People Data Labs

FINTECH'S BIG DATA FUTURE

2022 Survey Results

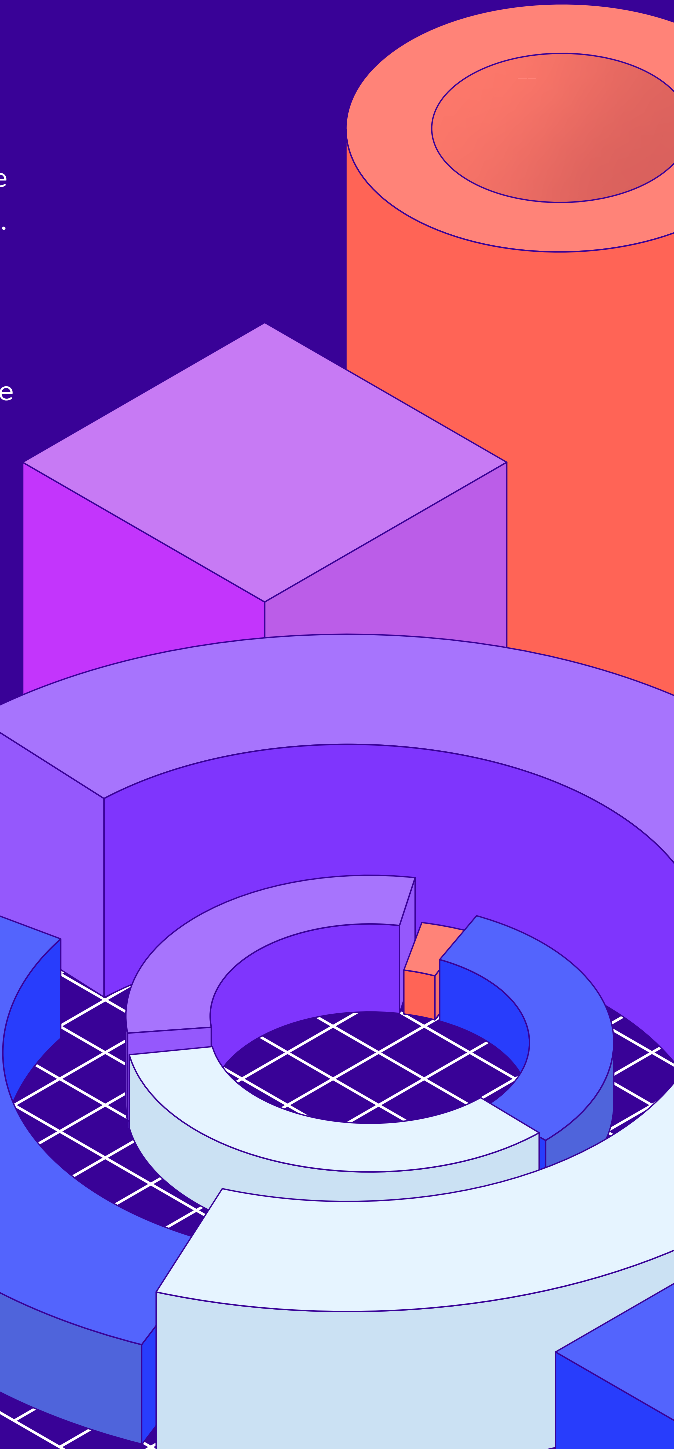
Table of Contents

Introduction

The fintech industry is in a period of unprecedented growth. While first generation fintech products were often built on top of traditional banking infrastructure, designed to serve those banks' customers by bringing their services online, a new generation of fintech aims to deliver new financial services and products directly to digital consumers, often unmediated by traditional banking institutions. This change, already underway by the end of 2019, was accelerated by the COVID-19 pandemic and its resulting lock downs and periods of social isolation. As world events brought more consumers online, they also drove increased demand for end-to-end digital financial services and products.

