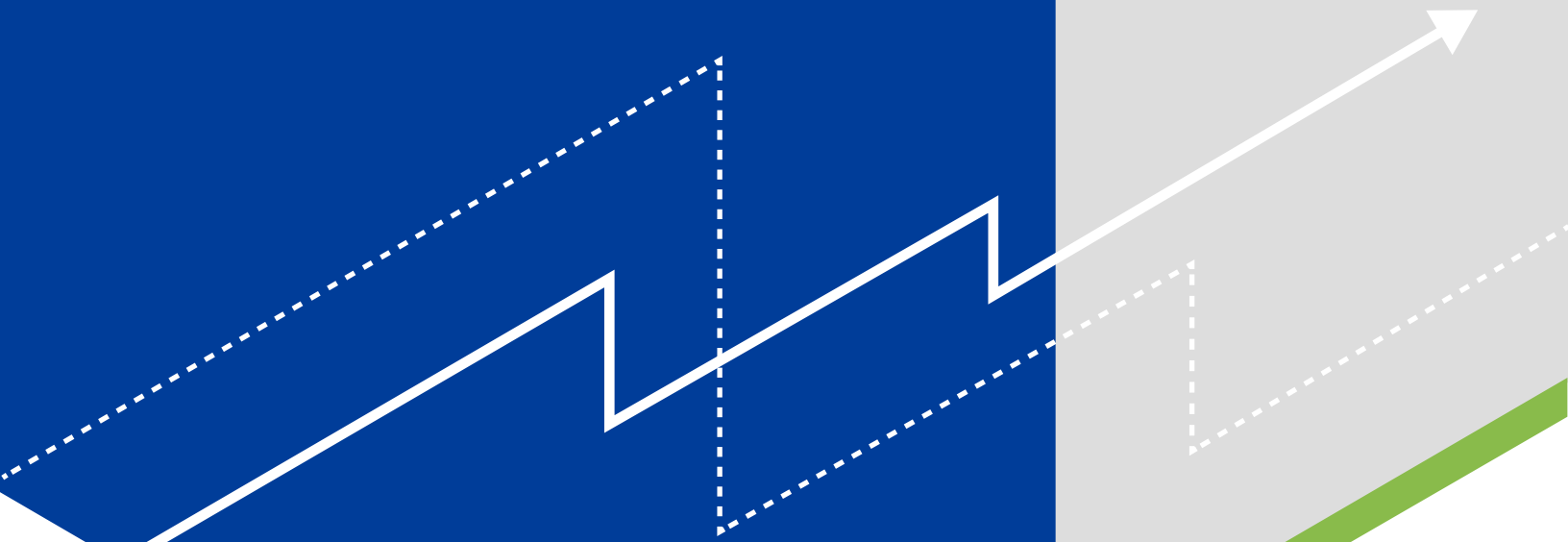
A Forrester Consulting
Thought Leadership Paper
Commissioned By ID.me

April 2017

Bridging The Gap Between Customer Experience And Fraud Prevention

The Fight Against Fraud Demands Robust Identity Verification And Authentication



FORRESTER®

Table Of Contents

Project Director:
Heather Vallis,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

As consumers spend more time online and engage with organizations more frequently through digital channels, criminals are also increasing the rate of digital identity theft and fraud. It's estimated that the incidence of identity fraud across US consumers increased by 16% in 2016 compared with the previous year.[1] The financial cost to consumers also saw a significant bump, increasing by nearly $1 billion over 2015. But the financial cost is just one aspect of loss for identity fraud victims — there is also an emotional toll and time invested to resolve associated issues.

Identity fraud is a two-sided issue — the organizations that serve consumers share the pain of identity theft and fraud. The cost of identity fraud to US businesses is estimated to be tens of billions of dollars a year.[2] The bigger costs, however, are in brand perception, damage to the customer relationship, and loss of productivity. Despite the substantial harm, the aging tools organizations use to tackle identity theft and fraud are less and less effective as fraudsters become more sophisticated. Today's organizations are challenged to implement effective identity verification (IDV) without detracting from the customer experience.

In December 2016, ID.me commissioned Forrester Consulting to evaluate the impact of identity fraud on US consumers as well as the measures that financial services, financial technology (fintech), and government organizations are taking to curtail identity theft and fraud. As part of this effort, Forrester Consulting surveyed 2,016 online US consumers and 300 decision makers from financial services, fintech, and government organizations.

KEY FINDINGS

- **Both consumers and businesses endure fraud attacks without sufficient tools for prevention.** Nine out of 10 consumers fear fraudulent use of their data, but only 16% feel they have complete control over their data. Meanwhile, common types of fraud cost businesses upward of $11 million. Combined with an overreliance on outdated tools, the risk to consumers and businesses is likely to grow.
- **Organizations struggle to balance ease of ID verification with strength of protection.** Even while consumers worry about their identity online, their expectation for easy digital experience increases. As a result, companies rely on the least secure, yet widely accepted, forms of verification. The widening gap between strength and ease of use leaves consumers and organizations vulnerable.
- **Federated ID verification with a single sign-on (SSO) reduces risk of fraud while improving consumer experience.** Eighty-five percent of decision makers surveyed believe federated IDV will reduce their risk of ID theft and fraud. When combined with SSO, 82% of consumers are willing to use it to confirm their identity. It's no wonder then that 88% of organizations will implement this technology within three years.

Identity Fraud Is A Growing Issue

Today's consumers are firmly ensconced in the digital age. They are empowered by technology and engage with organizations that deliver what they need, when they need it, regardless of the delivery mechanism or channel. In our survey of online US consumers, 83% reported they go online for personal reasons several times a day; another 15% are online on a daily basis.[3] But as consumers spend more and more time online, it has become much easier for fraudsters to steal consumer identities and commit fraud. The number of identity fraud victims has increased dramatically over recent years, from 11.6 million in 2011 to 15.4 million in 2016, with losses estimated at $16 billion last year.[4]

