

Socure identity risk insights:

Defining and solving the elusive challenge
of first-party fraud



Table of contents

Solving an elusive problem	3
— Executive summary	4
The insidious problem of first-party fraud	6
— No one is immune	8
— Future regulatory shifts will increase first-party fraud losses	8
Are banks and fintechs renewing their fight against first-party fraud?	10
From the field: Consumer sentiment around first-party fraud	11
— Trending first-party fraud behaviors in financial services	12
Breaking down current first-party fraud detection efforts, and why they aren't working	20
— The limitations of current first-party fraud solutions	21
Investing in a path forward	22
— Start here: A suggested first-party fraud definition	22
— How you can participate in solving first-party fraud	24
— Taking the next step	25



Solving an elusive problem

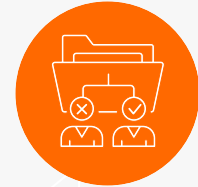
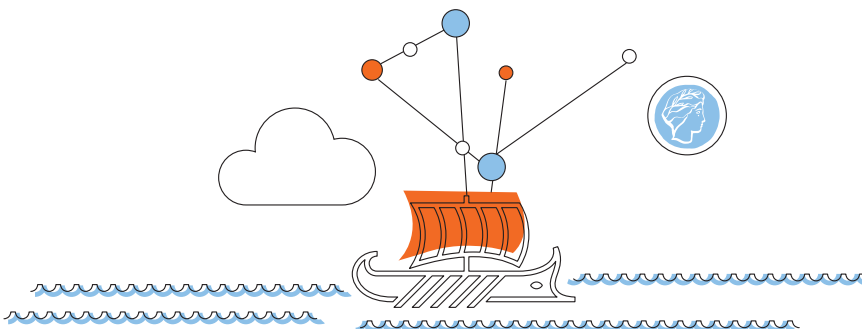
When we think of fraud, shadowy figures stealing identities from behind a screen often come to mind. But there's a more elusive type of fraud that's challenging to detect at best, and impossible at worst. First-party fraud, or the use of one's own identity to commit a dishonest act for financial gain, requires a different set of remediation tactics from the usual third-party fraud. Therefore, solving for this type of fraud requires a new approach.

But first, a history lesson.

Financial fraud dates back to the year 300 B.C. A Greek merchant named Hegestratos took out a large loan on his boat, known as "bottomry." Using his boat as collateral, Hegestratos borrowed the money and agreed to pay it back with interest when the cargo — in this case, corn — was delivered. If he neglected to pay back the loan, the lender could claim the cargo and the boat used for its transportation. Hegestratos planned to sink his empty boat, keep the loan, and sell the corn. Unfortunately for him, the plan failed. When his crew and passengers caught him in the act, Hegestratos drowned trying to escape.

You may have heard this story before. Previous mentions found on the internet have suggested Hegestratos perpetrated different types of fraud, including insurance fraud. However, no insurance premium was paid. In fact, a loan was made and paid out to the party who used their own identity in a deceitful attempt to make a financial gain for themselves. The first recorded incident of financial fraud was first-party fraud.

Here we are, 2,313 years after Hegestratos' death, still cursed with the insidious problem of first-party fraud. We're sitting with the uncomfortable realization that we have continued to address the problem the same way as it was handled back in 300 B.C.



First-party fraud definition:

When a consumer their own true personally identifiable information (PII), including name, DOB and SSN, and knowingly and deceitfully manipulates one or more characteristics about their identity or commits a dishonest act, for financial gain.

Executive summary

The financial services industry has long relied on assessing consumer “intent” – or the thought behind a consumer’s transaction or purchase – to detect first-party fraud. But intent is fluid – it shifts as life circumstances change. A customer may open an account legitimately, only to later perpetrate fraud if they lose their job or face economic hardship. Proprietary consumer research* conducted by Socure found that of the respondents who admitted to committing first-party fraud, 34% did so due to economic hardship. Measuring consumer intent is nothing more than a guessing game, with losses in the U.S. alone projected to exceed \$100 billion annually.

To date, there is not a comprehensive solution that solves first-party fraud across scheme types and industries, while returning low false positives and high fraud capture rates. In this report, we’ll outline a cross-industry and pioneering approach to finally begin to solve the problem of first-party fraud.

We’ll cover:

- How the shift in liability of authorized push payment fraud from consumers to banks and fintechs for certain types of transactions will fuel a substantial increase in first-party fraud attempts over the next several years, and banks are not ready.
- Highlights from Socure’s proprietary research that demonstrates real-life, data-driven patterns of first-party fraud schemes in fintech and traditional banking environments. These signals created by consumers performing first-party fraud can be used in future solutions to identify and stop this crime. Some of those findings include:
 - Consumers who have 2 or more closed accounts associated with first-party fraud behavior (i.e. fraudulent disputes) are 189 times more likely to commit first-party fraud again if given the chance.
 - Accounts with 5 or more registered authorized users are 22 times more likely to be first-party fraud.
 - First-party fraud was committed by 30% of the consumers who held accounts across at least four financial institutions that participated in Socure’s consortium study.
 - An account closed within 90 days from opening is 3 times more likely to be first-party fraud in a new account opened following the closure.
 - Based on Socure customer observations, consumers perpetrating first-party fraud at the new account level often use newly created identity contact elements such as email, address, and phone numbers, likely in an attempt to avoid the anticipated collection efforts.
- The need for a cross-industry developed standard definition for first-party fraud and why changing the definition of first-party fraud from consumer “intent” toward “deceitful” and “fraudulent” consumer activity will greatly enhance our ability to stop first-party fraud.

- Banks and fintechs have increased their efforts to fight back against first-party fraudsters and attempt to recapture financial losses from illegitimate disputes and other fraudulent account activities.
 - Based on a Socure customer study, 50% of respondents said they take steps to recapture lost funds from a consumer dispute of a transaction that is determined to be first-party fraud.
 - Of the 50% who said they take steps to recapture losses from first-party fraud, 67% of respondents said their efforts have become “slightly” or “much” more aggressive in the last 12 months.
 - 66% of respondents said they label first-party fraud as a “fraud loss,” with the remaining respondents saying they report the loss as “credit loss.”
- Socure research highlighted that 35% of Americans admit they’ve engaged in some form of first-party fraud at least once, with 10% admitting they have engaged in several different types of first-party fraud.

Some additional insights include:

- The most commonly admitted type of first-party fraud – 22% of surveyed Americans – is requesting a refund on an online purchase even when the item was received, followed closely by choosing not to pay off credit card bills indefinitely (21%), and disputing legitimate financial transactions (20%).
- 40% of Americans know someone who has engaged in first-party fraud.
- Nearly a third of Gen Z respondents (30%) have made a purchase through Buy Now, Pay Later (BNPL) without intending to pay it back.
- Most Americans who admit to first-party fraud say they did so due to economic hardship (34%). 29% claim it was an accident, and 19% committed first-party fraud because they know someone else who does it.
- 12% of Americans – 1 in 5 of Gen Z respondents – don’t consider first-party fraud to be ethically wrong.
- A majority (52%) of Gen Z say they’d commit first-party fraud if they knew there would be no negative consequences.
- When it comes to first-party fraud activities, men are more likely than women to have perpetrated it at least once (42% among men vs. 28% among women).
- First-party fraud is notoriously difficult to classify. Analysis of Socure customers who provide performance feedback on fraud showed that 30% of labeled third-party fraud is actually first-party fraud where the consumer has lied and said “I did not open that account.”

At Socure, we believe that by fully embracing pioneering solutions, increased collaboration, and proactive policy changes, the financial industry can dramatically reduce current first-party fraud losses and forge an ecosystem of trust that’s resilient to emerging threats. United, we have the power to solve this complex challenge.

Let’s begin.

The insidious problem of first-party fraud

First-party fraud is a common and growing problem across banking, credit card, and merchant environments. Without a combined industry effort to attack first-party fraud, current economic forces, changing consumer sentiment, and shifts in liability in authorized push payment (APP) fraud will likely create even greater risks over the next several years. Socure is leading the cross-industry effort to address the problem of first-party fraud at the new account level and for fraudulently disputed transactions.



The industry generally defines first-party fraud as the use of one's own identity to open an account and use it to commit a dishonest act for personal or financial gain.

While this definition covers first-party fraud activity at new accounts, it does not necessarily consider transaction, deposit, withdrawal, or payment activities in demand deposit accounts (DDA) and credit card accounts. Accounts opened with good intentions and plans to pay for purchases can certainly go awry as a consumer's motivations or economic situation changes over time. Consumers can backslide into falsely disputing account transactions, or be coaxed into acting as money mules and perpetrate fraudulent money movement for bad actors, in exchange for a skim of the transaction.