While the next generation of fintech providers holds great promise for the financial services industry as a whole, the move toward greater reliance on fintechs does present challenges. By moving away from services that are built on existing banking infrastructure, this new wave of fintech's has found itself in need of solutions to various problems, in particular the problem of identity. No longer able to rely on the traditional identity verification alone, fintech's must seek out new sources of data and new approaches to understanding consumer identity fully and efficiently if they wish to continue delivering new services in a timely manner while guarding against undue risk.

To better understand these needs, People Data Labs commissioned a survey of over 150 fintech professionals across small startups, large enterprise fintech businesses, and legacy financial institutions. Our goal was to assess the challenges that fintech providers faced around identity, the data they currently use to address those concerns, and what additional resources they will need to deliver on the full promise of next-generation fintech solutions.



Methodology

To assess the state of the fintech industry it was important to capture a cross-section of fintech professionals representing the breadth of the sector from startups, to established enterprise player, and tech organizations within legacy financial institutions. Our survey captured responses from **156 fintech professionals.** While respondents ranged from companies comprised of fewer than 20 employees to those with over 10,000, the majority hailed from established companies with between **500 and 5,000 employees.**

Fintech is a vast sector that encompasses a number of distinct services and tools from consumer payments to institutional lending and crypto currency. Our sample included representatives from all of these sectors with the majority hailing from established fintech players in the payments, banking, and financial services space while the remainder hailed from emerging sectors like insurance technology, lending, and crypto currency.

Fig.1 How many employees does your company have?

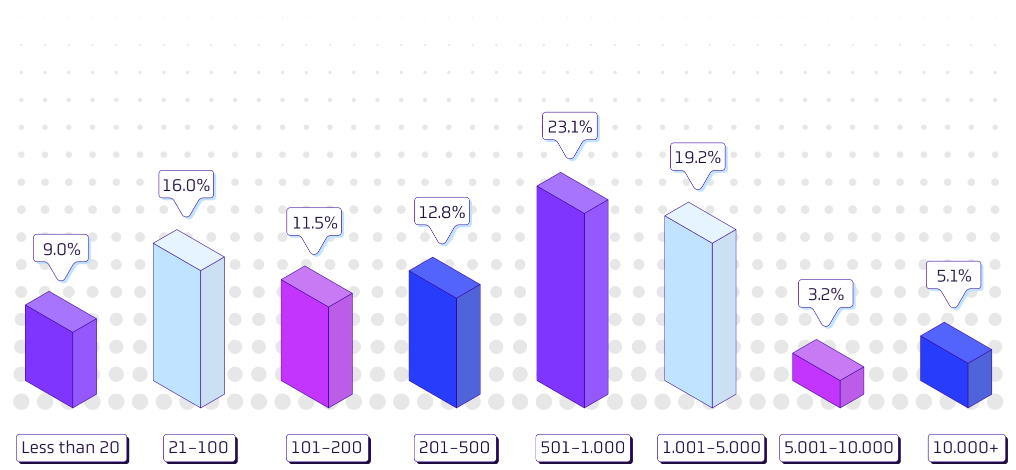
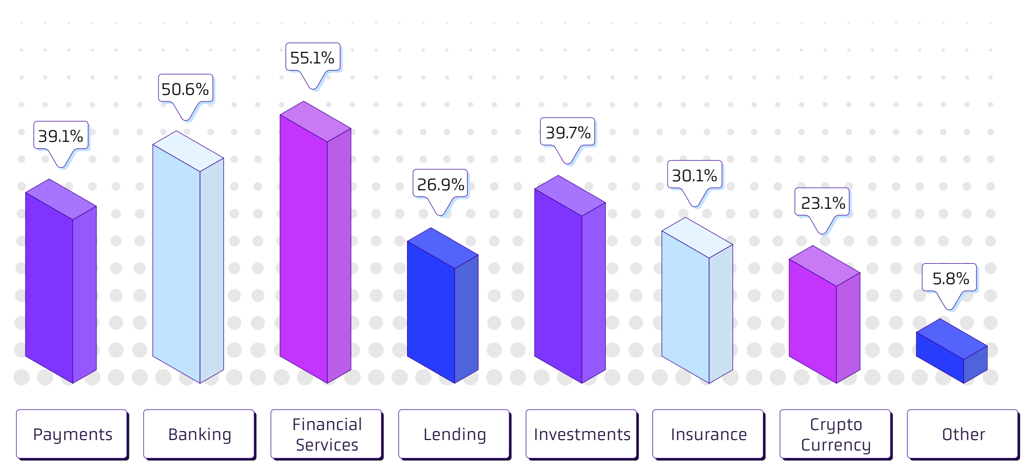


