, 2020. <https://bscresearch.com.sg/wp-content/uploads/2021/02/Scams-Infographics-HTSBC.pdf>
- 12 Survey on ‘Scams and Fraud Experienced by Consumers’, European Commission, 2020. https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf
- 13 The Silent Threat - The Impact of Fraud on UK National Security, Royal United Services Institute, 2021. https://static.rusi.org/the_silent_threat_web_version.pdf
- 14 The Economic and Social Costs of Crime, Home Office, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954485/the-economic-and-social-costs-of-crime-horr99.pdf
- 15 Note: Historically, reports of fraud to public safety agencies have been relatively low. Yet as the volume of fraud has risen, so have the number of victim reports. Our modeling of future scenarios takes the annual growth of victim reports to law enforcement and applies this factor to data from national crime surveys. We believe this approach provides a truer picture of consumer fraud’s prevalence.
- 16 Survey on ‘Scams and Fraud Experienced by Consumers’, European Commission, 2020. https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf
- 17 ‘European Money Mule Action leads to 1803 arrests’, Europol, 2022. <https://www.europol.europa.eu/media-press/newsroom/news/european-money-mule-action-leads-to-1-803-arrests>
- 18 National Cyber-Forensics and Training Alliance, 2022. <https://www.ncfta.net/>
- 19 ‘Private-Public Collaboration Puts Pittsburgh at Fore of Cybercrime Fight’, Wall Street Journal, 2015. <https://www.wsj.com/articles/private-public-collaboration-puts-pittsburgh-at-fore-of-cybercrime-fight-1439508624>
- 20 ‘Internet Crime Complaint Center Marks 20 Years’, FBI, 2020. <https://www.fbi.gov/news/stories/ic3-20th-anniversary-050820>
- 21 CIFAS Annual Report, CIFAS, 2020. <https://www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas%20Annual%20Report%202020-combined%20copy.pdf>
- 22 Wellbeing Guidance for Appraisal: Supplementary Green Book Guidance, July 2021, HM Treasury
- 23 ‘INTERPOL-coordinated global operation HAECHE-II targets cyber-enabled financial crime’, EAST, 2021. <https://www.association-secure-transactions.eu/interpol-operation-haechi-ii-targets-cyber-enabled-financial-crime/>
- 24 ‘Police Anti-Scam Centre Marks First Year of Operation’, Singapore Police Force, 2020. https://www.police.gov.sg/media-room/news/20200730_police-anti-scam-centre-marks-first-year-of-operationalisation
- 25 World Economic Outlook: October 2021 Database, International Monetary Fund, 2021. <https://www.imf.org/en/Publications/WEO/weo-database/2021/October>
- 26 ‘Scams impact on victims’ wellbeing amounts to £9.3bn’, Which?, 2021. <https://www.which.co.uk/news/2021/10/scams-impact-on-victims-costs-9-3-billion-a-year/>
- 27 ‘Newly launched Green Book Supplementary Guidance recommends Simetrica-Jacobs income coefficient to measure life satisfaction’, Simetrica-Jacobs, 2021. <https://simetrica-jacobs.com/newly-launched-green-book-supplementary-guidance-recommends-simetrica-jacobs-income-coefficient-to-measure-life-satisfaction/#:~:text=Last%20week%2C%20HM%20Treasury%20published%20new%20Green%20Book,provides%20the%20step-by-step%20guidance%20to%20implement%20in%20practice>
- 28 ‘Simetrica-Jacobs Contributes to New Guidance on Wellbeing Analysis’, Simetrica-Jacobs, 2021. https://www.jacobs.com/newsroom/news/simetrica-jacobs-contributes-new-guidance-wellbeing-analysis?utm_source=social&utm_medium=twitter&utm_term=02c0acaf-cb62-4790-b117-ec1247c649ae&utm_content=&utm_campaign=newsroom

accenture