Identity fraud cost US consumers **$16 billion in 2016.**

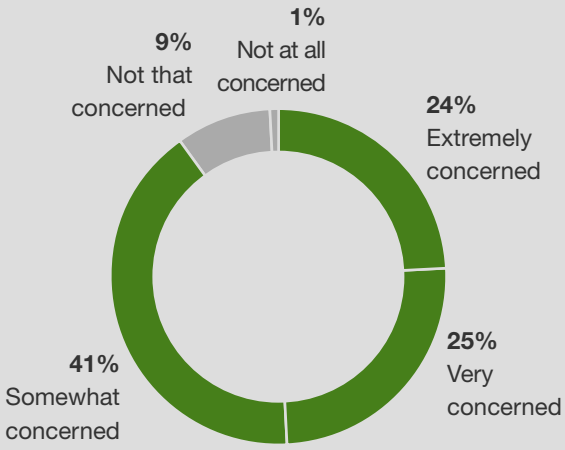
CONSUMERS ARE CONCERNED WITH IDENTITY THEFT BUT LACK THE MEANS TO PREVENT IT

The threat of identity theft is not lost upon consumers. Our study found that:

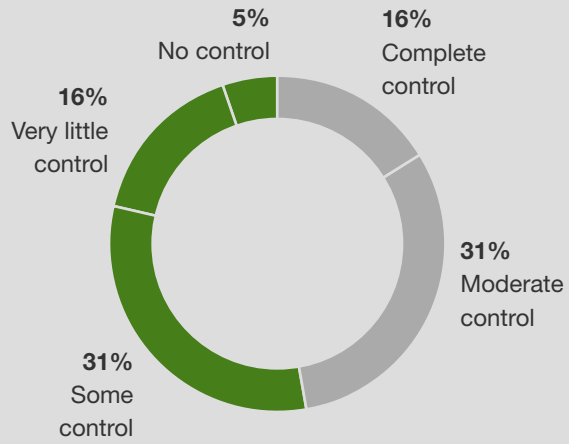
- **Fear of identity theft is widespread. . . .** Ninety percent of consumers are concerned that their personal information will be stolen for fraudulent purposes, with nearly half indicating they are very or extremely concerned (see Figure 1).
- **. . . . but many feel they lack control.** Over half of consumers surveyed felt they had, at the most, only some control over protecting their personal information; just 16% felt they had complete control over their personal data.

Figure 1

"How concerned are you that your personal information will be stolen and used for fraudulent purposes?"



"How much control do you feel you have over protecting your personal data or information?"



Base: 2,016 US consumers who go online at least once per week
(Percentages may not total 100 because of rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

FORRESTER®

As a result, many consumers are taking passive measures to protect their personal information, including regularly checking bank or credit card statements and credit reports (see Figure 2). While monitoring accounts is indeed an important step to take, it is a reactive — rather than preventative — measure, doing little to reduce the risk of identity theft. Far fewer consumers are taking proactive measures to protect their information, such as activating two-factor authentication, using privacy protection tools, or using a mobile app for additional identity authentication.

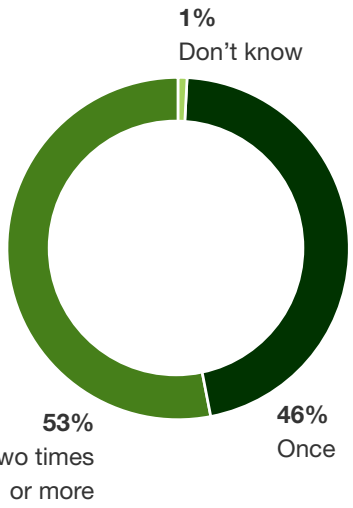
Some of the most commonly used methods to protect personal information are **reactive** rather than **preventative**.

VICTIMS OF IDENTITY THEFT OFTEN SUFFER REPEATED ATTACKS

Our study found that over one out of three consumers have been victims of identity theft: 37% of US consumers surveyed indicated their identity or personal information had been stolen — 21% within the past 24 months. For many, identity theft is not a one-time occurrence. Over half of recent victims reported their identity had been stolen two or more times over a two-year period (see Figure 3). Unauthorized use of an existing account (55%) and new account fraud (32%) were the most common types of misuse of personal information among victims.

Figure 3

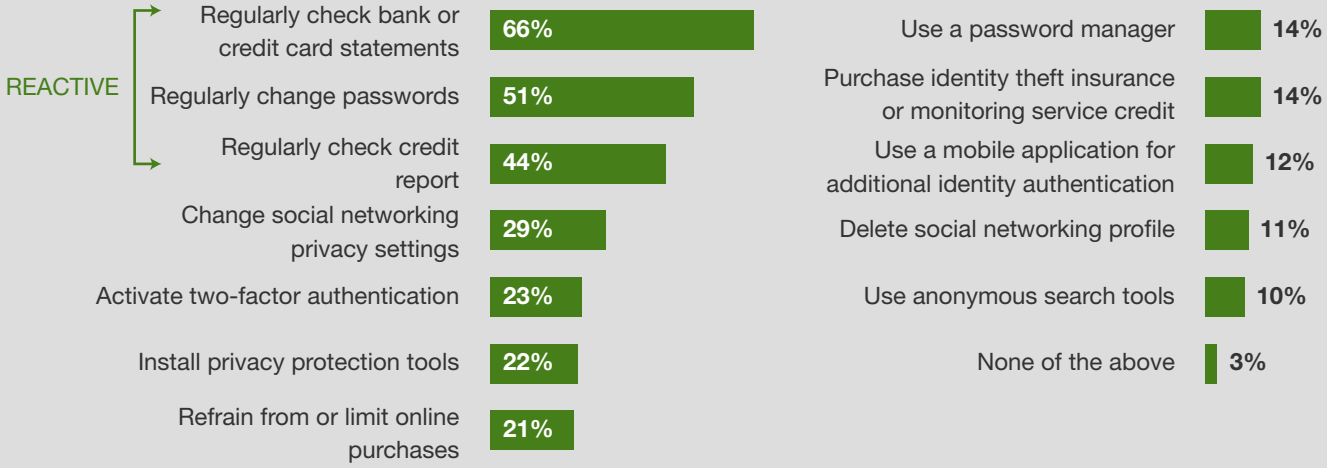
"Approximately how many times over the past 24 months have you been a victim of identity theft?"