Fig.2 What type of financial services do you provide?



Privacy Challenges

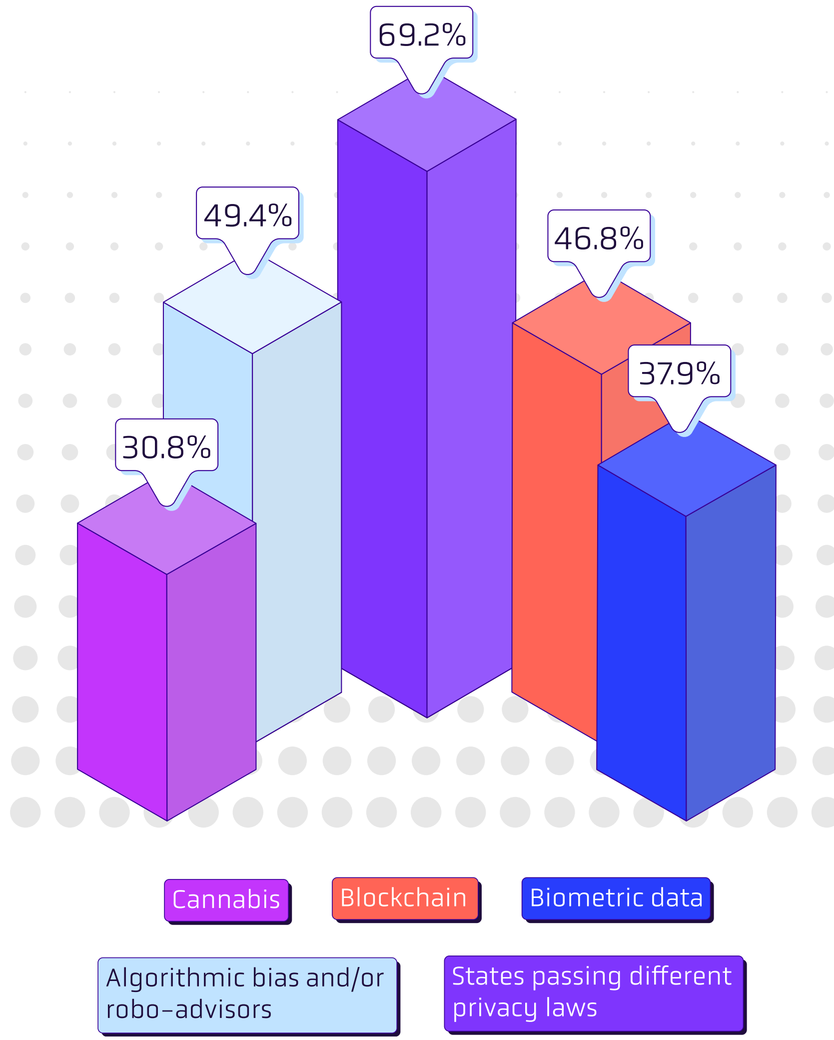
The fintech industry is expanding rapidly as consumers take more and more of their financial lives fully online, however that growth has presented challenges for a still nascent industry. Among these growing pains, a regulatory environment that hasn't fully formed leaving businesses on the leading edge of a new technology to navigate government rules that haven't been fully tested or in some cases even fully written. Respondents ranked their concerns: rules governing emerging block chain technology, legal cannabis, the use of algorithms and AI driven robo-advisors, and the handling of users biometric data.

