IDOLOGY

IDology 2015 Fraud Report

Survey Result Highlights

- Suspected fraud attempts continue to climb
- Fraudsters continue to target website applications
- Mobile and call center fraud intensifies
- Volume of activity through mobile devices grows
- Account takeover via porting, ANI spoofing and device cloning top mobile fraud tactics
- Level of investment on mobile expected to increase
- Phishing and information theft become more widespread
- Organizations shift their focus in order to detect and prevent evolving fraud techniques
- Recon & social engineering lead call center fraud schemes
- Shifting fraud tactics remain a challenge
- Growing concerns about fraud prevention resources
- Suspected small dollar fraud attempts give way to larger sums
- New geographic regions emerge as centers of suspected fraud
- Ease of implementation, ability to meet compliance requirements, reduction of manual review, higher locate rates and increased customer acquisition top IDology customer benefits, among others

Fraud Trend:

"Fraud schemes over the last 12 months have been a combination of enrollment fraud and account takeover."

~ VP of Risk & Compliance, Fortune 500, Financial Services Enterprise

About the Research

The IDology 2015 Fraud Survey polled senior executives from IDology's customer base. IDology customers come from a variety of industries – from banking and other financial services, to healthcare, retail, telecommunications, energy & utilities as well as other consumer and business services. Sizes of the companies range from large enterprise organizations to small business as well as non-profit and educational institutions.

Of those who responded, *23%* are senior C-level contacts, *29%* are VP/Director level contacts and *27%* are managers whose daily experiences revolve around ensuring a positive customer experience while still mitigating fraud. Additionally, *21%* of respondents were Analyst-level contacts.

This report brings together these survey results with the experience and expertise of IDology, a leading provider of multi-layered, end-to-end authentication and fraud prevention solutions that verify an individual's identity and age for organizations doing business in a customer-not-present environment.

IDOLOGY

Introduction

We are thrilled to be launching our 3rd annual fraud report. Thank you for your interest in the research. We hope you find this information beneficial as you continue to develop and expand your identity verification and fraud prevention programs.

Several years ago we came to the realization that identity proofing and data matching were no longer enough. As data breaches became more widespread and as fraud tactics continued to evolve, countless identities became available for sale on black markets that can be accessed, for example, on the dark web. The stolen data from these breaches, as well as other identity theft schemes, contain enough personal information on a consumer for a fraudster to accurately impersonate that individual. We call these compromised identities "perfect identities." This is where fraudsters capitalize - they can purchase a perfect identity and attempt to open or access financial accounts, file a tax return, submit a medical claim and much more. As a result, we came to a decision that IDology's solutions needed to innovate - and to continue to innovate - in order to ensure that our customers remain confident that their customer, "John Smith," really is John Smith and not a criminal.

IDology offers a collaborative and multi-layered identity verification and fraud prevention platform that allows customers to take a "deeper dive" than what simple identity verification affords. We are able to look at multiple factors - from identity to device, location, activity and more in order to evaluate risk based on an organization's individual business requirements. Customers can then dynamically decision to escalate a transaction to a higher level of verification based on this risk.

Over the past year, we have put significant time and effort into launching one of our most recent innovations, ExpectID Mobile. As consumers increasingly adopt the mobile channel, and more organizations move to mobile platforms, we saw an amplified need in the marketplace for mobile-specific identity verification and fraud prevention solutions. Our ExpectID Mobile solution allows businesses to establish, maintain and ultimately trust the identity of a consumer on a mobile device, which is a complex task given the rise in mobile account takeovers, improved mobile spoofing technology and the millions of change events that occur with mobile devices such as a consumer porting a device between carriers. Our enhanced identity solution for mobile commerce enables companies to assess mobile risk, deter fraud and improve the user experience by creating a unique and persistent mobile identity. Certainly visit our website to learn more.

Overall, our goal as a solution provider, is to not only prevent fraud in the best way possible, but also to ensure that good customers encounter a streamlined experience without friction, and those identities with potential fraud flags are seamlessly escalated and either approved through automated manual review processes or declined if determined fraudulent.