Base: 426 US consumers who had their identity stolen in the past 24 months
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

Figure 2

"What measures are you taking to protect your personal information?" (Select all that apply)



Base: 2,016 US consumers who go online at least once per week
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

FORRESTER®

IDENTITY THEFT TAKES A TOLL ON VICTIMS

For victims, the cost of identity theft goes beyond the financial loss. It takes time to resolve incidents of fraud, and for many, it can be an emotionally taxing ordeal. Our study revealed:

- **Victims suffer significant financial loss.** Of those who had their personal information stolen within the past 24 months, 59% reported $100 or more in direct financial loss, that is, the estimated value of goods, services, or cash obtained as a result of the incident. But victims must also absorb indirect financial losses like legal fees or bounced checks. Fifty-nine percent reported indirect losses of $100 or more.
- **Resolving incidents takes time.** It is rare for an incident of identity theft to occur and for a victim to not encounter subsequent issues: Just 6% of identity theft victims surveyed were issue-free. When there are issues, victims can spend days, weeks, and even months resolving them. While the majority said it took up to a week to deal with the fallout from identity theft incidents, 35% spent more than a week dealing with problems, and for 4%, issues have gone unresolved.
- **ID theft takes an emotional toll.** When asked how stressful it was to learn their personal information had been stolen, 87% said it was a stressful experience, with 42% reporting it was extremely stressful.

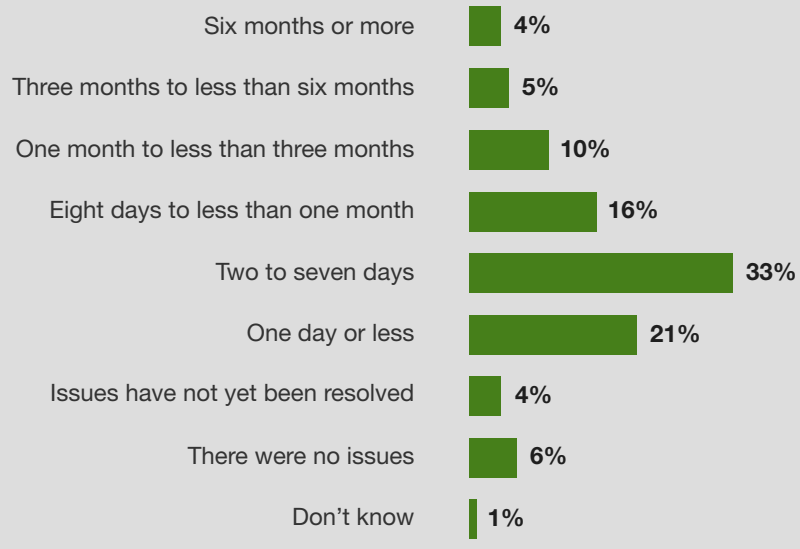
Identity theft is an extremely stressful experience for **42% of victims.**

"Students are really at a disadvantage when these things happen. If [their PII] got published it would be bad. . . . Here, students have the greatest risk and have full careers ahead of them. They won't have the benefit of resources, like legal protection, if something goes wrong."

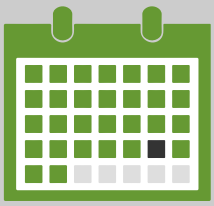
Director of IT, US federal agency

Figure 4

"Thinking about your most recent incident where your identity or personal information was stolen or compromised, how long did it take you to resolve issues associated with the incident?"



Base: 426 US consumers who had their identity stolen in the past 24 months
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017



It took **35%** of identity theft victims **over a week to resolve issues.**

FORRESTER®

ORGANIZATIONS SHARE THE PAIN OF ID THEFT AND FRAUD

While the impact of identity theft and fraud is considerable for consumers, on the other side of the coin are the organizations that are trusted with the stewardship and security of that personal information. When data breaches occur, they compromise consumers' names, addresses, DOBs, SSNs, usernames, passwords, and credit card numbers. This has raised the risk of identity theft and fraud: 51% of decision makers at the financial services, fintech, and government organizations included in our study reported an increase in risk compared with the previous year.

Our study results show that this feeling of elevated risk is not unfounded: 76% of financial services, 68% of fintech, and 62% of government organizations reported they had experienced fraud involving the use of customer or citizen data in the past 12 months. Regardless of sector, fraudsters most commonly used personally identifiable information (PII) (60%) and payment or credit card data (57%) to perpetuate incidents of fraud. Unfortunately, many organizations aren't aware that consumer data has been compromised until notified by an external party.[5]

When asked to identify the types of fraud perpetuated over the past year, financial services and fintech firms pointed to credit card application fraud, new banking account or synthetic identity fraud, and check fraud as most common. Top fraudulent incidents for government agencies included government benefits fraud, account takeover fraud, and improper payments (see Figure 5).

51% say their organization's **risk of identity theft and fraud has increased.**

THE COST OF IDENTITY FRAUD FOR ORGANIZATIONS CAN BE STAGGERING

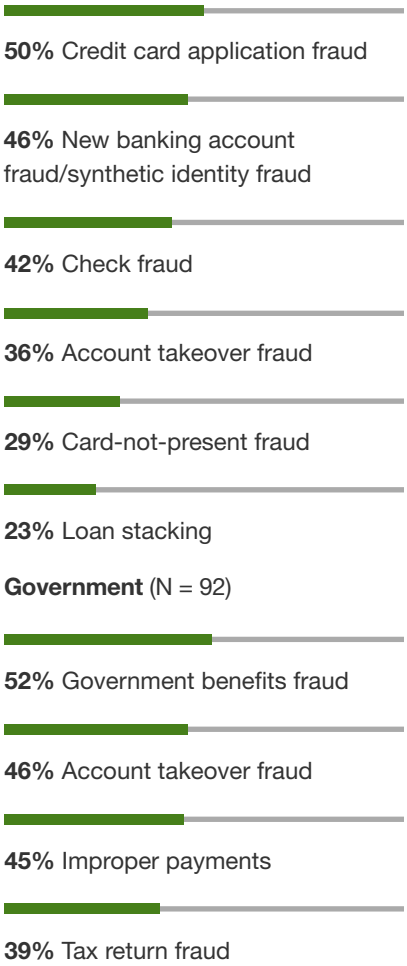
The high cost of fraud takes away from the bottom line. The cost of identity fraud to US businesses is estimated to be in excess of $50 billion a year.[6] Our study found that when accounting for both tangible and intangible losses associated with fraud, many organizations reported annual losses in excess of $11 million. For financial services and fintech organizations, loan stacking, card-not-present, and new account or synthetic identity fraud packed the greatest financial punch (see Figure 6). For government, tax return fraud has by far the greatest financial impact: Three-quarters of organizations experiencing this type of fraud suffered losses in excess of $11 million.

