



Protect Your Business:

An Analysis of 2022 Financial Technology Fraud Trends





Table of Contents

Introduction // 1

Fraud Prevention In The Era of Fintech // 2

What's Driving Fintech? // 4

Fintech Trends in 2022 // 6

Regulations in 2022 // 8

Security Risks and Threats // 8

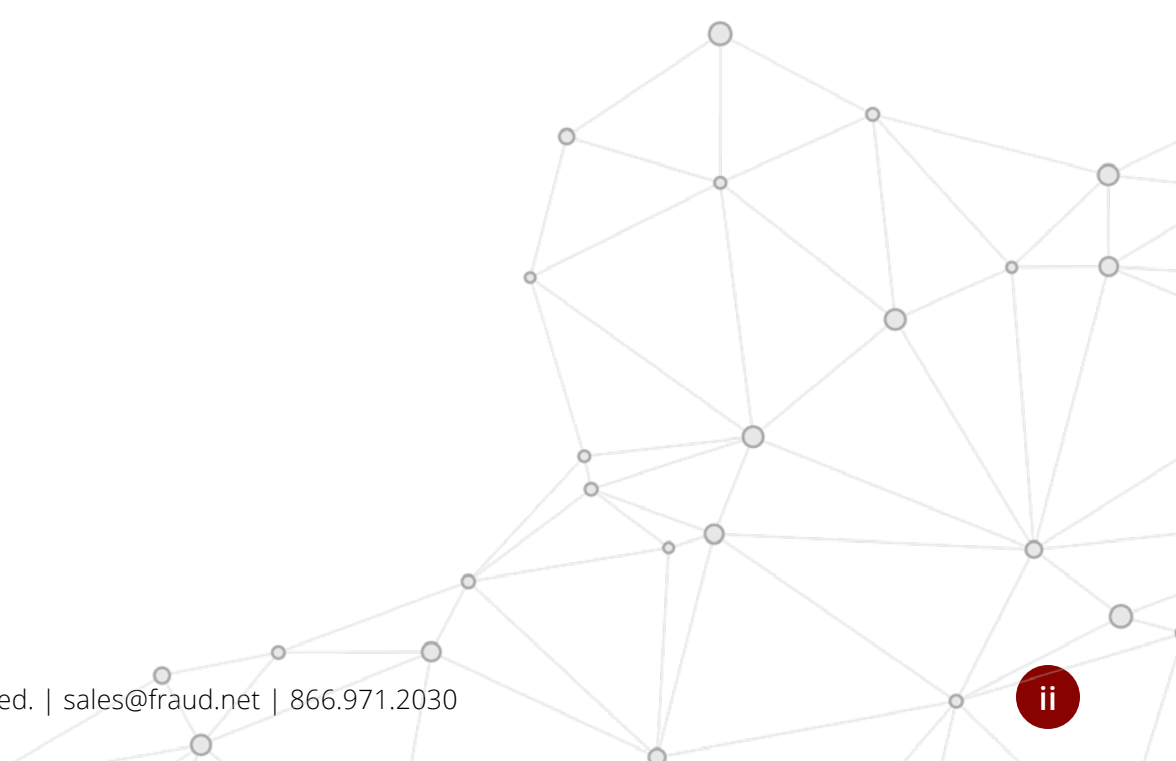
Cost of Online Fraud // 9

The Real-World Impact of Fraud in Fintech // 10

Moving Forward // 11

How Could Companies Prevent Pandemic Fraud? // 11

Conclusion // 14



Introduction: Protecting Your Business in The Changing Landscape of Fintech Fraud



In recent years, the financial technology industry has become a significant global force that impacts nearly every aspect of our digital lives. This unprecedented growth in financial technology has increased opportunities for those looking to exploit our use of convenient digital financial services and online marketplaces.

Of course, fraud prevention for financial technologies is not a new concept by any means. From the first computer virus known as The Brain Boot Sector Virus to the wildly sophisticated fraud tactics of today's day and age, the financial sector has always been a massive target for exploitation.