This report presents the collective input of some of the world's most talented and diligent anti-fraud practitioners who have direct experience with this delicate security vs. convenience balance. I hope this research provides some useful insights and helps you identify emerging threats and opportunities for your business.

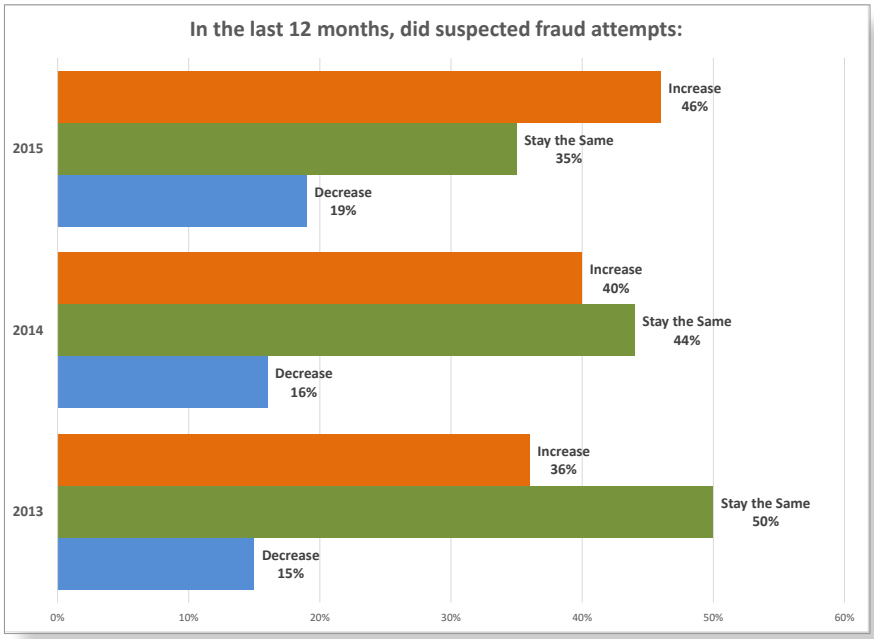
John Dancu
CEO, IDology, Inc.

About IDology: At IDology, we maintain a results-driven, entrepreneurial approach to identity verification and fraud prevention. With our solution, you gain multiple opportunities to approve a customer which increases approval rates and allows the legitimate customers easy access to your products or services. Good customers are passed and move forward without any friction - while those that require increased verification are escalated and approved...or not. Our solutions are built to help you to effectively acquire new customers and build your business.

IDOLOGY

Survey Results & Analysis

Suspected Fraud Attempts Continue to Climb



For a third year in a row, the amount of survey respondents reporting an *increase* in suspected fraud attempts rose. From *36%* in 2013 and subsequently *40%* in 2014 to *46%* in 2015. In addition, those that reported suspected fraud attempts having stayed the same continued to decline - from *50%* in 2013, *44%* in 2014 to *35%* in 2015.

On the other hand, those reporting suspected fraud attempts decreasing year over year also rose - from *15%* in 2013 to *19%* in 2015. However, this increase was minor in comparison to those experiencing intensified fraud challenges.

While overall, organizations that experienced suspected fraud attempts in the last 12 months has declined from *87%* in 2014 to *77%* in 2015, the majority of participants surveyed are still experiencing attempted fraud at a greater rate than when this survey was introduced in 2013 *(66%)*.

As suspected fraud attempts remain problematic for organizations, and as these attempts continue to climb, the need for businesses to detect fraudulent activity and take the steps needed to protect their organization is clear. However, companies must also remain focused on improving the user experience by employing multiple layers of verification in order to ensure that the good customers can gain access to products and services without friction and criminals are escalated to higher levels of verification and ultimately stopped.

How have data breaches impacted your industry?

"Fraudsters use stolen data to sell what looks to be legitimate financial applications to lending companies. They also use the same stolen data to obtain loans in victims' names, close accounts and steal the loan dollars."