The cost of identity fraud to US businesses is **estimated to exceed $50 billion a year.**

> "I would say we are pretty secure. However, we only know when PII gets published. If it's out there, but not published, we don't know."
>
> *Director of IT, US federal agency*

Figure 5

Types of Fraud

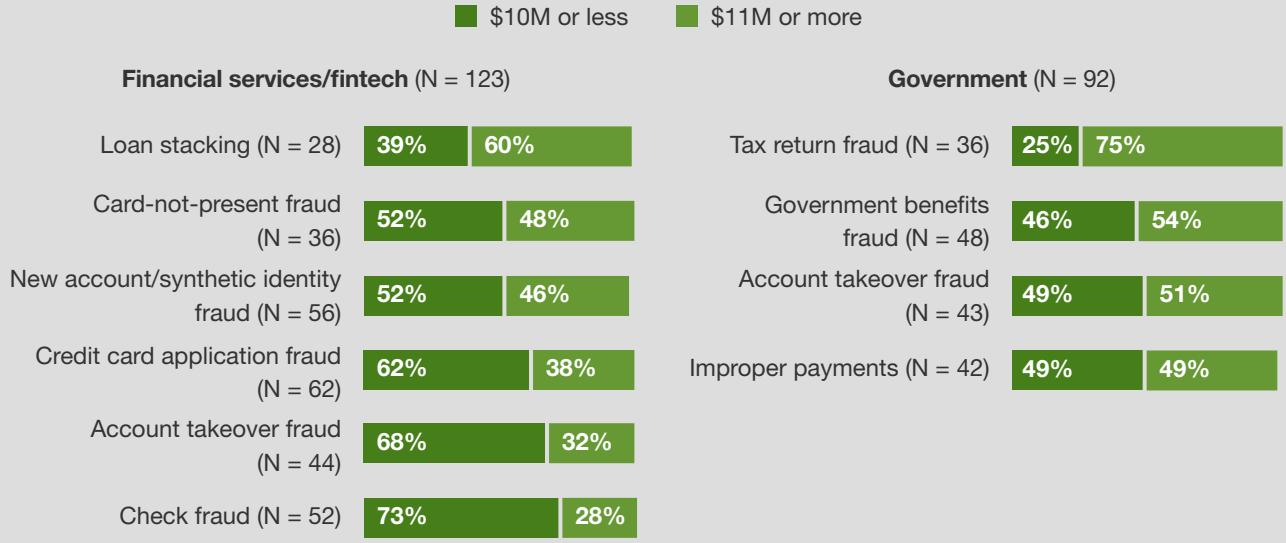


Base: Decision makers at US-based government, financial services, and fintech organizations that experienced fraud in the past 12 months
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

FORRESTER®

Figure 6

"Thinking about both the tangible and intangible, for each type of fraud experienced, what was the approximate total annual loss for your organization?"



Base: varies; decision makers at US-based government, financial services, and fintech organizations that experienced each type of fraud in the past 12 months (Percentages may not equal 100 due to rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

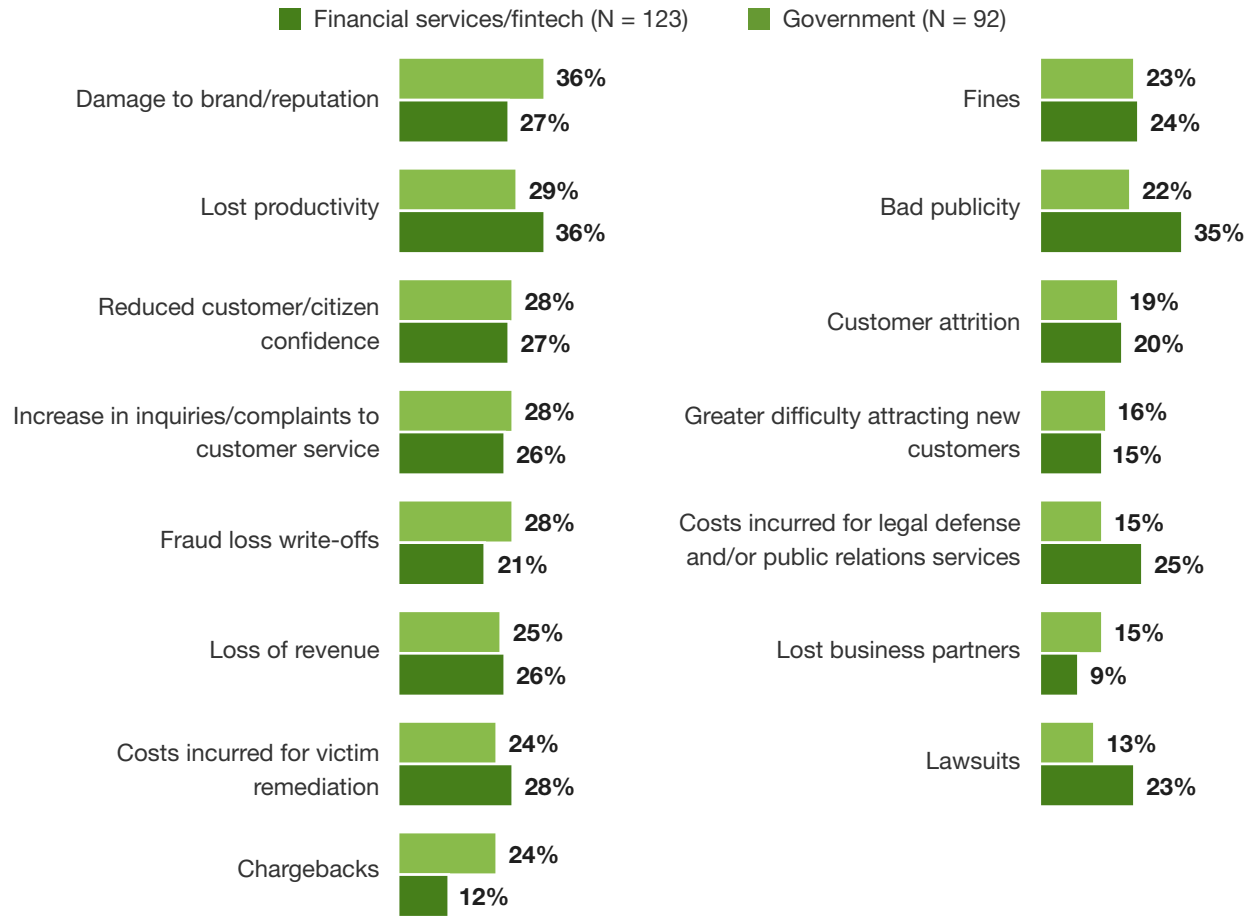
The implicit cost of fraud affects more than the bottom line — it affects how organizations do business and how they are perceived. While organizations experiencing fraud in the past 12 months reported financial fallout such as costs incurred for victim remediation, loss of revenue, fraud loss write-offs, and fines, the bigger costs are in brand perception, damage to the consumer relationship, and a loss of productivity (see Figure 7). While the financial sector (including both financial services and fintech) was more likely to suffer damage to reputation as a result of fraud, government agencies were more likely to report a loss of productivity and bad publicity.