However, with accelerated changes and updates to financial business operations and technologies, the fraud economy is growing at an unprecedented rate. In this piece, we'll look at some of the major drivers influencing fraud in fintech and the most influential fraud prevention trends keeping businesses safe in 2022.



Fraud Prevention In The Era of Fintech

What is Fintech?

Fintech, or financial technology, encompasses a large industry and touches many different sectors in the global economy. Fintech companies began as disruptors to traditional financial institutions, offering heightened accessibility to banking and financial services, often without visiting a physical location. Fintech revolutionized how both individual users and the long-standing financial institutions approach managing money, making stock trades, or applying for loans.

Beyond popular fintech options like Apple Pay, PayPal, Venmo, Mint, and Wealthfront, major financial institutions and local hometown banks have begun embracing fintech, offering internet banking options or mobile applications to support their customers' financial needs.

Fintechs are also a significant part of the powerful eCommerce global industry. Any goods or services bought, sold, or traded online use financial technology to complete the financial aspect of these transactions. Additionally, fintech has expanded into the insurance industry and plays a part in the recent cryptocurrency boom.

Current Market Share

In 2020, according to the **Global Fintech Market Report**, the market share for fintech was valued at \$7.3 trillion and is projected to grow at a compound annual growth rate of 26.87% over the next four years. Anyone that sends money, makes a payment, purchases goods, deposits a check, or makes a stock trade within an application is an active part of this industry and its astronomical growth.

The investment and development of fintechs have grown just as quickly. Countless financial, investment, and banking applications flood online app stores. Financial institutions have seen the promise and potential of fintech, investing over \$27 billion since 2015, according to KPMG. Additionally, eCommerce incorporates many aspects of fintech, and like fintech, eCommerce has enjoyed substantial growth in recent years, averaging over 31% since 2019.

Fintech at a Glance

\$7.3
trillion
market share

26.87 %
compound annual
growth rate

over 31%
growth since 2019

\$27
Billion
invested since 2015



Fintech Solutions

Perhaps the biggest solution that fintech provides is the ease of use and accessibility to financial services that a traditional bank could not (or would not) provide. The underbanked and unbanked have far more options and financial solutions available to them now than previous generations could ever imagine.

Aside from those just discovering the world of fintech, some newer innovations and services are gaining popularity. The rapid rise in cryptocurrency offers new wealth growth and investment options, similar to what automated AI-driven investment services provide. Online insurance applications are gaining a larger market share, disrupting traditional insurance companies in similar ways as applications like PayPal disrupt conventional financial institutions.

In many ways, financial technology makes the process of buying and selling goods or services online seamless and easy. With little more than a bank account or a credit card uploaded to a profile or account, anyone can buy most things online. User-driven marketplaces, such as Craigslist, eBay, or Facebook Marketplace allow anyone to sell almost anything online.

Fraud Prevention and Cybersecurity

The integration and ease of use with fintech solutions also requires an unwavering focus on cybersecurity and fraud prevention risks and measures. Financial data and personally identifiable information (social security numbers, bank, or credit account information) are prime targets for data thieves and hackers.

Furthermore, COVID-19 has exacerbated these risks and concerns. The global pandemic disrupted much of our daily lives, driving more people to work from home and shop online. With this shift came an increased opportunity for fraud within the fintech industry. The massive increase in people's online activities, combined with governments devoting attention and resources to combatting the pandemic, allowed opportunistic bad actors to increase fraudulent activity across all the sectors that fintech touches.

More than ever, cybersecurity specialists, companies, and individuals must be vigilant against fraudulent activities.

What's Driving Fintech?

An Analysis of Key Drivers of Fintech Growth Activity.



Mobile Applications

Perhaps the single biggest driver in the fintech industry is mobile applications. There is, quite literally, an application available for every type of financial need a customer has, including banking, financial management, online bill pay, and loan applications, often all within a single application. However, many brick-and-mortar banking and financial institutions offer an accompanying mobile application option in addition to their in-person services.

Customers primarily interact with fintech through software programs and applications, of which there are hundreds of choices within the Mac and Windows app stores. For many people, there is almost no need to step foot inside of a physical bank to embrace the bevy of digital financial solutions; they simply need to download an application and set up an account. Within minutes, anyone could begin saving, investing, buying, or selling.