How do merchants define first-party fraud? One commonly used definition: First-party fraud occurs when an individual receives goods or services after promising to make a future payment for those items.

This definition includes post-origination first-party fraud activity, but leaves out the new account level.



Socure is leading the cross-industry effort to address the problem of first-party fraud at the new account level and for fraudulently disputed transactions.



\$100B

Losses connected with first-party fraud annually in the U.S. across financial institutions and merchants.

Today, losses connected with first-party fraud total more than \$100 billion annually in the U.S. across financial institutions and merchants. [Here's the math:](#)

Credit Card

According to PaymentsJournal, 60% of financial institutions report first-party fraud as the prominent source of fraud losses.¹ First-party fraud usually comprises 10% of the volume of credit card losses.² The current 12-month average charge-off rate as of the February 2023 distribution date is 1.82% and Americans now hold a record amount of credit card debt — nearly \$988 billion, according to the Federal Reserve Bank's latest data.^{3,4} This equates to \$18 billion lost annually to first-party fraud.

Merchant

Merchants are not exempt from these losses, spending more than \$50 billion per year in first-party fraud losses according to Mercator Advisory Group.⁵ Additionally, first-party fraudsters abuse chargebacks, promotions, returns, or merchant and financial services firms' policies to get free merchandise or payouts, costing merchants upwards of \$89 billion per year.

Bank Disputes Resolution

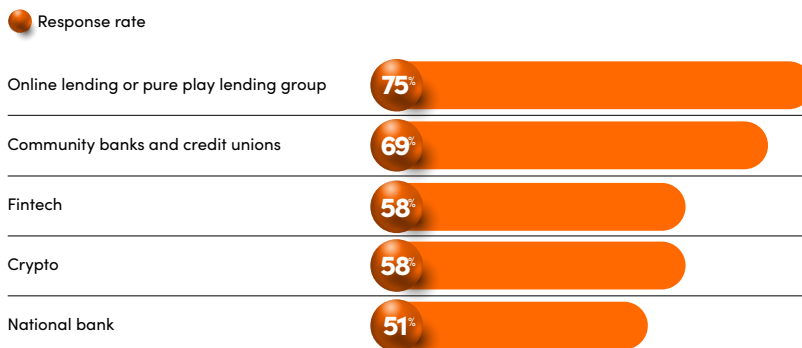
All of these loss estimates originate at a single point: when the consumer disputes a transaction. This may include an ACH, a credit card purchase, a wire transfer, a bitcoin payment made through an ATM transaction using a QR code, or a P2P payment. McKinsey estimates that the top 15 U.S. banks spend approximately \$3 billion each year, combined, on disputes processing.⁶ About 50 million to 100 million disputes occur annually in the U.S., with a cost per dispute ranging from \$10 to \$50.

No one is immune

First-party fraud attacks lenders, banks, and fintechs both large and small. More than 69% of respondents to Alloy's Fraud Benchmark study reported being attacked by this fraud vector. Additionally, 58% of both the Fintech and Crypto industries also fight against first-party fraud.

First-party fraud by industry sector

First-party fraud, the most common type among those surveyed, hit lenders and community banks and credit unions the most.



Respondents were told to check all that apply to their particular instance with fraud.
Source: Alloy - Get the data - Created with Datawrapper

At Socure, we often see high levels of first-party fraud in customer analysis for sectors such as online gaming and gambling, Buy Now Pay Later (BNPL), payment platforms, and marketplace lending industries. One example? Socure research shows that nearly a third of Gen Z has made a purchase through BNPL without intending to pay it back.

But the problem of first-party fraud continues to grow in size and complexity across every industry we serve. This is especially true during periods of economic downturn in which more individuals may commit bust-out fraud — when consumers establish a normal usage pattern and repayment history and then max out the credit line with no intention of repaying.

Future regulatory shifts will increase first-party fraud losses

There is a major shift in liability related to specific types of consumer scam losses on the horizon. Today, consumers shoulder most of the financial burden from romance, imposter, and other social engineering scams. Their originating banks — normally on the hook for fraud liability — are not fully responsible when account holders willingly send money to a fraudster in a receiving bank.

More than 69% of respondents to Alloy's Fraud Benchmark study reported being attacked by this fraud vector.

The dark side of liability shifts



- Bad actors – including fraudsters and money mules – will exploit new liability rules once details are made public, driving an increase in social engineering scams.
- With banks and fintechs now responsible for scam losses, consumers may be more willing to act as money mules moving fraudulent funds.
- Fraudsters can recruit consumers to make dubious claims for reimbursement from their banks for nonexistent losses, a form of first-party fraud.

However, since June 2022 a string of U.S. Senators and regulators like the Consumer Financial Protection Bureau (CFPB) have been pushing to move the losses linked to payment scams away from consumers and onto banks and fintechs that hold the receiving depository account in a transaction. This potential shift in liability will most likely cover all payment types, including ACH, wire transfer, check, ATM crypto transfers, and P2P payments, among others.

The Federal Trade Commission's (FTC) most current 2022 Consumer Sentinel Network report highlights that \$2.732 billion was lost last year by consumers impacted by imposter scams across the aforementioned types of payment channels.⁷ This equates to 1 in 5 U.S. consumers impacted by social engineering scams, which averaged \$1,000 per incident.

With the liability burden removed from consumers, some industry leaders worry the shift will make lucrative first and second-party fraud scams even more enticing, fueling a wave of attempts to exploit the system.

Notably, Zelle and its bank owners have taken a proactive approach and are now creating a playbook for refunding customers and each bank member for certain scam payments.

In March 2023, when a Zelle spokesperson was asked if the rule change would provide reimbursements to customers who are tricked into sending money via Zelle, the Zelle spokesperson responded: *"I can confirm that Zelle is revising its network rules as part of ongoing efforts to protect users against the most recent fraudulent schemes. We will not issue details because we then risk tipping off the fraudsters."*⁸

While Zelle is the only known real-time payments channel that is taking steps to self-regulate prior to government intervention, we can assume that other P2P payment platforms will follow suit and that banks and fintechs will have to develop similar rules for ACH, checks, and other payment processes.

While the U.S. banking system is working to accommodate the potential changes to authorized push payment liability, organized actors will undoubtedly be enlisting money mules and willing consumers to participate in first party and other types of fraud scams.

In our estimation, the use of "complicit" money mules and consumers who are willing to participate in first-party fraud schemes will explode. This tactic, known as "mule activity" has increased by 41% in 2020 in comparison to attack rates prior to the pandemic.⁹

Are banks and fintechs renewing their fight against first-party fraud?

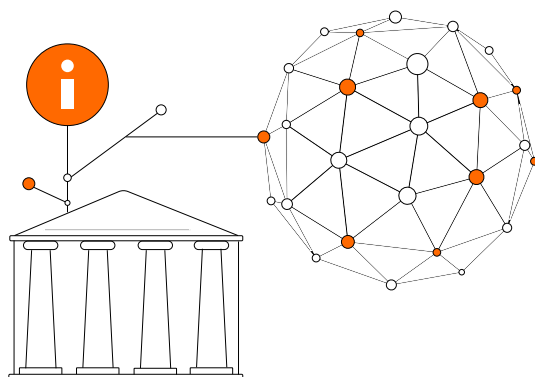
Some banks and fintechs taking losses from first-party fraud attempts are ramping up their efforts to fight back. They're launching formal investigations against high-balance offenders and sending more "demand letters." These letters state a legal claim demanding restitution or performance of some obligation, owing to the recipients' alleged breach of contract, or for a legal wrong to recapture fraudulently obtained goods or dollars lost.

But this aggressive, proactive approach is not universal.

In a recent survey, Socure found that almost 50% of respondents said that they "do not go back to the consumer to collect funds, even if we determine it is first-party fraud." In these instances, the respondents said they "just take a loss." While this may be the path of least resistance to avoid the costs of taking legal action, what if there was a better way to address this challenge?

For the other half that does attempt to collect on disputed transactions that are considered first-party fraud, those participants said overwhelmingly that they first "call the consumer and ask for the funds." If that does not work, they "pursue collection legally," generally through demand letters.

When asked if their efforts to pursue losses generated by first-party fraud had remained the same, lessened, or increased over the last 12 months, 60% of respondents said, "our efforts have become slightly more aggressive and we are taking steps to collect on certain types of first-party fraud losses." The remaining portion of respondents said, "we have not changed our efforts over the past 12 months to collect first-party fraud losses."



50%

of surveyed financial institutions do not go back to the consumer to collect funds, even if they determine first-party fraud.