However, one challenge stands out among the rest. A significant majority of those surveyed, **69.2%, reported that privacy laws passed by different states were their primary concern.** It's a reasonable fear considering the need for fintech providers to handle sensitive customer data, as well as leverage third-party data, in the increasingly uneven landscape of U.S. privacy laws. In absence of national privacy regulations, states have endeavored to set up their own data privacy regimes.

Learn More: For more on the rapidly changing landscape of U.S. privacy regulation, download [The Ultimated Guide to Privacy Compliance]

Fig.3

What emerging privacy or regulatory concerns are you dealing with right now and for the next year?



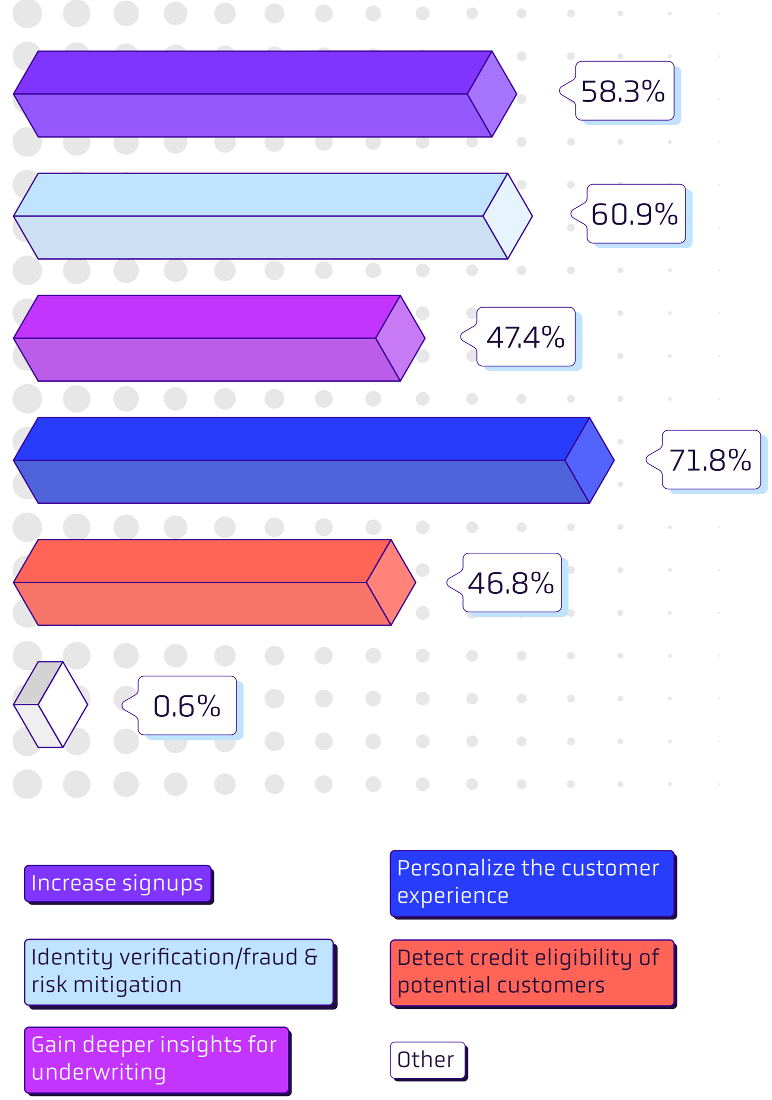
Putting Data to Use

Its only natural for privacy regulation to be top of mind of fintech professionals. Delivering financial products and services digitally requires fintech vendors to handle large amounts of sensitive data both from customers and from third party providers. We asked fintech professionals what purposes their businesses were leveraging data for. While the majority cited personalization and customer experience as a key data use case, over **60% cited identity verification and risk mitigation** as a key driver of their data usage, while **47% pointed to detecting credit eligibility and 47% use data to enhance their underwriting practice** suggesting that understanding identity at a deeper level is essential for fintech.