Customer Experience

One of the biggest appeals of fintech applications is the customer experience. Beyond ease of use, fintech applications are designed with ease-of-use in mind. Apple Pay, for example, makes it disturbingly easy to buy items and send money. Some messaging applications, such as WhatsApp, allow people to send money to each other within a chat. Additionally, investing in cryptocurrency is more accessible than before with apps like Coinbase, and PayPal offers a nearly one-click method to begin investing, embedded within the application.

For fintech applications, the customer drives the tools and features provided, as most apps are designed with individual user experience in mind. Fintech decision-makers focus more on markets and customer segments rather than geographic concerns, allowing a more tailored approach to an application that solves specific problems.

A good example is Chime, an entirely online bank. Chime built its fintech to offer free and easy banking to anyone, and the application provides almost complete control to the customer, with clean, straightforward interfaces and customer education.



Big Data

The most significant driver of fintech applications and programs is data. Based on our research, **over 2.5 quintillion** bytes of data are created every day. Reliance on traditional demographic research to inform strategic decisions, shape customer outreach, or inform application design has transformed into analytics provided by customer data and application usage.

Data-driven analytics informs a better understanding of customers by collecting information such as the number of credit card transactions per month, credit score trends, or average daily account balance. With the granularity and volume of data within a target market or customer base, fintech applications can innovate, iterate, and improve the services provided to the individual customer’s experience and interaction.

Low Barrier - Customer First

In 2020, according to **Statista**, nearly 6 billion people worldwide owned a mobile device, with this number expected to surpass 7.5 billion by 2026. This growth and unprecedented online access provide the potential for increased engagement with fintech. With applications designed to make digital finance simple and easy, availability is a significant driver of fintech growth.

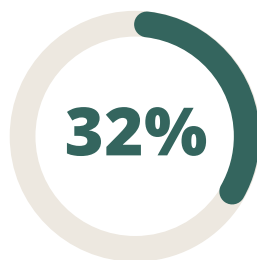
The increase in access to financial services represents a paradigm shift that fintech companies continue to capitalize on. These applications put the customer first, often leading to excellent customer retention and loyalty. People who prefer fintech applications embrace the feeling of control of their finances and banking, with the ability to look at account balances and investment returns in real-time.



\$613 billion
 growth in
 eCommerce in the
 first three quarters
 of 2020



of the worlds
 economy is
 comprised
 of financial
 services



eCommerce
 growth during
 the pandemic.

Fintech Trends in 2022

Global Finance Industry

By all accounts, the global finance industry is massive and touches nearly every other sector or industry. Fintech has become a partner with many established financial sectors with estimated growth **projections of 9.9%** for an industry that comprises up to 24% of the world’s economy.

Fintech continues to drive these growth estimates, especially between eCommerce and the global finance industry. Even before the COVID-19 global pandemic drove more people to their homes and the online marketplace, the ease and convenience of eCommerce saw steady and sustained growth. During 2020, however, eCommerce and online shopping grew by 16.4%, reaching \$613 billion through the first three quarters. In the US, eCommerce grew by over 32% during the pandemic.

Integration into Traditional Institutions

In some ways, fintech is still viewed as a disruptor to traditional financial establishments and services, despite increased integration and collaborative efforts. However, that perception is shifting as the arrangement between fintech and financial institutions benefits both parties.

Partnerships allow financial institutions to access technology without developing it in-house. In return, fintech companies gain access to an already-established customer base, often eager to engage with online applications.

Nearly every major financial institution has some form of online or mobile presence. Some newer banking, investment, or insurance options are entirely digital, a direct result of the impact and growth of fintech.