~ Vice President Small Business, Financial Services Organization

Survey Results & Analysis

Fraudsters Continue to Target Website Applications. Mobile & Call Center Fraud Intensifies.

In line with IDology's 2014 Fraud Report, website applications continue to bear the brunt of attempted fraud with *71%* of respondents reporting fraud as most prevalent online. This is in comparison to *86%* in 2014.

As EMV continues to gain traction in the United States, it is expected that fraud will shift to website applications since "chip and pin" technology is more difficult to duplicate than the current magnetic-stripe variety in use. This, in combination with an increased amount of businesses moving their products and services to the card-not-present environment has lead criminals to alter their methods and move their activities online. As new fraud schemes arise targeting online applications, businesses will need to take increased action to boost their identity verification and fraud prevention programs.

One interesting development in this year's results is the rise in organizations reporting suspected call center fraud attempts - from *2%* in 2014 to *13%* in 2015. Call center fraud can take on many forms. For example, it can occur when criminals contact an organization's call center pretending to be someone they are not.

This can be done using information learned about an account holder as a result of a data breach or compromised personal identifiable information available online or it can be accomplished by a fraudster misleading a customer service representative with stories of hardship in order to gain information and access. These survey results demonstrate the increased need for organizations to implement improved identity verification and fraud prevention programs in order to quickly and accurately identify callers within their call center environment.

Respondents reporting mobile fraud tactics also rose this year - from *3%* in 2014 to *8%* in 2015. Mobile fraud has become increasingly top of mind for businesses as the use of smart devices gain in popularity and usage. With the convenience of smart devices being able to access a consumer's personal accounts across multiple industries, security is becoming more and more of a priority for organizations of all sizes.

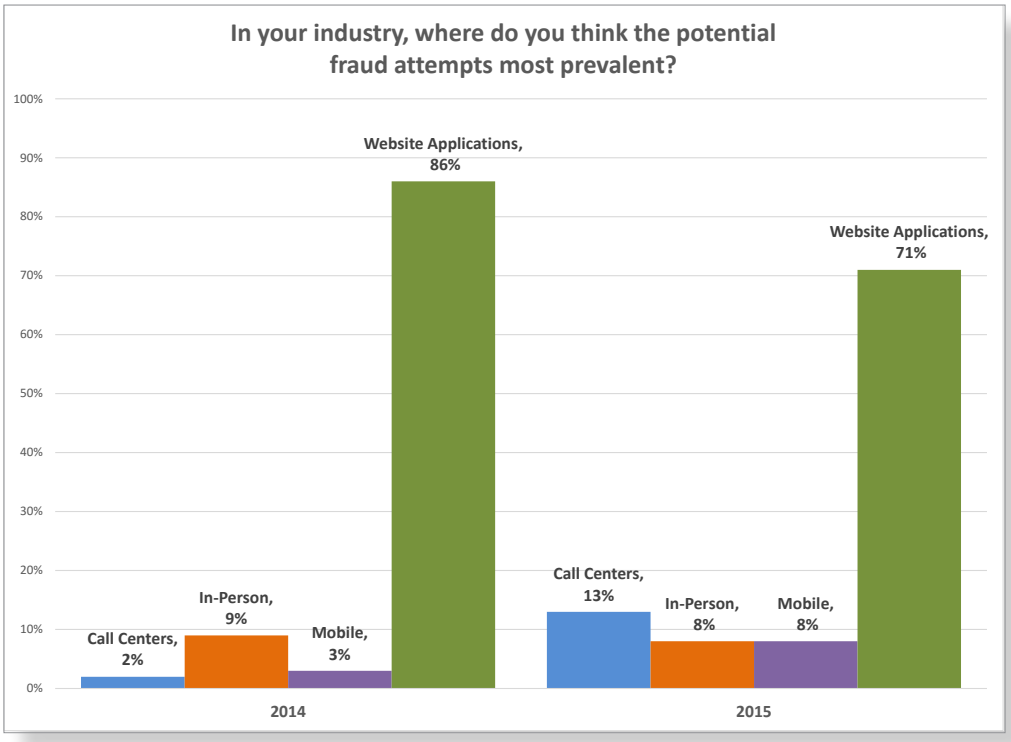
How have data breaches impacted your industry?