This makes particular sense when you consider that the next generation of emerging fintech providers will be largely untethered from traditional banks and legacy financial institutions. As a result, these vendors will need to leverage more data to concretely establish the identity of customers who may have never entered a brick-and-mortar banking establishment or performed the type of in-person verification procedures that were a signature of 20th century banking. As a result, fintech will need to rely on 21st century versions of identity grounded in third-party data which provides additional context and dimension.

Fig.4

How is your company utilizing data?

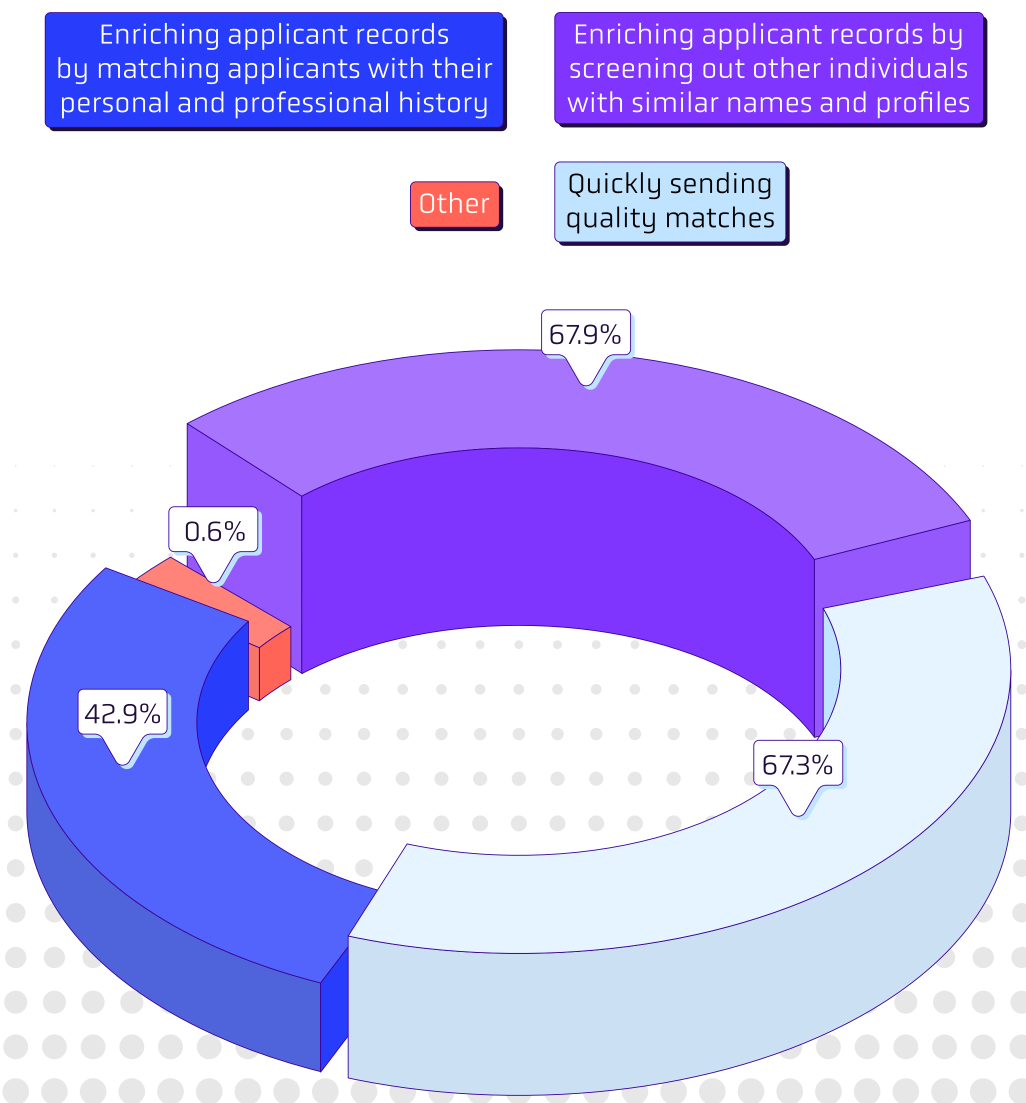


Powering Efficiency

The thread that seemingly connects all of the major fintech data usecases is efficiency. In order to deliver services, fintechs need to be able to verify and understand their customers more quickly than traditional financial institutions. Processing applications quickly and accurately is [critical to achieving wide adoption](). We asked participants to explain how data entered into this process. For the majority, **67.9%, of vendors** the answer was enrichment. By enriching applicant records with additional sources of data, fintech's can quickly understand more about their potential customers. Factoring in the personal and professional history of applicants paints a more complete picture of the customer and their ability to fully leverage a service. This allows vendors to match that applicant with the services that are most appropriate for them based on their income, work history, professional attainment, and biographical details. While enriching records for context was the top priority of most vendors, speed and quality were a close second. **67.3% of all vendors** noted that quickly finding quality matches was critical as they attempted to turn around applications more quickly and avoid consumer delays. Interestingly, while fraud detection and risk mitigation were noted as top priorities for vendors looking to employ data, only **42.9% listed enrichment to screen out individuals with similar names and profiles** as a top priority.

Fig.5

How does using data help your company turnaround applications faster?