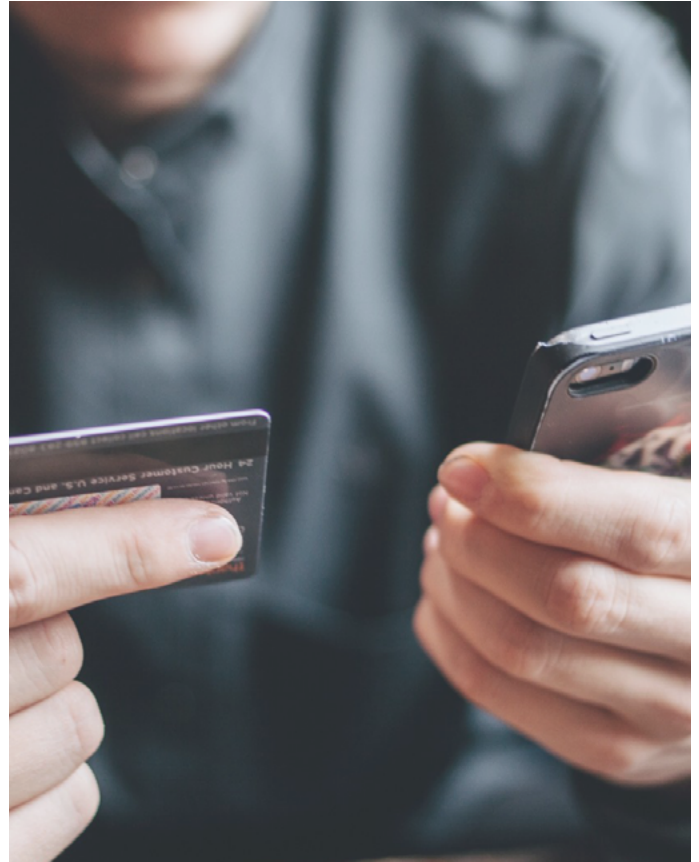
As the fintech infrastructure and ecosystem grows and matures, integration into traditional financial institutions will continue.

Data-Driven Customer Experiences

Data is behind many of the significant design and customer experience decisions for fintech - entire applications are designed and built based on data gathered from customer usage and habits, creating friction-reducing products and experiences.

Consider the ease of use with applications such as PayPal or Venmo to send or receive payments. Amazon provides one-click purchasing options once you find what you are looking for, and their returns program is almost painless. Mint, a program designed to help manage budgets and expenses, puts the user experience first.

Many of these applications, and the services or features they offer, are a direct result of data analysis. Data-driven custom experiences are somewhat self-fulfilling. The more people who download and interact with a given fintech application, the more data is available to innovate products and services further.



As the fintech infrastructure and ecosystem grows and matures, integration into traditional financial institutions will continue.

Regulations in 2022

Much like other tech industries, regulations in some ways have lagged behind innovation with fintech. This includes regulation geared towards traditional financial institutions and protecting customers and service providers.

Many new fintech options do not automatically comply with the established regulatory framework worldwide.

Two significant trends are shaping fintech regulation in 2022: antitrust regulations and cryptocurrency regulation.



Antitrust regulations - Antitrust regulations are nothing new to the financial industry. However, 2022 is projected to be a big year in antitrust regulation related to fintech. Similar to other regulations, the rapid growth and expansion of fintech have brought a renewed focus on business practices. By some estimates, over \$1 trillion in investment equity has been raised since 2010. Perhaps unsurprisingly, a big push by antitrust regulators revolves around privacy, customers, and data use.

Cryptocurrency - Cryptocurrency has seen astronomical growth and is a market disrupter in a league of its own. With this growth and the promise of wealth comes innovation and increased accessibility for investing. Today, cryptocurrency's buying, selling, and trading remains largely unregulated worldwide. Much like aging banking regulations, the world of cryptocurrency does not fit very well within the current regulatory framework. And due to the decentralized nature of crypto, lawmakers are finding it difficult to maintain a steady oversight of this revolutionary technology. A shift in regulations, and perhaps dedicated cryptocurrency regulation, could become

Security Risks and Threats

A World of Threats

The fintech industry is no stranger to the risks associated with financial fraud. Fintech companies and financial institutions must remain vigilant against many cyber threats, including



Phishing



DDoS Attacks



Chargebacks



Account Takeovers



Default Borrowers



Fines



Cost of Online Fraud

No matter how you slice the numbers, the cost of fintech fraud is not only staggering but growing.

According to a **Juniper Research study of Online Payment Fraud**, eCommerce merchants could lose upwards of \$206 billion.