*"**1.** Loss of customer trust.*

***2.** Cost to remediate breach impacts.*

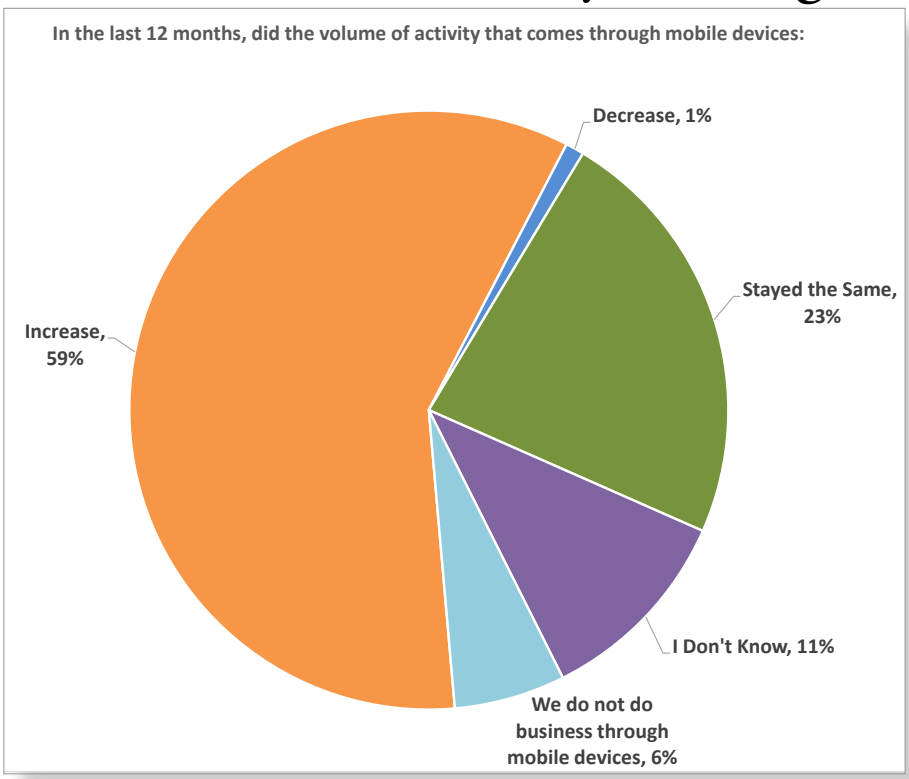
***3.** Increased cost to monitor and prevent."*

~ President, Medium Enterprise, Financial Services Organization



Survey Results & Analysis

Volume of Activity Through Mobile Devices Grows



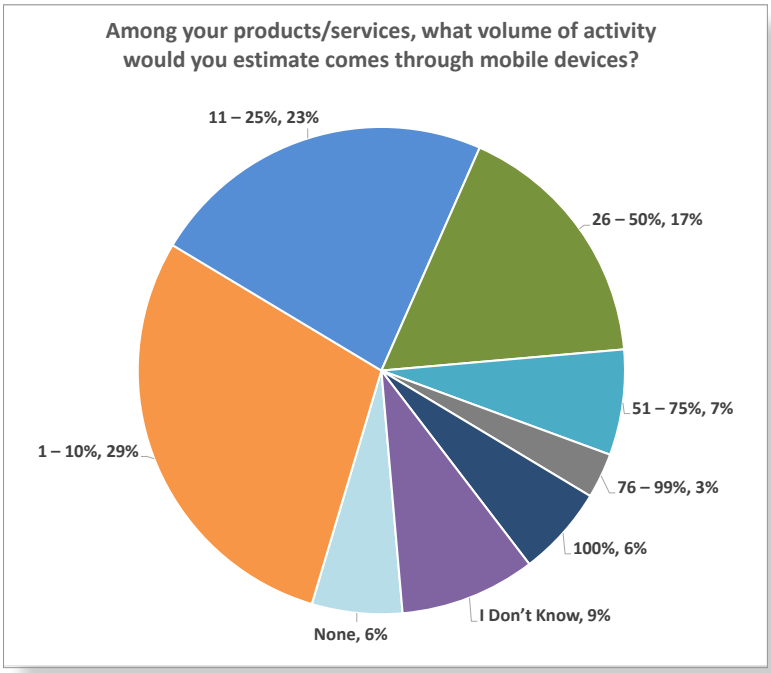
It's no secret that mobile is gaining in popularity. As a result, this year, IDology asked customers a series of mobile questions in order to gauge the volume of activity originating from mobile devices, what types of mobile fraud tactics are most prevalent and what is the level of investment on mobile they anticipate their organization making in over the next 12 months.