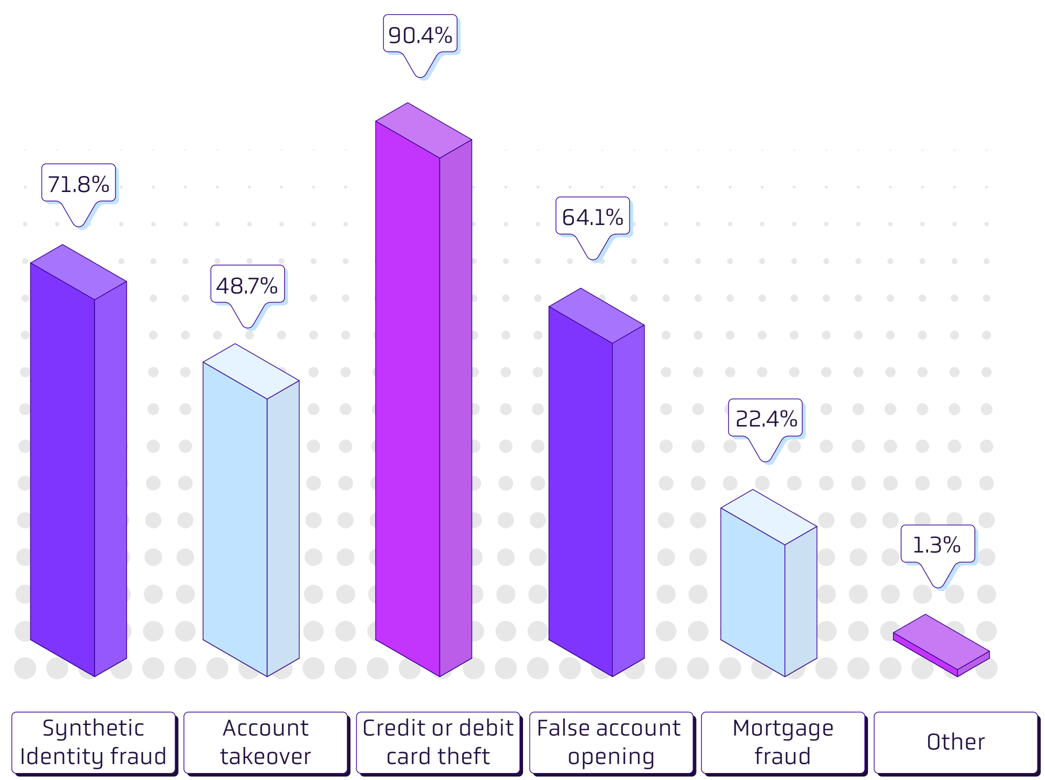
Fighting Financial Crime

The first wave of the fintech industry was built on top of traditional banking, to perform banking functions digitally for bank customers. As a result, first-generation fintechs were able to rely on the infrastructure of traditional banks to verify identities, manage risk, and prevent fraud. Banks, rather than fintech brands had final regulatory responsibility for every transaction. However, the next wave of fintechs are disaggregated from traditional banking structures. They are primarily standalone service providers, offering services like lending, insurance, and credit, and responsible for their own customer due diligence. As a result, their culture around identity verification is less advanced. Our survey found that fintech professionals are acutely aware of this difference, and that fighting financial crime and fraudulent activity is top of mind as they seek out data sources to enhance their diligence and risk mitigation process.

While traditional first party fraud remains a concern for most (90.4% report that credit and debit card theft are prevalent issues) more sophisticated identity fraud remains a major concern. In particular, the use of synthetic identities presents a challenge that vendors are actively looking to solve for. 71.8% of the professionals surveyed noted that synthetic identities are a key concern, due in part to the fact that adequate solutions remain elusive. While traditional tools like credit file data can provide clues to the validity of an applicants identity, these sources are also rife with fraudulent or inaccurate information that can make detecting sophisticated synthetic identities challenging. Bad information that infiltrates these systems can easily proliferate leaving fintech vendors to seek out other sources of data with lower rates for fraud, such as professional and B2B data.

Fig.6

Which financial crimes related to individuals were most prevalent?



Fighting Financial Crime

While individual customer risk is a critical issue for many consumer-facing fintech providers, it's equally important to the fast growing sector of fintechs designed to serve business clients. With typically higher dollar figures at stake and time and efficiency of even greater import, these vendors face an even higher threshold of risk. This challenge is further exacerbated by the rise of entrepreneurship and the gig economy, both of which have given rise to significantly more small businesses and solo proprietorships, often lacking the transparency and accountability of more established firms. Among those surveyed the majority have seen a significant (33.3%) or slight (36.5%) uptick in financial crime related to small and medium sized businesses.

Fig.7

How was the rate of attempted financial crime related to small and medium business changed this year in comparison to last year?