In 2018, according to the **Associate of Finance Professionals**, 82% of organizations reported payment fraud incidents.

Forbes reports that in 2020, identity fraud was responsible for losses of \$56 billion for financial firms.

Our research at **Fraud.net** uncovered that companies could face as much as \$50 billion in fraudulent chargebacks by 2025.

Companies lose revenue at **an average of \$71 on a \$30 chargeback**. This number compounded when considering the inventory loss, the cost associated with the employees' time to process the chargebacks, and the shipping costs involved in such transactions.

False declines, or the flagging of legitimate transactions as fraudulent, also cost eCommerce businesses a lot of money. The culprit, most often, is outdated or legacy anti-fraud protection programs.

What isn't as easily quantified are the indirect costs resulting from fraud. Damage to brand reputation and loss of customer confidence can be damaging to the bottom line over the long term, while employees and fraud departments suffer a loss in productivity. Legal fees and the fallout from fraud also contribute to mounting indirect fraud costs.



of organizations reported payment fraud incidents

<p>\$206 Billion eCommerce losses</p>	<p>\$56 Billion losses for financial firms in 2020 to identity fraud</p>	<p>\$71 average loss for a \$30 chargeback</p>
--	---	---

The Real-World Impact of Fraud in Fintech

COVID-19 Relief Loans

The COVID-19 pandemic altered many ways of life around the world. At the onset of the pandemic, many governments instituted some version of reduced public access and gatherings, effectively locking down entire cities, municipalities, or even countries. A byproduct of this was the inability of people to earn a wage. A stop-gap option came in the form of COVID-19 relief loans.

In the United States, Government-guaranteed loans were intended to provide financial relief to small businesses hit the hardest by the pandemic. With these loans came the inevitable fraud schemes from those looking to take advantage of the situation. One such example is the attempt by **Justin Cheng**. He admitted guilt to major fraud in obtaining over \$7 million from COVID-19 pandemic relief loans by lying about his businesses, the number of his employees, and how the loans would be used, among other charges.



Snapchat BEC Attack

A business email compromise (BEC) results from a successful phishing attack. In the case of Snapchat, the target was the payroll department, and the damage was extensive. Despite these challenges, the employee who fell victim to the phishing attack believed that the email was from the CEO of Snapchat. The imposter CEO asked for payroll information on employees, and at least one person responded to the request.

To Snapchat's credit, the damage was mitigated, and further data leaks, aside from the sent information, were stopped. While the leak impacted none of Snapchat's user data, the same could not be said for the employees whose financial information was handed over to the hacker.

Financial Fraud in South Africa

In one of our **recent studies**, we found no practical or enforceable cybercrime law in place for South Africa. A direct result of this lagging legislation and the rapid increase in consumer eCommerce combined to see several troubling fintech fraudulent activities.

Although a 2020 data leak at Experian South Africa garnered the headlines, loan scams are the biggest and most common type of fintech fraud. Perhaps the most alarming aspect is the culprits are fintech businesses themselves, looking to exploit those in need of money. The fraud scheme included asking for upfront payment for an approved loan, and when received, the lender disappears, leaving the victim without the loan and out the money.



Moving Forward

One can easily surmise that the fraud ecosystem - and tactics to mitigate fraud - are incredibly dynamic. To truly stay one step ahead of these challenges requires time, resources, and matured industry knowledge. That's where Fraud.net can help.

Fraud.net: Our Methodology

Fraud.net emphasizes partnership to combat the growing threat of fraud within the fintech industry. With the rapid growth of fintech startups and established companies, the ever-present threat of fraud can create a situation where time and resources must be diverted to protect against vulnerabilities and exploits. Our combination of high-tech risk intelligence and tried-and-true financial controls are the basis of our methodology.

Challenges







Despite the best efforts and intentions of fraud protection programs and cyber security protocols, bad actors continually search for cyber weaknesses to exploit. Social engineering is one such example, where manipulating people is the goal. Training and awareness are the best defense against this threat. However, it is equally vital to early-detect against malware and malicious bots that might infect your data or servers. Companies must remain ever vigilant in preventing fraud by safeguarding sensitive customer data.