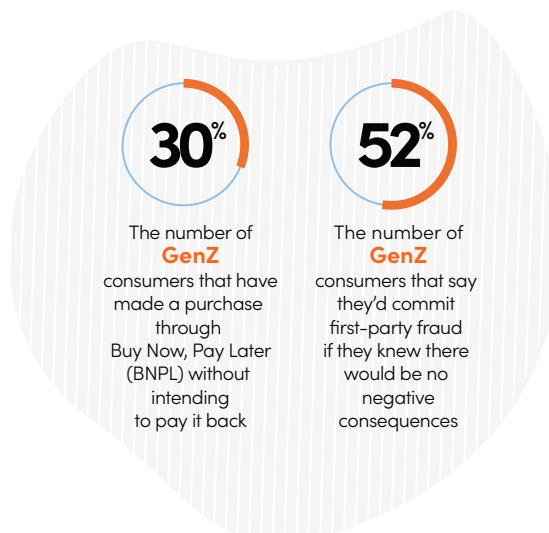
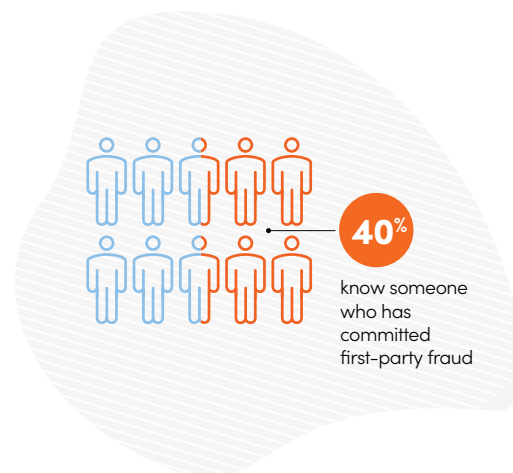
From the field:

Consumer sentiment around first-party fraud

Financial fraud is alarmingly common in America today. In October 2023, Socure conducted research to measure consumer sentiment when it comes to committing first-party fraud. A shocking 35% of survey respondents admitted to engaging in some form of first-party fraud, such as making a Buy Now, Pay Later (BNPL) purchase without intending to pay it back. 45% know someone who has committed first-party fraud.

We also learned who is committing financial fraud and why. The research shows economic hardship and accidental fraud as the top reasons given, though some admit that curiosity or feeling owed by a company led them to commit fraud.

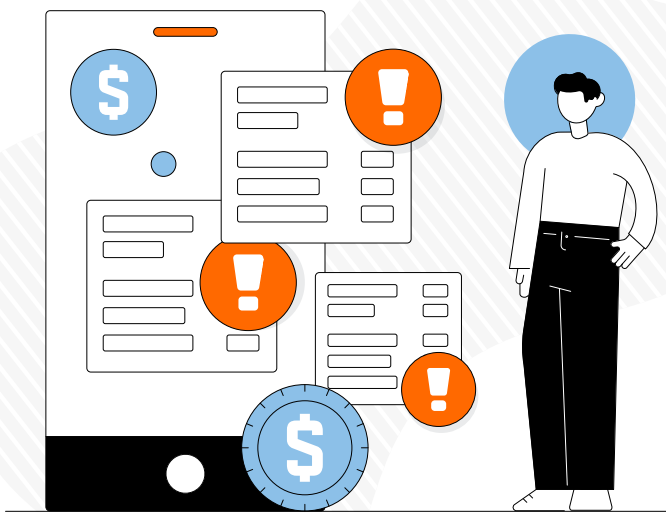
Overall, 77% believe some fraud should not face legal punishment. First-party fraud rates are highest among younger Americans, with 30% of Gen Z abusing BNPL specifically. Interestingly, Gen Z is far less likely to consider this behavior fraudulent compared to Baby Boomers. In fact, half of Gen Z admits they would commit first-party fraud if there were no consequences. This generational divide highlights shifting attitudes toward financial ethics and the need for consumer education.



Trending first-party fraud behaviors in financial services

To better understand first-party fraud and behaviors within the industry, Socure worked with several industry-leading fintechs to develop a consortium of payments, transactions, new account applications, and other information. The data for the analysis included hundreds of millions of financial transactions, both “good” transactions or non-delinquent, and “bad” transactions labeled as first-party fraud, spanning 36 months, from January 2019 through December 2021. Data was provided from large fintechs offering deposit and card accounts as well as fintechs offering lending products.

Socure also studied our current first-party fraud customer consortium data, which is associated with hundreds of millions of account opening attempts. The records used in the study span more than a decade and were analyzed alongside data from our wider customer consortium, including industries such as the largest U.S. traditional banks and fintechs, point-of-sale lenders, Buy Now Pay Later (BNPL), online gaming and gambling, and investment accounts.



Socure worked with several industry-leading fintechs to develop a consortium of payments, transactions, new account applications, and other information.

To our knowledge, this is the most comprehensive study of first-party fraud undertaken in the U.S. to date.

From this analysis, we learned that first-party fraud behaviors leave tell-tale signs that can be used to identify and stop financial loss.

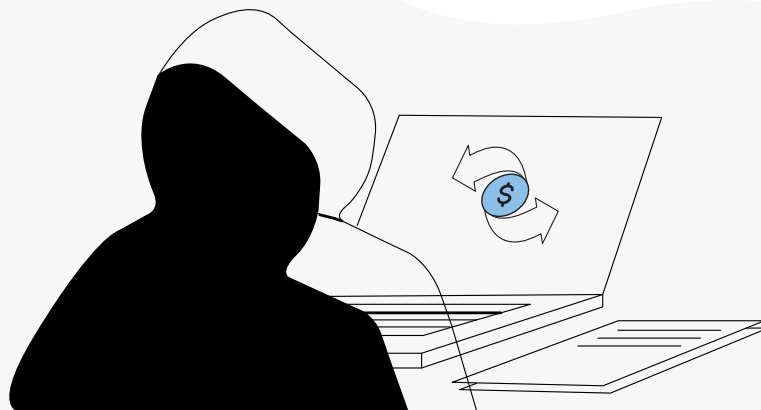
These signs include:

- **At the point of a new application**

- Loan stacking efforts across several institutions over the course of a short period of time.
- Use of recently created identity contact elements such as email, address, and phone numbers used in new applications.
- Rapid velocity of many opened accounts that are shortly closed by the deposit institution. In fact, our study suggests that an account closed within 90 days from opening is 3 times more likely to be first-party fraud.
- Consumers who have 2 or more closed accounts associated with first-party fraud behavior (i.e. fraudulent disputes) are 189 times more likely to commit first-party fraud again.
- Large amounts of Card Not Present (CNP) transactions returned due to insufficient funds.

- **Disputes of transactions made by the consumer**

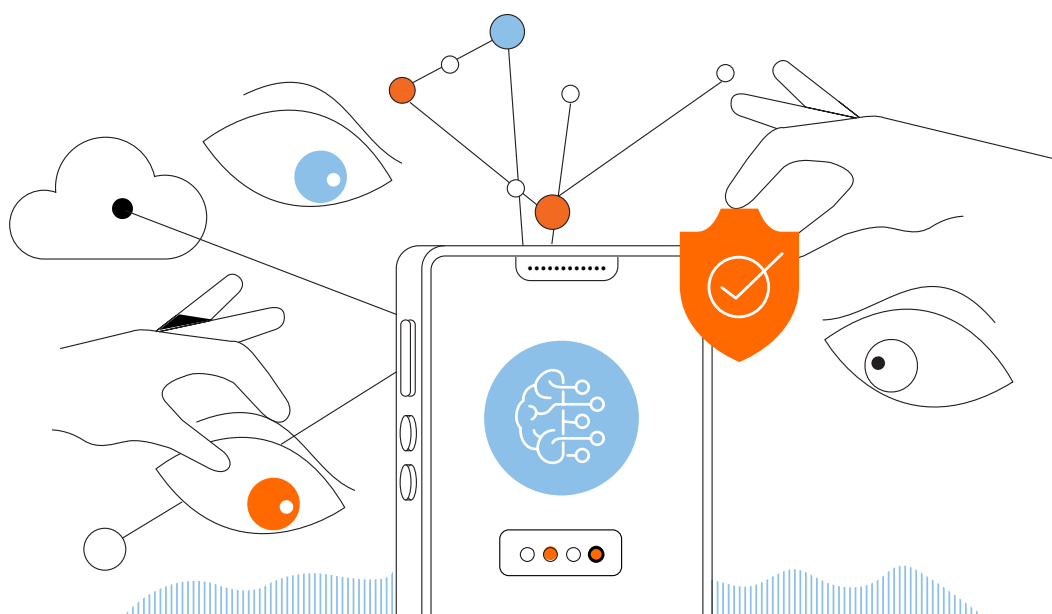
- Overlap of previous dispute rates and velocity across fintechs. For instance, signals of first-party fraud were detected in 30% of consumers who held accounts across at least 4 consortium study participants.
- Higher levels of first-party fraud disputes when a consumer has several of the same type of account across several different fintechs or traditional banks.
- Higher dispute rates on transactions across differing fintechs and traditional banks within close time proximity of one another.