The **implicit cost of fraud** affects more than the **bottom line** — it affects **how organizations do business and how they are perceived.**

FORRESTER®

Figure 7

"What impact did this incident or incidents of fraud have on your organization?"



Base: Decision makers at US-based government, financial services, and fintech organizations that experienced fraud in the past 12 months
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

Today's Battle Against Fraud Can't Be Fought With Yesterday's Tools

Given the high stakes of identity fraud, it comes as little surprise that the pressure to reduce fraud is mounting for the vast majority of organizations: 93% of decision makers in our study reported their organizations are making it a high or top priority. But implementing measures to counter identity theft and fraud is no easy task, with incumbent approaches hindering both effectiveness as well as the user experience. Our study identified challenges around:

- **Reliance on legacy methods.** The tools used by organizations today to combat identity theft and fraud are insufficient to counter the sophisticated measures fraudsters use today. While static identifiers are easily breached, rendering them useless, solely relying on credit-file header data is not enough to protect against fraud. Traditional tools are also limited in their ability to recognize new fraud patterns and lack the flexibility to adjust in real time (Figure 8).
- **User experience.** Organizations reported issues with users remembering login information and a poor experience due to complicated authentication processes.

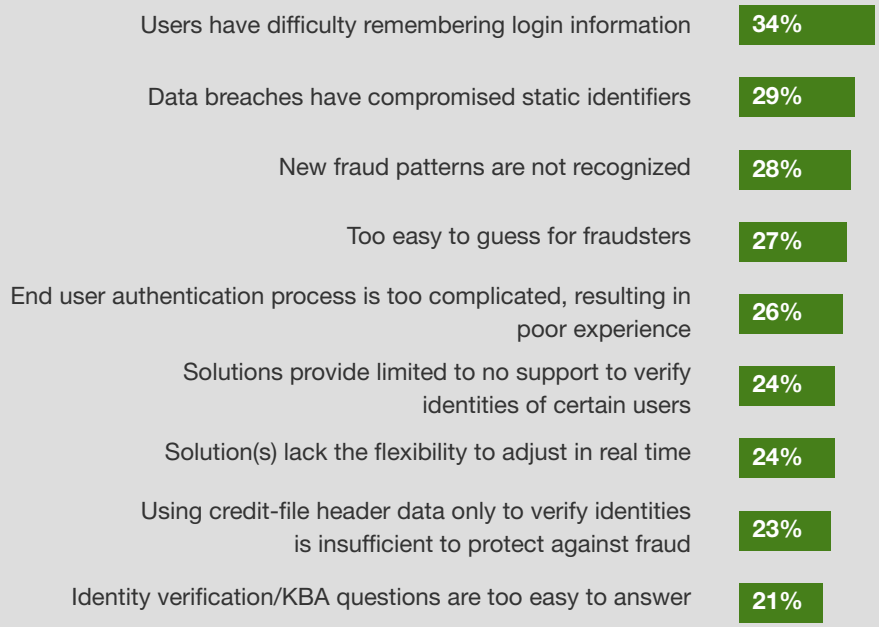
93% of organizations are prioritizing the **prevention and reduction of identity fraud.**

"If [a fraudster] logs into my account, and we don't analyze it for six hours, the damage is already done. We are monitoring, but we are behind 6 to 8 hours. If it was real time and we had more resources while the fraud was happening, we could mitigate the risk."

Vice president, information risk management, at a large US financial services firm

Figure 8

"What are the top challenges you've encountered implementing anti-identity theft and fraud measures?"



Base: 319 decision makers at US-based government, financial services, and fintech organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