Many of our products and solutions combat fraud on multiple fronts. These options include data mining and discovery services, analytics and reporting, third-party monitoring services, and a full suite of identity verification services.



Artificial Intelligence-backed Solutions

Here at Fraud.net, we've brought an array of AI-backed security solutions to the market to stay one step ahead of these bad actors. From authentication verification to secure login, we use the power of artificial intelligence to mitigate the risk of attack.

					
Email AI	Transaction AI	Login AI	Account AI	Device AI	Application AI

We've employed machine learning models that focus on your business to combat fraudulent activities. Our process provides detailed analysis and a comprehensive risk score as our AI learns and adapts to your business. Over time, with continued interaction and machine learning algorithms, the AI becomes more intelligent and accurate, providing better analysis.

Our AI performs this analysis at scale, rapidly processing large amounts of data, using deep learning to increase analytical results. Together, working with your business, we will run your risk AI program and allow you to focus on growing your company.



Protect your Fintech with Fraud.net's Case Management Solution

With the rising trend of fintech fraud schemes, legacy case management workflows are not only outdated and tedious, but dangerous. One of the major causes of team burnout and underperformance is the flood of alerts and potential cases to manually sift through - and with cases only rising, even the best teams will struggle.

Fortunately, Fraud.net has a solution, in our streamlined Case Management Console. With the fraud Case Management Console, you get a comprehensive overview of key details and risk analysis results. These include transaction ID, customer identity profile, address, contact information, and even links to social media profiles for verification purposes.

With our solution, you can:

01. Actualize team administration by grouping personnel based on location, business unit, or expertise, and keep track of team and individual efficiencies with unique data displays to assign and monitor SLAs.
02. Control access to different dashboard views, ensuring only certain personnel can see or manage certain matters.
03. Queue action items for review so that your fraud teams can address suspicious transactions for a final sign-off.
04. Optimize rule creation with over 600 preset filters for better fraud case management
05. Plus, approve, deny or escalate flagged transactions to initiate the appropriate workflows with a few simple clicks.

With Case Management Console, you can automate the majority of fraud case reviews. This helps reduce the symptoms of burnout and frees up personnel to focus on other investigations.



Prevent Fraud Before it Happens

The history of verified and rejected transactions for a given customer offers your fraud teams the ability to determine how often that person has been flagged in the system and how much risk is associated with a particular identity.

By aggregating similar details from every vendor and partner in Fraud.net's Collective Intelligence Network, the risk scores are much more meaningful when making decisions regarding transactions.

This holds a particular benefit for your organization. Even if you have never interacted with a particular entity before, the Collective Intelligence Network uses data from millions of points across Fraud.net's consortium so you know an entity is bad before it's too late.

With Case Management Console, tracking changes to an entity's account over time becomes easier than ever while providing insight to interactions with organizations outside your own.

The Service Lookup feature allows individual pieces of information to be searched within Fraud.net's vast databases to verify any previous fraudulent activity associated with the information.

Geographic data that populates pinpointed locations on maps, as well as geolocation performed by IP address tracking, can help your fraud teams trace activity all over the globe from any location. The robust list of filter categories helps you obtain fine-grain detail in an instant to conduct in-depth investigations.

By placing the right information at the right time in the hands of your fraud teams, what once took days or weeks only takes a few seconds. This means fewer people can do exponentially more work, which is a major return on investment on day one operations.



With our solution, fewer people can do exponentially more work, which is a major return on investment on day one operations.

Conclusion

Fintech has become firmly integrated into our daily lives. They have partnered successfully with established financial institutions to benefit both parties. The shift to work-from-home, and the boom of eCommerce in 2020, further fueled the need for fintech companies to expand and innovate.

With this exponential growth comes no small measure of cyber security risks. Fraud remains the single biggest threat to fintech. However, fraud can be combatted, and the damage from fraud can be mitigated with a cohesive and rapid response when it can't be prevented.

[Fraud.net](#) is your strategic and analytical partner in the fight against fintech fraud. Talk with one of our experts today. Let's stop fintech fraud in its tracks.

[LEARN MORE](#)