59% of survey respondents said that the volume of activity that comes through mobile devices has increased over the last 12 months. Only *1%* responded that this activity has decreased during this time-frame. Only *6%* of organizations reported that they do not do business through mobile devices at this time and *23%* said that this activity has stayed the same.

When it comes to the percentage of volume this mobile activity makes up in relation to an organization's overall transactions, *29%* of survey respondents said that only 1-10% of their current activity comes through mobile devices. *23%* responded that 11-25% of transactions come through mobile and *17%* said that their mobile volume is between 26-50%.

While mobile activity does not currently make up the majority of overall transactions for the surveyed organizations, these results indicate that the volume is growing and we anticipate this activity will continue to grow into 2016 and beyond.

Organizations operating or planning to operate in the mobile environment must ensure that their identity verification and security solutions are optimized for the unique requirements of mobile commerce. Companies should be able to verify a consumer's identity based on a persistent mobile identifier that also combats the advanced techniques used by fraudsters and ensures the highest ease of use of the mobile application.



Survey Results & Analysis

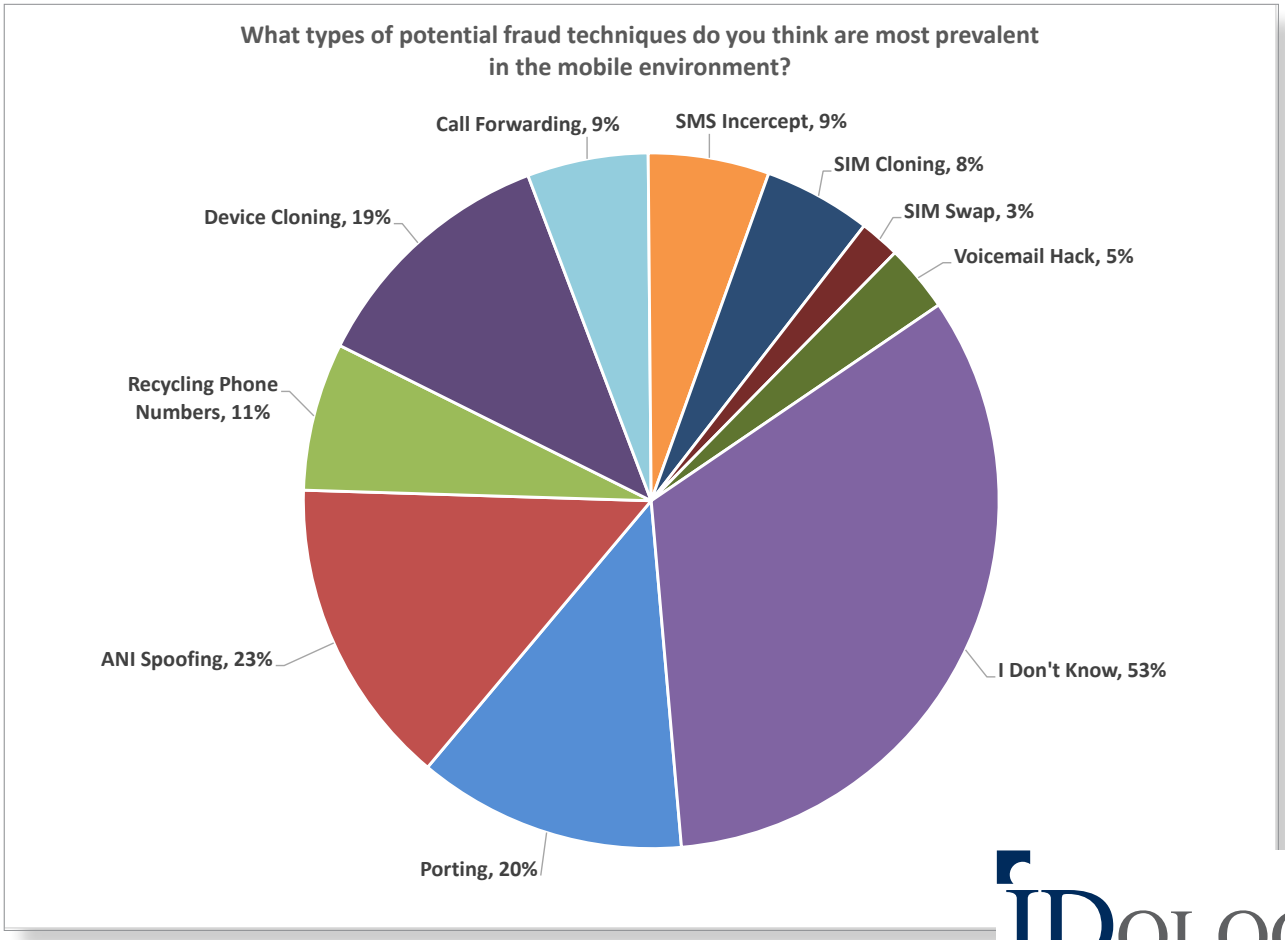
Account Takeover via Porting, ANI Spoofing and Device Cloning Top Mobile Fraud Tactics

As more and more consumers turn to mobile devices to perform every day activities as well as share sensitive personal data, an increasing amount of fraudsters are embracing mobile as a way of targeting them. Mobile fraud takes on many shapes and sizes. In our survey, ANI Spoofing *(23%)*, Account Takeover via Porting *(20%)*, and Device Cloning *(19%)* received the top three responses from customers reporting that these methods are most prevalent in the mobile environment. Other tactics include Recycling Phone Numbers *(11%)*, Call Forwarding *(9%)*, SMS Intercept *(9%)*, SIM Cloning *(8%)*, Voice-mail Hack *(5%)* and SIM Swap *(3%)*.

Glossary of Mobile Fraud Tactics:

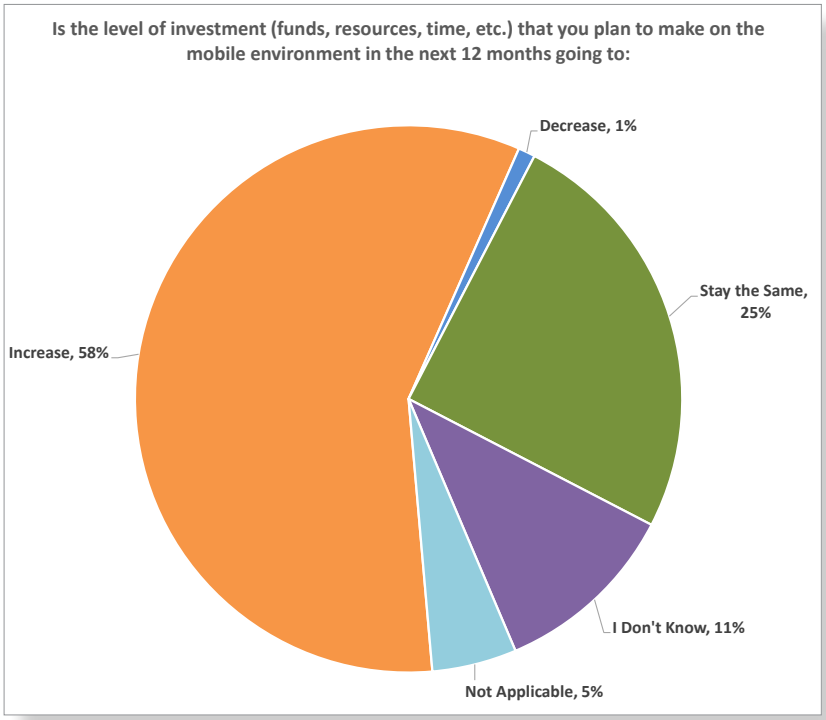
- **Account Takeover via Porting:** Fraudster social engineers the mobile network operator call center to "port" ownership from victim device to himself in order to obtain mobile terminating one time passwords, or even generate outgoing communication.
- **ANI Spoofing:** Fraudster calls into the call center pretending to be from the victim's phone number.
- **Recycling Phone Numbers:** Fraudster attempts to activate phones with new numbers with aim to receive a recycled number that is currently attached to a tenured victim's account.
- **Device cloning:** Fraudster makes a software image of the device in order to impersonate the device from a software perspective and fool device fingerprinting solutions.
- **Call Forwarding:** Fraudster enables call forwarding on the victims phone in order to hijack mobile terminating voice calls from the bank that contain sensitive information (one time passwords, transaction confirmations)
- **SMS Intercept:** Fraudster intercepts inbound SMS communication.
- **SIM Cloning:** SIM values from victim are copied to fraudster SIM so fraudster can impersonate subscriber on the network and obtain all incoming communication.
- **SIM Swap:** Fraudster social engineers the mobile network operator call center with stolen PII to deactivate existing users SIM and activates a device in their possession in order to hijack all mobile terminating communication.
- **Voice-mail Hack:** Fraudster breaks into victim's voice-mail. Fraudster causes mobile terminating voice one time passwords sent to phone to go to voice-mail and obtains them for fraudulent use.

With mobile fraud tactics constantly evolving, it is critical for organizations to employ robust id verification and fraud prevention solutions that enable changes to be made on-demand in order to stay ahead of fraud and minimize risk associated with mobile devices.



Survey Results & Analysis

Level of Investment on Mobile Expected to Increase



Business and user adoption of mobile technology and commerce are growing exponentially. Because of this, it is no surprise that organizations are planning to invest more in mobile over the next 12 months. *58%* of those surveyed reported a plan to increase their level of mobile investments (funds, resources, time, etc.) in the coming year. Only 1% of respondents said that they plan on decreasing their investment in mobile.

One area that many organizations plan on investing further in is mobile security. As consumers increasingly adopt the mobile channel, and more organizations move to mobile platforms, there is an amplified need for mobile-specific security solutions that enable real-time identity verification and fraud prevention.

One way in which businesses are able to accomplish this is by establishing, maintaining and ultimately trusting a customer's mobile identity. However, establishing a mobile identity and reducing the risk associated with the mobile environment is a complex challenge. It is critical for companies to allow legitimate customers to be able to seamlessly and securely gain access to mobile products and services. On the other hand, it is equally as crucial for organizations to spot and stop potential fraud. Fraudsters have become quite skilled at exploiting the many nuances that accompany mobile devices - from the millions of change events to the increasing ability of fraudsters to attack mobile technology with methods similar to what we found in these survey results - porting, spoofing, cloning and more.

How have data breaches impacted your industry?

"Increase in tax refund fraud, primarily associated with web-based tax preparation software."

~ Vice President & Risk Manager, Medium Enterprise, Banking Organization

Organizations need to employ robust id verification and fraud prevention solutions that are able to create and verify the unique and persistent mobile identity of a customer. Along with detecting and preventing fraud, this mobile identity needs to be persistent through all of the different change events that may occur as a consumer changes devices or carriers, ports their phone, swaps their SIM and more. Knowledge of these change events is extremely valuable as they can be deterministic of an account takeover.