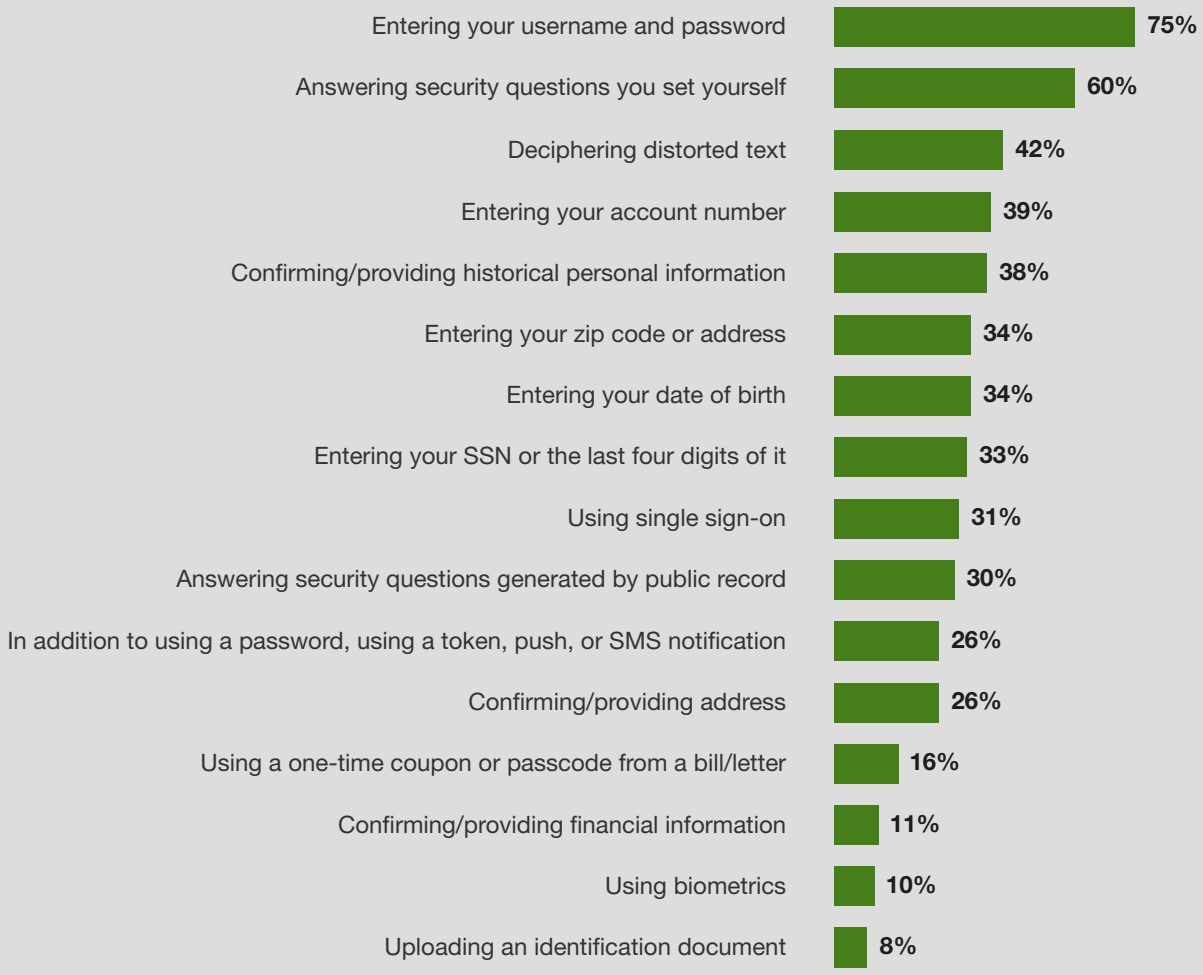
FORRESTER®

ORGANIZATIONS STRUGGLE TO BALANCE EFFECTIVE IDENTITY VERIFICATION WITH USER EXPERENICE

Organizations still rely on dated practices, many of which are ill-equipped to counter fraud. Consumers are presented with many different ways to verify their identities online; however, the predominant verification methods employed by organizations still include entering a username and password and answering user-defined knowledge-based authentication questions (KBA) (see Figure 9). But simple usernames and passwords are easy for fraudsters to crack, and with the proliferation of personal information available via social networks, self-asserted KBA questions are a less-than-bulletproof approach. It is far less common for organizations to present consumers with more advanced methods, such as two-factor or multifactor authentication or biometrics.

Figure 9

"Thinking about the websites for which you have registered a personal account or identity, what approaches do they use to verify your account or identity?"



Base: 1,987 US consumers who registered for an online account
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

FORRESTER®

The challenge, of course, is to strike the right balance between effective verification and the user experience. Current verification processes create friction with customers and establish a false sense of security. For example, the consumers we surveyed are quite willing to enter a username and password or answer self-asserted KBA questions and find these approaches relatively easy to navigate and trustworthy; however, as mentioned above, their trust in these methods is largely misplaced (see Figure 10). Conversely, consumers find biometrics easy to navigate and trust in this approach, but they are seldom presented with this method of authentication.

> "Forty percent of the complaints we get are for inconvenience because [the customer] has to do two-factor authentication. They ask, 'Why do I have to use my phone when I'm using this? Why do I have to enter an additional number? Why is my PIN not enough?' Those are the kind of complaints we get."
>
> *Vice president, information risk management, at a large US financial services firm*

Figure 10

Verification processes create friction with consumers and a false sense of security

	Rank (by average rating)			
Methods	Use	Willingness to use	Ease of use	Trustworthiness
Entering your username and password (N = 1,493)	1	2	6	8
Answering security questions you set yourself (N = 1,183)	2	1	8	3
Deciphering distorted text (N = 844)	3	5	14	13
Entering your account number (N = 771)	4	12	11	10
Confirming/providing historical personal information (N = 756)	5	7	9	7
Entering your date of birth (N = 684)	6	10	1	14
Entering your zip code or address (N = 668)	6	9	2	16
Entering your SSN or the last four digits of it (N = 663)	8	16	5	9
Using single sign-on (N = 611)	9	8	3	15
Answering security questions generated by public record (N = 597)	10	13	13	12
Confirming/providing address (N = 509)	11	11	7	11
In addition to using a password, using a token, push, or SMS notification (N = 508)	11	4	12	2
Using a one-time coupon or passcode from a bill/letter (N = 310)	13	6	10	6
Confirming/providing financial information (N = 223)	14	14	15	4
Using biometrics (N = 199)	15	3	4	1
Uploading an identification document (N = 156)	16	15	16	5

Base: 1,987 US consumers who registered for an online account
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

ORGANIZATIONS SEEK TO BUILD ON EXISTING CAPABILITIES

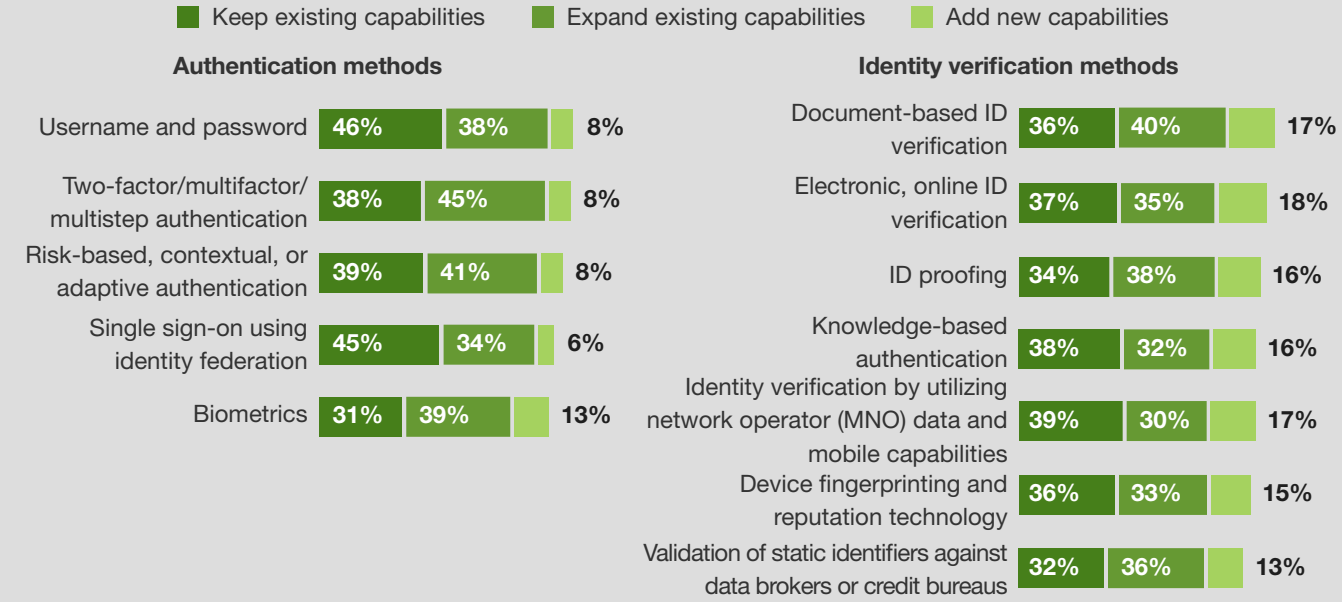
In order to effectively combat fraud, organizations need to implement true verification, not just a false sense of security. Identity verification mitigates the risk of identity fraud by verifying identity at the initial setup stage and as an added layer of authentication for subsequent use to establish a required level of confidence that the presented identity information and/or credentials are legitimate. Our study found that organizations are expanding on both authentication and verification methods, which is a definite step in the right direction:

› **Organizations are expanding on both traditional and advanced authentication methods.** The good news is that organizations are taking measures to build out their authentication capabilities, with two-factor/multifactor authentication, biometrics, and risk-based authentication as key areas of expansion (see Figure 11). However, many are still hanging their hat on the use of usernames and passwords, despite just 39% of decision makers reporting this method is very effective at reducing identity theft and fraud.

› **Identity verification is part of a multilayered fraud management strategy.** There is no silver bullet when it comes to IDV — no one method offers complete protection against identity theft and fraud. The organizations in our study seemed to grasp this concept, with the majority employing multiple IDV methods. While many are expanding or adding tried-and-true IDV approaches — such as document-based verification and KBA — still others are building out their ID proofing, online ID verification, and device fingerprinting and reputation capabilities.

Figure 11

"What are your organization's plans for the following authentication and identity verification methods?"



Base: 319 decision makers at US-based government, financial services, and fintech organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

FORRESTER®

Organizations Need To Move Beyond "Fill In The Gap" Strategies

Of course, using multiple solutions to build a comprehensive identity verification strategy is no easy task. Disparate systems are difficult to integrate and often leave gaps in capabilities.

The organizations we surveyed are looking for an identity verification solution that can truly do it all — including real-time identity verification, multifactor authentication, and the ability to support both in-person and remote identity verification flows — without hurting the customer digital experience (see Figure 12).

The top requirement identified by study respondents, however, was that an identity verification provider (IdP) is certified under federal government standards as a trusted identity solution. Indeed, nearly two-thirds of those surveyed reported that their organization is currently outsourcing (22%) or highly likely to outsource (42%) IDV to a federally accredited IdP.

The federal government plays a critical role as a standards-setting body. Founded in 2015 as part of the National Institute of Standards and Technology's (NIST's) Applied Cybersecurity Division, the Trusted Identities Group (TIG) promotes government and commercial adoption of privacy-enhancing, secure, interoperable, and easy-to-use digital identity solutions.[7] In alignment with the "National Strategy For Trusted Identities In Cyberspace," outlined in 2011, TIG works to advance standards adoption to improve digital identity. To date, TIG's Pilot Program has convened more than 170 organizations to work together in advancing trusted digital identity solutions.[8]

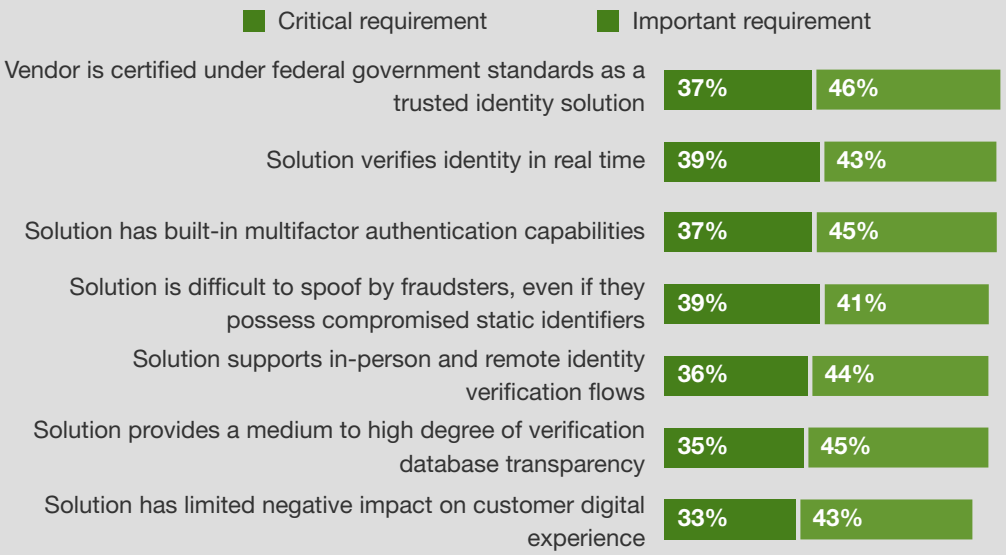
64% of organizations outsource or are highly likely to **outsource IDV to a federally accredited IdP.**

"We do not have a single solution. Implementing between them was a challenge. We had to change a lot of software to get the correct requirements. . . . We needed three different [types of] software from one vendor to get it to talk to the other vendor."

Director of IT, US federal agency

Figure 12

"How important are the following capabilities in an identity verification solution or provider?"



Base: 319 decision makers at US-based government, financial services, and fintech organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