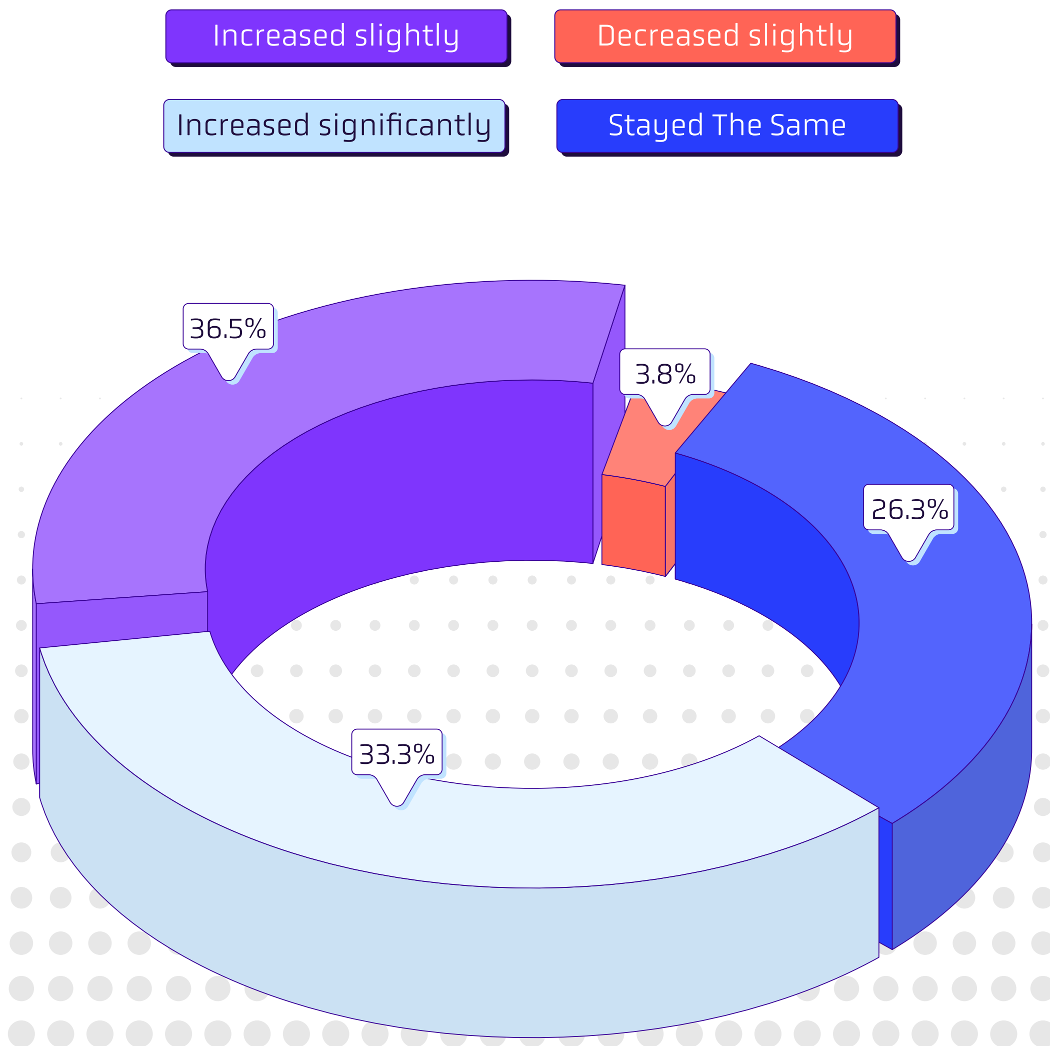


Fig.8 Which financial crimes against SMBs were most prevalent?