- **Other account activity**

- The same check attempted to be deposited using Remote Deposit Capture (RDC) across several different deposit accounts
- A high velocity of returned ACH transactions across several different deposit institutions
- A higher number of authorized users on an account reflects an increased propensity for the account to be closed for first-party fraud behavior. For instance, accounts with 5 or more registered authorized users are 22 times more likely to be first-party fraud
- High ACH withdrawal velocity, or higher dollar value of ACH and credit card transactions is an indicator of ungranted disputes, which is a strong proxy for first-party fraud behavior. For instance:
 - The average fraudulent ACH transaction value (\$1,631) was more than 10x the value of a legitimate ACH transaction (\$145).
 - The average fraudulent card transaction value (\$96) was ~4x the value of a legitimate ACH transaction (\$26).

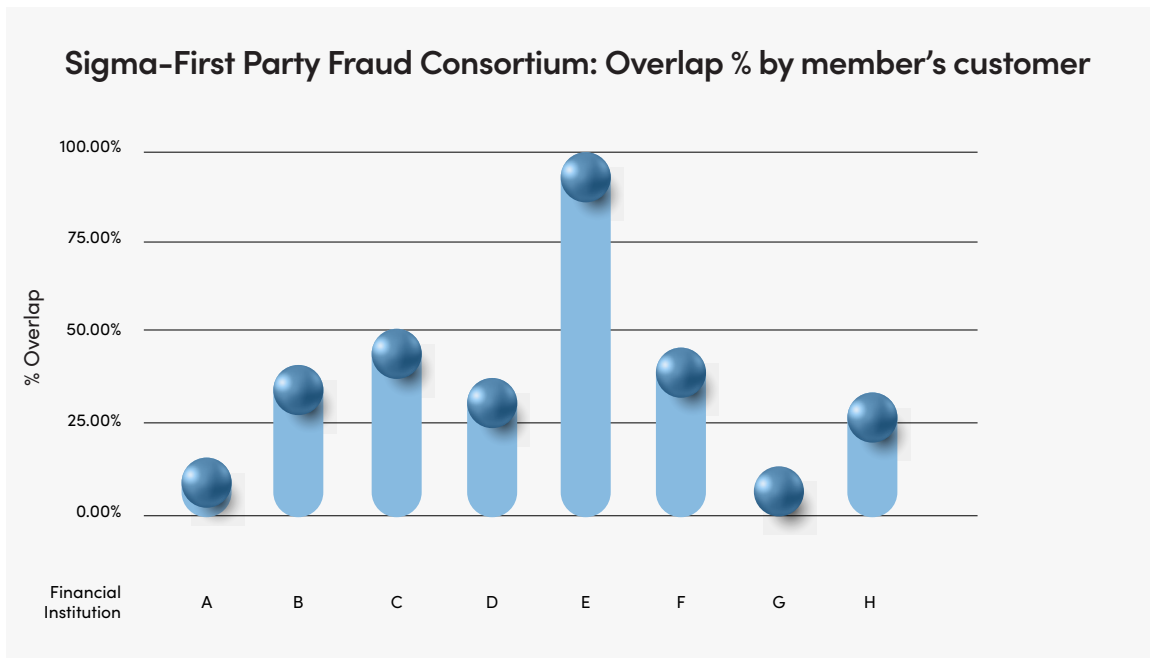
These behaviors are found across a range of financial services industries, as well as merchant and retail accounts. This is a testament to the need for cross-industry participation.



Below are some additional insights and case studies:

Individuals with accounts at multiple participants have vastly elevated first-party fraud rates

First-party fraudsters decide in advance to open several different accounts and then perpetrate fraudulent disputes or claim “third-party fraud” on an account at a similar time across many different accounts. On average, we saw an overlap of 45% across all accounts in the in Socure’s Sigma First-Party Fraud consortium study.”














As seen from the table above, the overlap differs substantially for individual financial services. Surprisingly, Financial Institution E almost overlapped 100% with other participants in the study. Financial institution E was very similar to several of the larger participants in the study and also had fewer overall accounts than the companies with which they overlapped. We are still analyzing this data to understand the interrelationships between players related to industry types, open dates, and geographic dispersity.

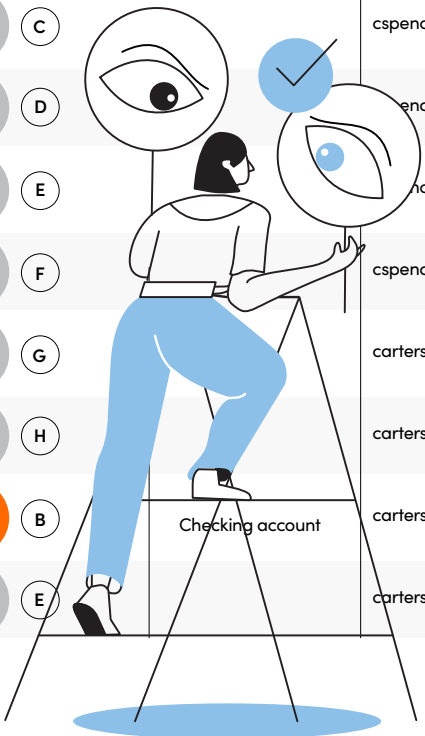
Consumers changed contact elements to avoid eventual collections activity

Consumers who open accounts and are found to be fraudulently disputing the opened account after the financial institution’s investigations often exhibit a similar pattern of providing newly created contact elements.

Here is an example of the types of email changes that are seen over a period of time within and across several different study participants. Consumers perpetrating first-party fraud will come back to lenders multiple times to apply for credit. *Note that these email addresses are representative and do not include the actual consumer PII.*

Socure Risk Insights: First-party fraud account scenarios

Network participant	Account type	Email addresses used	Date account opened
 A	Savings account	carterspencer31@example.com	2021-06-15
 A	Checking account	carterspencer31@example.com	2021-06-15
 B	Savings account	cspencer859@example.com	2021-07-02
 C		cspencer859@example.com	2021-11-01
 D		cspencer859@example.com	2020-11-01
 E		cspencer859@example.com	2020-10-15
 F		cspencer859@example.com	2020-10-15
 G		carterspencer0219@example.com	2021-03-01
 H		carterspencer31@example.com	2019-06-03
 B	Checking account	carterspencer31@example.com	2019-02-22
 E		carterspencer31@example.com	2019-02-21



At first we considered that these changes could have been made to direct account contacts by a “handler” working with the first party. However, manual fraud investigations of thousands of these types of accounts completed by Socure’s fraud investigation team found that most of these changes are the real consumer using new emails and phone numbers, likely in an attempt to avoid the expected collections efforts once the account goes into delinquency.

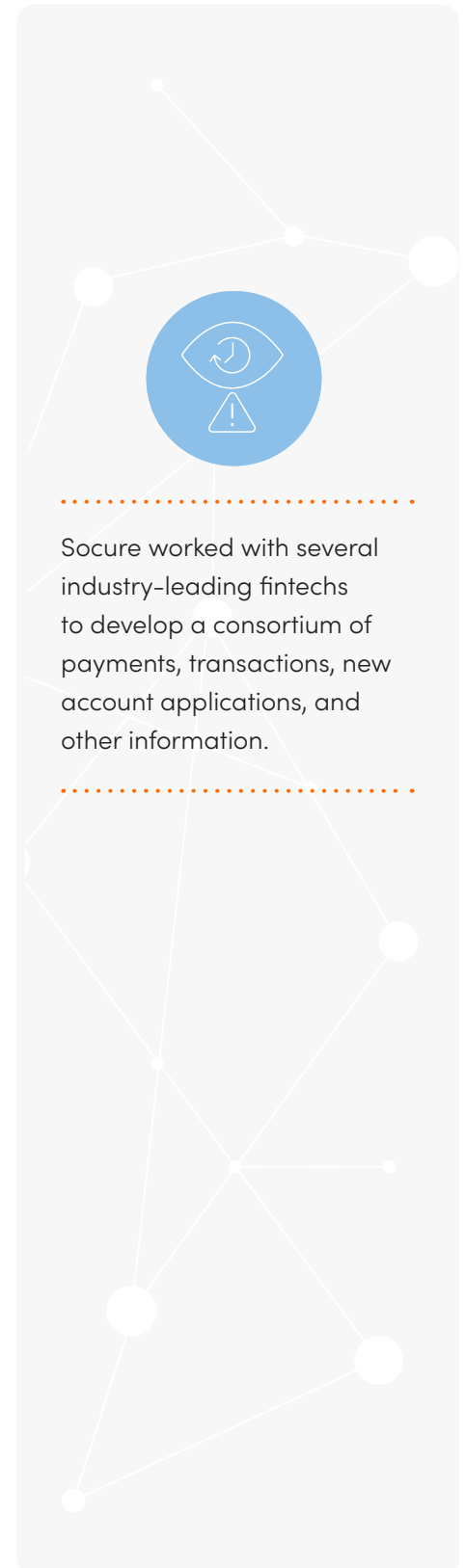
The higher number of deposit accounts a consumer holds ties directly to the amount of first-party fraud they perpetrate

Individuals who are members of at least four of Socure's consortium participants were seen committing first-party fraud in at least one of those participating financial institutions 30% of the time.