FORRESTER®

Federated IDV With Single Sign-On Bridges Access And Fraud Prevention

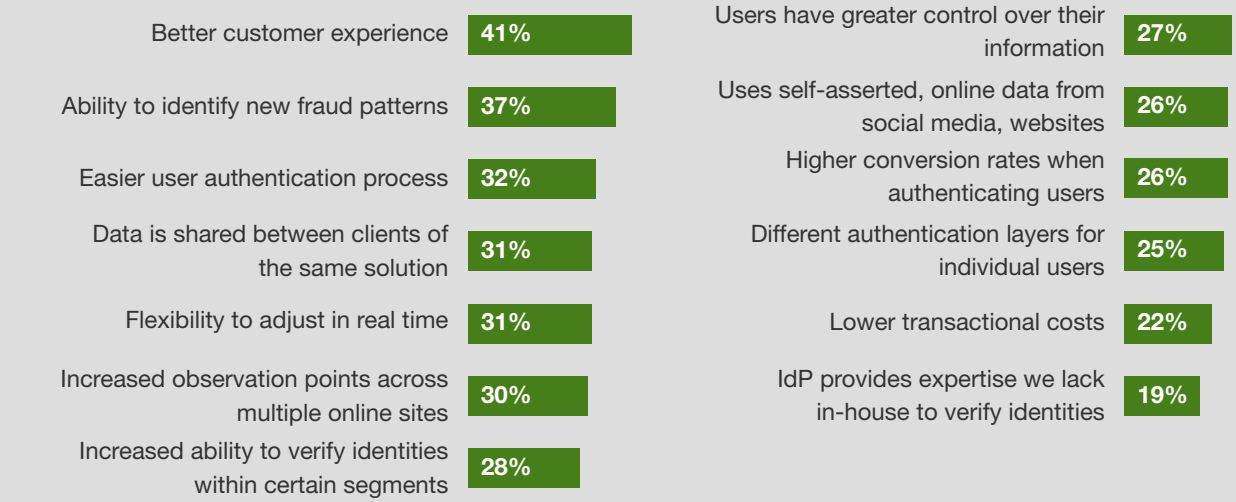
Federated identity verification is not a new concept. Federated identity verification is when an IdP performs the ID verification steps and then a relying party (RP) or service provider (SP) organization or application can rely on the already vetted identity that the IdP provides. The resulting certified single sign-on can be used on multiple online sites, eliminating the need for users to create new logins at each site they visit and repeatedly go through identity verification measures. Online users encounter federated identity verification every time they are prompted to log on or access a website or online application using their social media identity.

Federated identity verification presents an option that does not have an access versus fraud tradeoff, providing the ability to ensure the accuracy, security, and privacy of users' personal identification while minimizing the friction typically encountered with more traditional verification measures. Customers stand to gain an improved experience and authentication process, with greater control over their information and fewer logins to manage. Among the consumers surveyed, 82% indicated they would be "mildly" to "very willing" to use a federated IDV with SSO. On the flip side, federated IDV with SSO provides organizations with improved verification capabilities as well as the ability to identify new fraud patterns (see Figure 13). In fact, 85% of decision makers said federated IDV with SSO would reduce their organizations' risk for identity theft and fraud.

85% of decision makers say **federated IDV with SSO would reduce** their organizations' **risk for identity theft and fraud.**

Figure 13

"What are or would be the benefits of using a federated identity verification solution with single sign-on (SSO), where users can bring their verified identity to multiple online sites?"



Base: 310 decision makers at US-based government, financial services, and fintech organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ID.me, February 2017

FORRESTER®

And while just 29% of the financial services, fintech, and government organizations surveyed have already implemented federated IDV with SSO, there will be an increase in adoption over the next three years. Fifty-two percent of those surveyed plan to implement federated IDV with SSO within the next 12 months, with another 7% planning adoption within the next 24 to 36 months.

88% of organizations plan to have **federated IDV with SSO** in place **within the next three years.**

Digitized businesses with digital delivery of goods and services increasingly need to meet requirements of “faceless” (i.e., online) customer identity verification and authentication. Old-style and in-house-developed methods (using only credit file header-based identity verification and in-house-developed enrollment and authentication portals) are not only expensive but also inaccurate and nonrepeatable. Federated IDV embedded into a robust access policy enforcement process not only helps with stepping up an organization’s security game but also aids in improving the customer experience, helping to win, serve, and retain more customers.

Key Recommendations

To implement federated IDV, Forrester recommends that you:

Unify business and security data management. Having separate repositories of business information (such as delivery addresses and marketing list preferences) and security information (such as passwords, notification email addresses, and notification mobile numbers) leads to confusion and inconsistencies in managing these two data sets. Forrester recommends that you tie these data sets together at the time of customer identity verification.

Factor in system integration costs early on. Using a vendor solution for federated IDV and authentication is only the first step in creating an industrial-strength customer-facing identity management system. Forrester sees many firms struggle with customer identity and access management (CIAM) project delays because they forget to take into account the effort of integrating their existing transactional and identity data with the next-generation IDV platform.

Create and track proxy measures for the customer experience. Any implementation of federated IDV should have a good understanding of your baseline: your customers' abandon rates, unsuccessful registration rates, and login rates. As you implement any changes to your IDV processes, you should very carefully monitor these proxy measures and detect and correct any detrimental moves in them.

Do not count on rules as the next generation of policy management. Rule maintenance for identity verification and risk-based authentication is costly, inaccurate, and slow and does not fight fraud effectively enough. Seek to implement solutions that augment rule-based risk scoring and decisioning with machine learning and artificial intelligence methods (detecting baseline behaviors and then flagging and intercepting anomalies from them).

Appendix A: Methodology

In this study, Forrester conducted an online survey of 2,016 online US consumers and 319 executives at financial services, financial technology, and government organizations in the US to evaluate the impact of identity theft and fraud and the measures organizations are taking to reduce risk. Participants in the financial services, financial technology, and government survey included decision makers at the director level and above involved with risk management, fraud prevention, identity access management, security, governance, or compliance at their organizations. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in January 2017 and was completed in February 2017.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

"Breakout Vendors: Social Identity and Eligibility Verification (SIDEV)," Forrester Research, Inc., November 21, 2016

"The Future Of Identity And Access Management," Forrester Research, Inc., October 25, 2016

"Vendor Landscape: Identity Verification Solutions," Forrester Research, Inc., September 22, 2015

Appendix C: Endnotes

[1] Source: Al Pascual, Kyle Marchini, and Sarah Miller, "2017 Identity Fraud: Securing the Connected Life," Javelin Strategy & Research, February 1, 2017 (https://www.javelinstrategy.com/coverage-area/2017-identity-fraud).

[2] Source: CSID (https://www.csid.com/resources/stats/cost-of-identity-fraud/).

[3] In order to participate in the study, respondents to the consumer study had to be at least 18 years of age, reside in the US, and go online for personal purposes at least once a week.

[4] Source: Al Pascual, Kyle Marchini, and Sarah Miller, "2017 Identity Fraud: Securing the Connected Life," Javelin Strategy & Research, February 1, 2017 (https://www.javelinstrategy.com/coverage-area/2017-identity-fraud).

[5] Source: "Verizon's 2016 Data Breach Investigations Report," Verizon (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/).

[6] Source: CSID (https://www.csid.com/resources/stats/cost-of-identity-fraud/).

[7] Source: NIST's Trusted Identities Group (TIG) (https://www.nist.gov/itl/tig/about).

[8] Source: NIST's Trusted Identities Group (TIG) (https://www.nist.gov/itl/tig/pilot-projects).