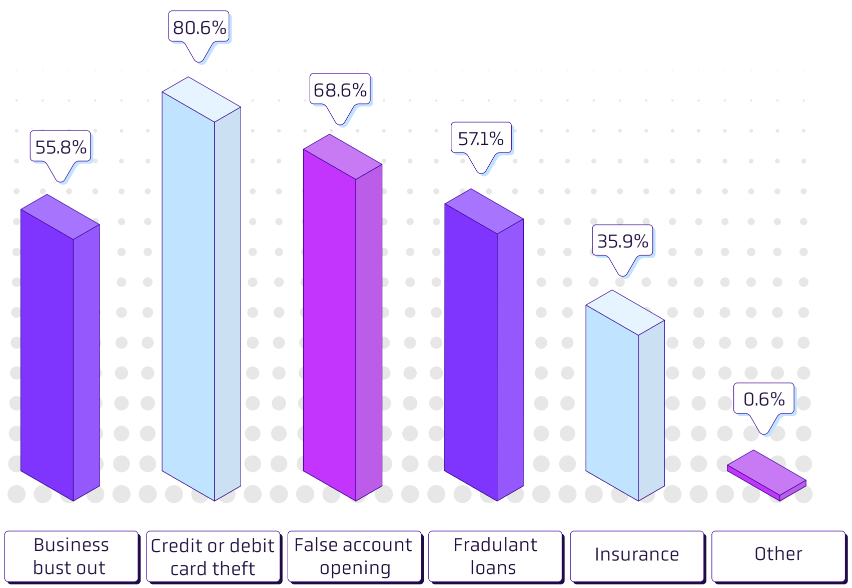


Fig.9 How does data help your company prevent financial crime?