In the chart above, of the consumers who have 6 or more financial institution relationships, they turn out to be first-party fraudsters 50% of the time.

It's also important to note that there is often a considerable lag between observation dates for fraud incidents, which affirms the value of consortium data as an early predictor of fraud.



Socure worked with several industry-leading fintechs to develop a consortium of payments, transactions, new account applications, and other information.



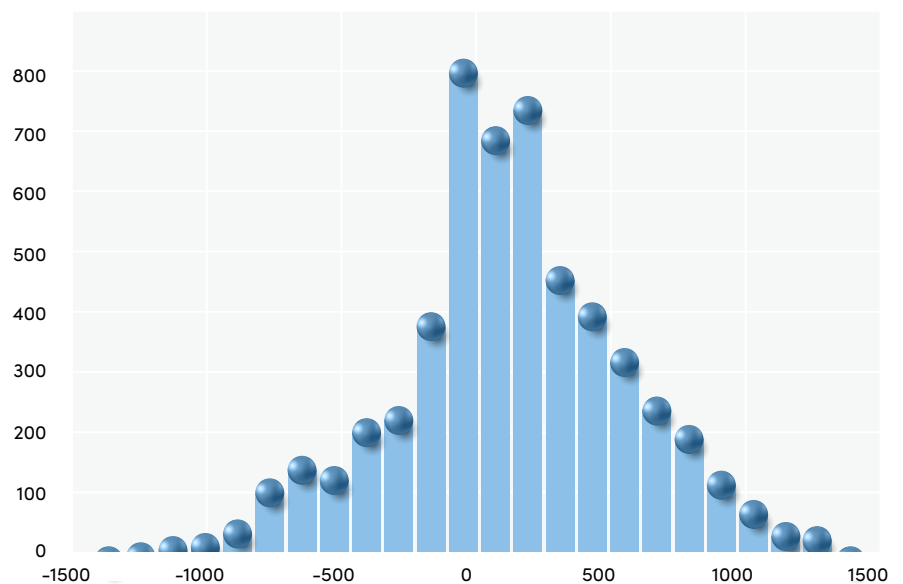
66%

Our analysis showed that 66% of the time, Socure could have reported on potential first-party fraudsters within our consortium participant's portfolio.

First-party fraudsters can be identified by using previously reported first-party fraud behaviors

As part of our data study, we focused on one of the larger institution's data to understand if we could have provided them an early warning, had our future first-party fraud solution been live. Our analysis showed that 66% of the time, we could have reported to that institution about potential first-party fraudsters within their portfolio. In many cases, these reports could have come months in advance of the first instance of fraud at each institution.

The distance in days between reported dates for fraud observations

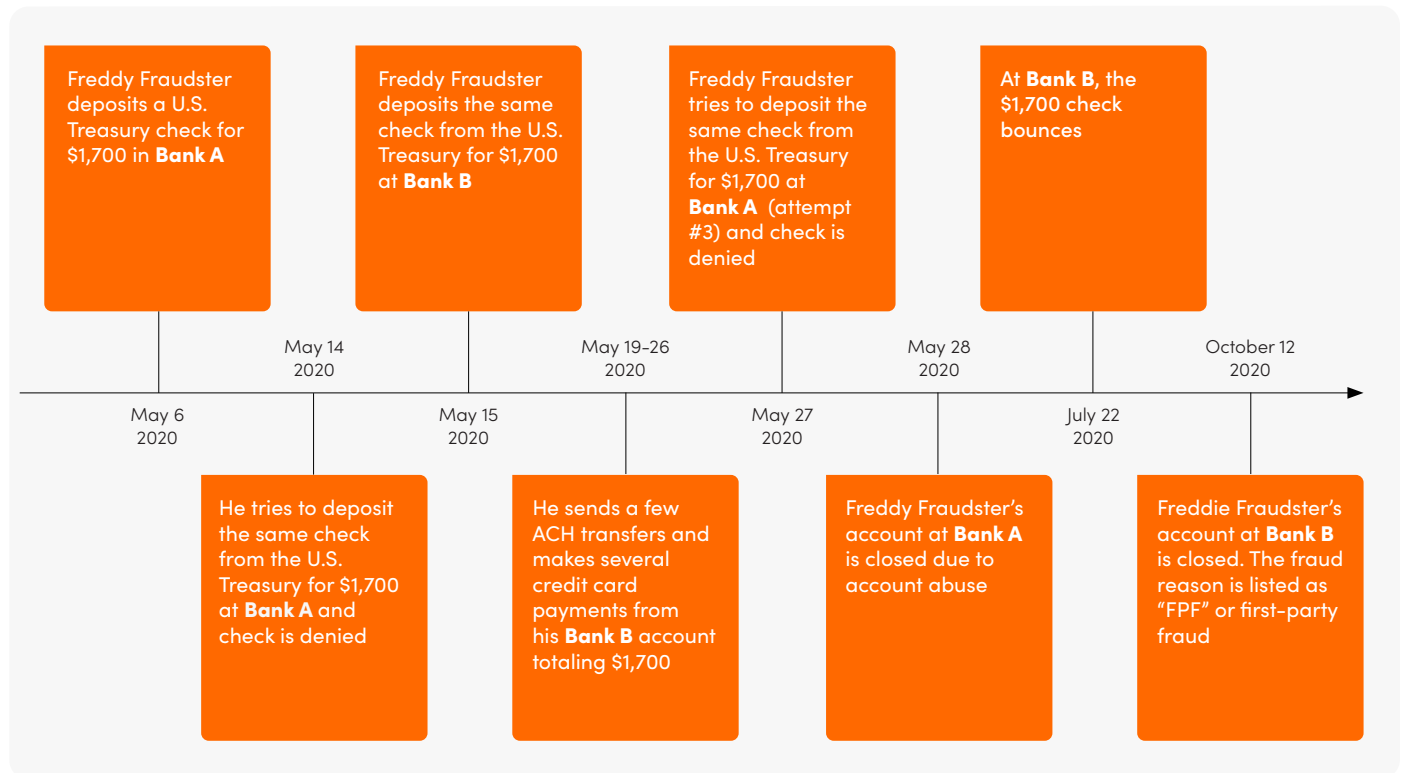


<0 days - first-party fraud detected by Bank A first
 >0 days - first-party fraud detected by other client first

Case Study:

Remote deposit capture first-party fraud efforts

The following timeline represents a real-world example of a consumer attempting, with some success, to deposit the same check via remote deposit capture (RDC).



As you can see from the timeline, the first-party fraudster attempts to deposit the same check four times during a three-week period in May 2020. Two of the deposit attempts are accepted. You can also see that the consumer quickly disperses the exact amount of the check, \$1,700, via ACH transfers and credit card payments in an attempt to quickly take advantage of their deceit. And apart from having his accounts closed, what happened to Freddy?

Probably nothing.

Breaking down current first-party fraud detection efforts, and why they aren't working

There are several methods to detect first-party fraud that have been used by both financial services and merchants.



Biometric data, such as fingerprints or facial recognition

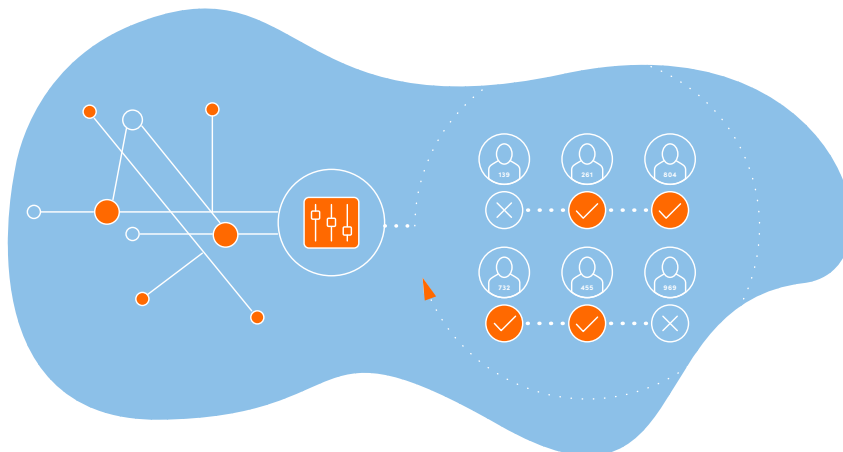
Institutions use this method to ensure a person opening an account or making a transaction is who they claim to be, and find it valuable when investigating a dispute.



Device “fingerprinting” and behavioral analysis

By understanding how the consumer’s device is used, institutions can employ device intelligence to analyze the unique characteristics of a customer’s device, such as the device’s operating system, the browser type, and the IP address.

Biometric data, photos, and device signals are important data points to validate that a consumer did make a transaction. But with the coming shifts in liability for APP fraud, these signals become obsolete in many instances, because the consumer is not disputing the fact that they actually sent the P2P payment, be that through ACH, wire transfer, or any other payment channel. In APP, the consumer is fraudulently saying they were duped into making the transaction, nullifying device signals, behavioral analytics, and photos in the investigation process.

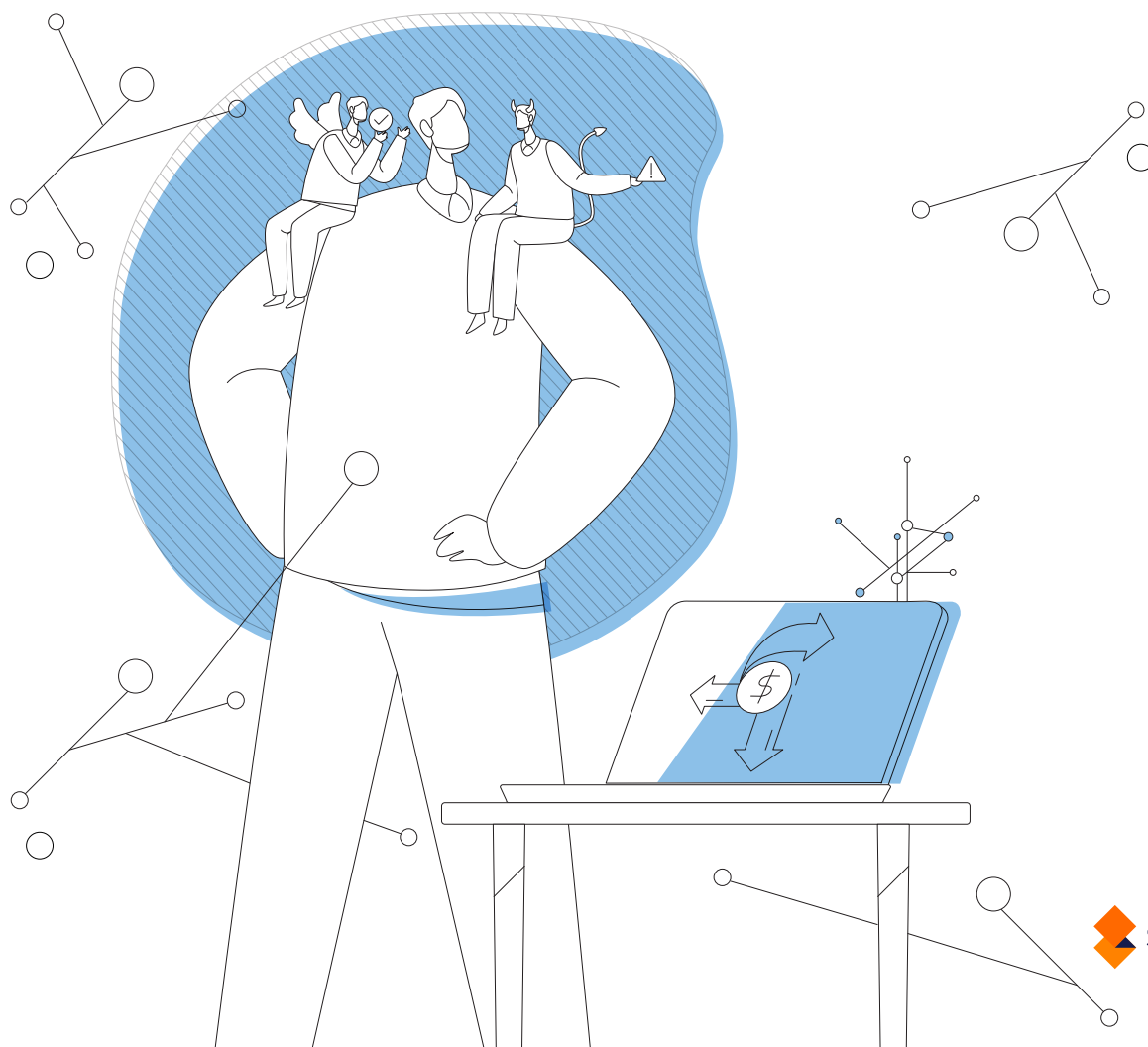


The limitations of current first-party fraud solutions

First-party fraud solutions in the market today are discombobulated because they focus on a single point of the account lifecycle, such as a new account or transaction, and a single industry, such as financial services or merchants.

This narrow focus greatly limits the signals that can be used to more precisely identify first-party fraud for both the merchant and financial services industries. Without exception, all first-party fraud solutions today limit themselves to addressing one type of fraud scheme, such as disputes or credit “abuse.”

To date, there is not a comprehensive solution that solves first-party fraud across scheme types and industries, while returning low false positives and high fraud capture rates.



Investing in a path forward

We believe that there should be a single definition that has several subtypes of first-party fraud. This will help identify additional details to use for fraud labeling and solution and model development. Our suggested version of a new first-party fraud definition is laid out below.



Start here: A suggested first-party fraud definition

When a consumer uses their own true personally identifiable information (PII), including name, DOB and SSN, and knowingly and deceitfully manipulates one or more characteristics about their identity or commits a dishonest act, for financial gain.

Why would a standard definition be useful?

- 1** It would help banks, credit issuers, and merchants perform additional “step-up” verification on a consumer who has committed fraud in the past. Step-up could include requiring further validation of bank account data or additional income screening based on previous fraudulent activity. Even deploying a “sentinel approach” to step-up by performing a document verification with a selfie might deter someone who is considering first-party fraud at the point of a new application.
- 2** A standard definition will help drive data sharing, which will provide consumers with the ability to dispute the legitimacy of the prior reported fraud, or give the consumer the ability to repay the debt and remove any previously reported fraudulent activity conducted by them.



A few types of first-party fraud:

Financial misrepresentation:

Providing inaccurate employment information, such as company, title, or self-reported income

False claim:

Falsely disputing a financial transaction that can be proven to have taken place

Identity manipulation:

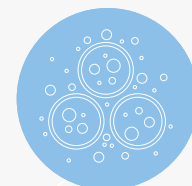
Changing contact elements in advance of first-party fraud behavior to avoid collection activity

3 It would provide the bank or lender with additional opportunities to claw back financial loss tied to a fraudulent event driven by a consumer.

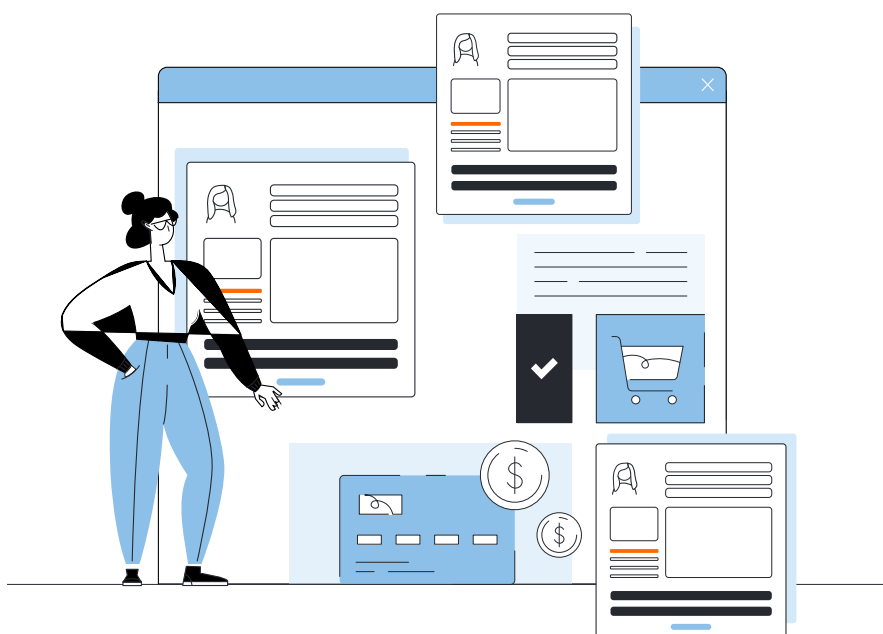
4 A standard definition helps establish more accurate data reporting and enables model development to cleanly target first-party fraud. This means that the industry can establish predictive signals to measure future fraudulent attempts, rather than trying to measure the “intent” of a consumer. These signals can be used to detect first-party fraud at new accounts, in real time during high-risk transactions, and even to help support consumer dispute investigation efforts.

First-party fraud is notoriously difficult to classify. Because there is not a consistent definition and fintechs and banks all label first-party fraud differently, we see poorly defined and labeled first-party fraud when analyzing data reported to Socure.

Our best analysis of Socure customers who provide performance feedback on fraud is that 30% of labeled third-party fraud is actually first-party fraud where the consumer has lied and said “I did not open that account.”



Without adopting a well-thought out, industry-wide standard definition, first-party fraud will continue to be misclassified as credit loss, third-party, or synthetic fraud, limiting any subsequent models in their ability to create predictive signals.



How you can participate in solving first-party fraud

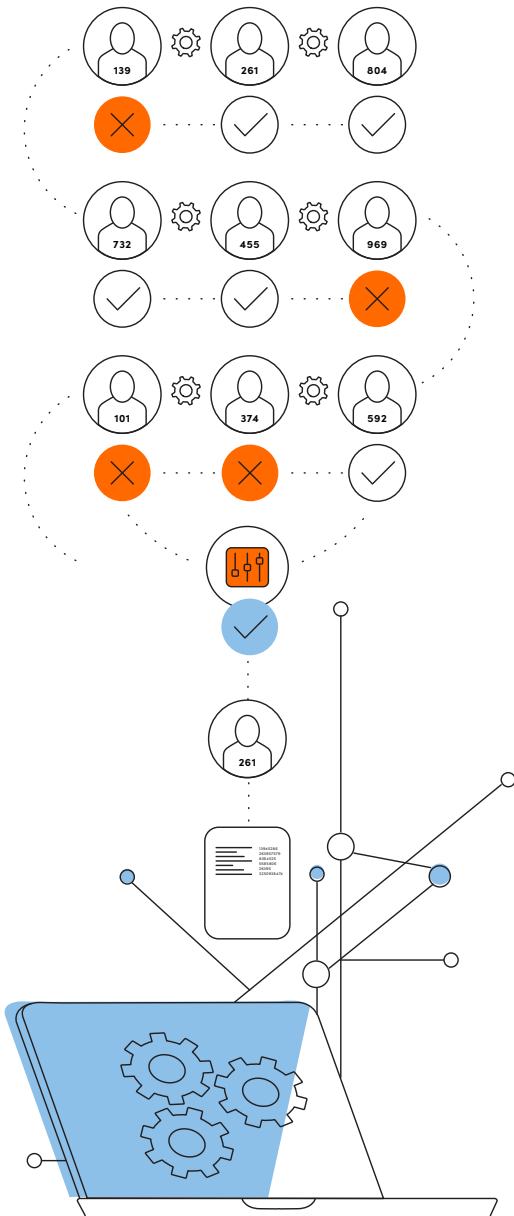
Using the power of collective intelligence across a consortium of financial institutions and merchants, Socure and our customers can begin to see the truth about consumer behavior in the data.

Fortunately, development of this consortium is already well underway and we are releasing a minimum lovable product (MLP) on October 18, 2023. Today the first-party fraud consortium, which receives data pursuant to GLBA consists of new application records with performance indicators, including first-party fraud tags, received from the majority of our 1,800+ customers.

We have also begun to include additional ACH, checking, and P2P transactional events, as well as deposits and other account behavior from a new set of consortium participants. This targeted first-party fraud data includes performance indicators and illegitimate disputes from hundreds of millions of events.

In the consortium, Socure has gathered, standardized, and formatted 36 months of historical data to enable a fast response to potential first-party fraud across high risk transactions, new accounts, and dispute investigations.

We are limiting the initial founding members to the first 15 invited companies who execute a simple agreement and integrate to a new "Sigma First-Party Fraud" module in our existing API, or establish a daily batch environment. These founding members are offered these unlimited services for free for one year, with a full batch run against their existing portfolios to better understand which of their existing customers will be most likely to participate in first-party fraud in the near future.



Taking the next step

First-party fraud is a complex and enduring issue rooted in deceit that demands a nuanced, collaborative approach to solve. Despite advances in fraud prevention technology, losses from first-party fraud continue near \$100 billion annually in the U.S. alone.

To make real and lasting progress on this persistent problem, financial institutions must align on an updated definition focused on verifiable fraudulent activities, not subjective determinations of intent that are difficult to prove.

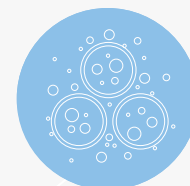
With a shared lexicon that classifies first-party fraud as a type of fraud rather than credit risk, the industry can begin normalizing data collection, reporting, and modeling methodologies. This will help reveal predictive insights into fraudster patterns across institutions. Equipped with enhanced consortium data and advanced analytics, financial institutions can deter fraud proactively at account origination through risk-based identity verification policies.

Unfortunately, there are several current regulatory loopholes that enable first-party fraud by allowing questionable practices like illegitimate credit washing, piggybacking on authorized user tradelines, and exploitation of Reg E dispute resolution timelines. As liability shifts related to authorized push payments loom on the horizon, carefully balanced policy updates that protect consumers while preventing fraud are needed. Updates should address blind spots that allow first-party fraud, while avoiding unintentional consequences that might disadvantage underserved groups.

Socure recommends the following path forward:

Socure research highlights the scale of the first-party fraud problem, with 35% of Americans admitting they've engaged in it at least once and 10% admitting to multiple types of fraud. The most common frauds are requesting refunds on received items (22%), not paying credit cards (21%), and disputing legitimate transactions (20%).

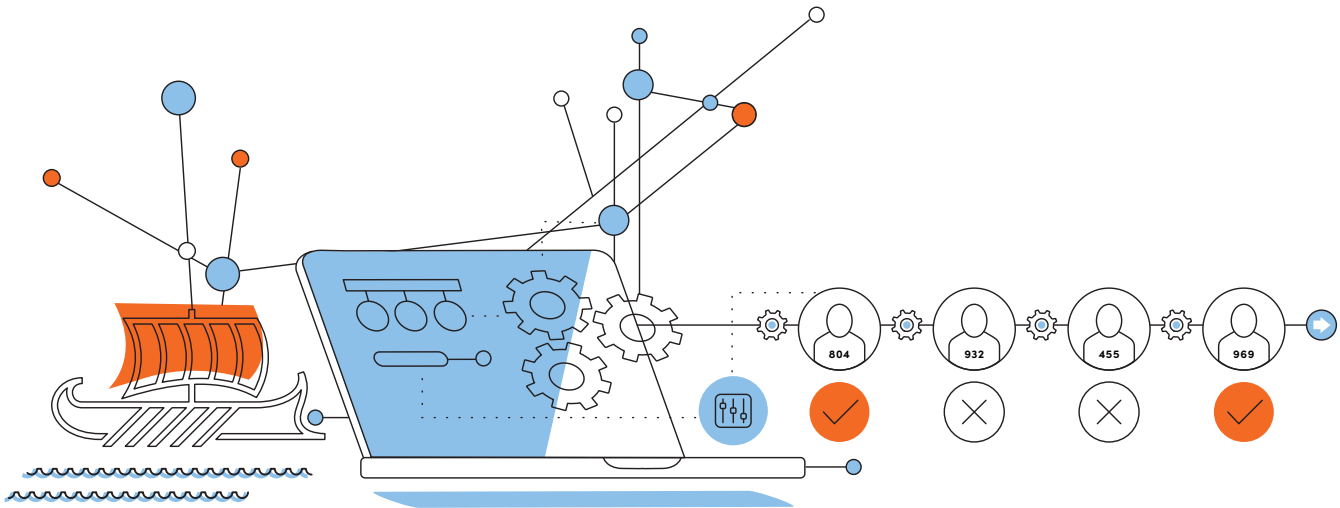
- Align on an updated industry definition of first-party fraud focused on verifiable fraudulent activities rather than subjective determinations of intent.
- Invest in cross-industry data sharing, modeling, and analytics techniques that reveal insights into fraudster patterns across institutions.
- Regulators should close loopholes enabling first-party fraud such as credit



With a shared lexicon that classifies first-party fraud as a type of fraud rather than credit risk, the industry can begin normalizing data collection, reporting, and modeling methodologies.

washing and piggybacking. In addition, we recommend amending the 1970 FCRA such that information related to fraudulent activities is exempted from the definition of a consumer report, which aligns with the GLBA protections against consumer opt-outs relating to the sharing of consumer information to detect fraud.

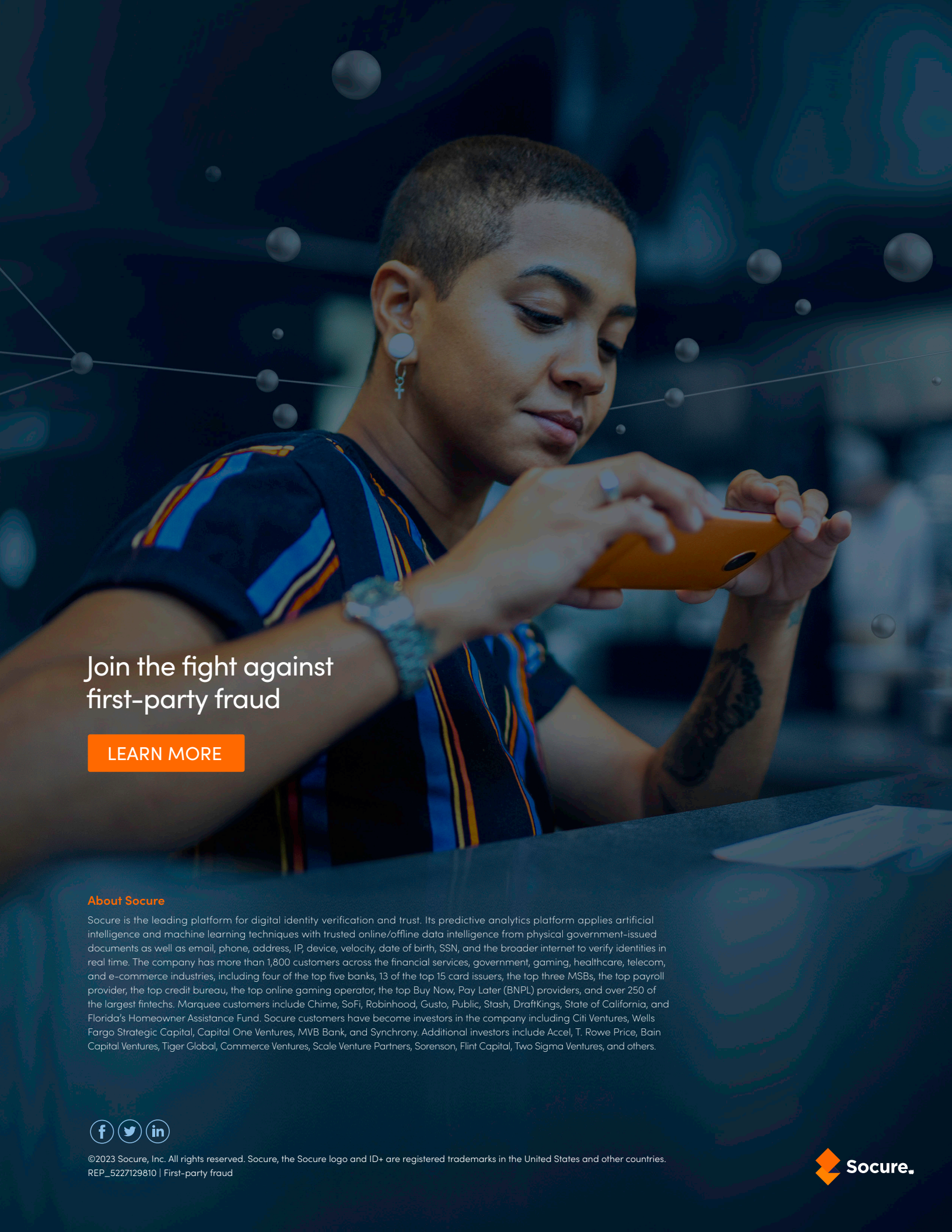
Long-term progress on first-party fraud also requires acknowledging its full scale and investing accordingly in pioneering techniques. Financial institutions have a unique window to get ahead of the incoming surge of first-party fraud attacks. By working together, we can develop enduring frameworks to detect and deter fraudsters while still providing value to legitimate consumers. Just as in 300 B.C., vigilance and communication is key to fighting this ancient challenge ■



Citations

*Socure conducted this research using an online survey prepared by Method Research and distributed by PureSpectrum among n=1,000 adults ages 18 - 77 in the United States. Respondents were evenly split on gender with a spread of ages and geographic location. Data was collected from October 1 to October 3, 2023.

1. Luttrell, C. (2018). The new fraud landscape: What it means for financial services. PaymentsJournal. Retrieved October 1, 2023, from <https://www.paymentsjournal.com/the-new-fraud-landscape-what-it-means-for-financial-services/?cmpid=Insightsblog-120920-solving-fraud-problem-first-party-fraud>
2. First-Party Fraud, and How To Prevent It? (2023, December 6). Diro. Retrieved October 1, 2023, from <https://diro.io/first-party-fraud/>
3. U.S. Credit Card ABS Charge-off Performance Deteriorates Further. (2023, March 14). FitchRatings. Retrieved October 1, 2023, from <https://www.fitchratings.com/research/structured-finance/us-credit-card-abs-charge-off-performance-deteriorates-further-14-03-2023>
4. DeVon, C. (2023, June 14). Americans owe nearly \$1 trillion in credit card debt—here's the breakdown by age. CNBC. Retrieved October 1, 2023, from <https://www.cnbc.com/2023/06/09/how-much-credit-card-debt-americans-hold-by-age.html>
5. Merchant chargebacks are on the rise due to friendly fraud. (n.d.). Javelin. <https://javelinstrategy.com/research/merchant-chargebacks-are-rise-due-friendly-fraud>
6. Deninzon, D., D'Silva, V., & Sood, R. (2018). Payment disputes in banking: A pathway to deeper customer relationships. McKinsey & Company. Retrieved October 1, 2023, from <https://www.mckinsey.com/industries/financial-services/our-insights/payment-disputes-in-banking-a-pathway-to-deeper-customer-relationships>
7. Consumer Sentinel Network Data Book 2022. (2023, February). Federal Trade Commission. Retrieved October 1, 2023, from <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022>
8. Sofastaj, M. (2023). Zelle's operator confirms fraud rule change, but current users lack recourse. WMAR 2 News Baltimore. Retrieved October 1, 2023, from <https://www.wmar2news.com/matterformallory/zelles-operator-confirms-fraud-rule-change-but-current-users-lack-recourse>
9. Ryan, C. (2023). Solving the Fraud Problem: What is First-Party Fraud? Experian Insights. Retrieved October 1, 2023, from <https://www.experian.com/blogs/insights/2020/12/solving-fraud-problem-first-party-fraud/>



Join the fight against first-party fraud

LEARN MORE

About Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from physical government-issued documents as well as email, phone, address, IP, device, velocity, date of birth, SSN, and the broader internet to verify identities in real time. The company has more than 1,800 customers across the financial services, government, gaming, healthcare, telecom, and e-commerce industries, including four of the top five banks, 13 of the top 15 card issuers, the top three MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers, and over 250 of the largest fintechs. Marquee customers include Chime, SoFi, Robinhood, Gusto, Public, Stash, DraftKings, State of California, and Florida's Homeowner Assistance Fund. Socure customers have become investors in the company including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, and Synchrony. Additional investors include Accel, T. Rowe Price, Bain Capital Ventures, Tiger Global, Commerce Ventures, Scale Venture Partners, Sorenson, Flint Capital, Two Sigma Ventures, and others.



©2023 Socure, Inc. All rights reserved. Socure, the Socure logo and ID+ are registered trademarks in the United States and other countries.
REP_5227129810 | First-party fraud