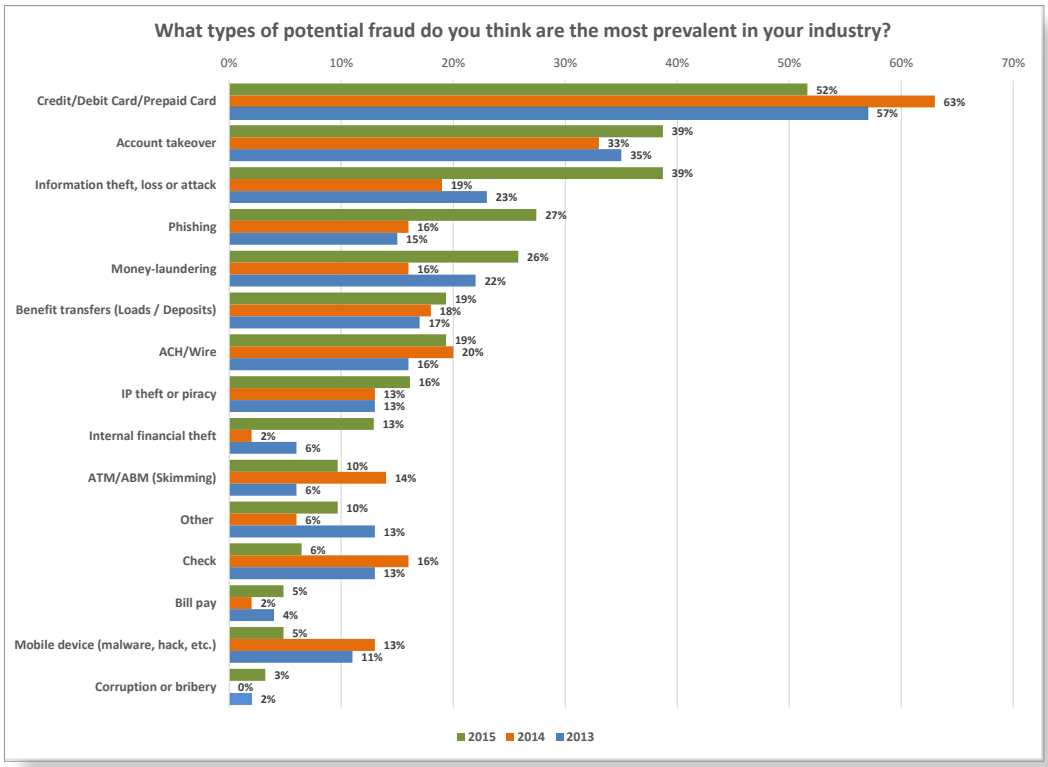
Criminals are showing greater levels of determination and sophistication in their efforts which is leading to more destructive attacks that are harder to spot. A robust mobile identity solution helps companies better understand the risks they face and subsequently act with a greater degree of security and vigilance – ensuring the legitimate customers experience less friction and raising the level of verification and ultimately blocking the fraud.

IDOLOGY

Survey Results & Analysis

Phishing and Information Theft Become More Widespread

While credit, debit and/or prepaid card fraud continues to be the most prevalent type of fraud for a third year in a row *(57% in 2013, 63% in 2014 and 52% in 2015)*, several other forms of potential fraud made large jumps this year. Information theft, loss or attack seems to have increased the most this year - from *19%* in 2014 to *39%* in 2015. We expect this to be, at least in part, a result of the widespread data breaches that have continued to plague the industry. Due to increased data breaches, valuable consumer information has become readily available on black markets such as the dark web. Fraudsters can then purchase this identity information and use it to impersonate a legitimate consumer. The survey also saw an increase in account takeovers this year - from *33%* in 2014 to *39%* in 2015 - which goes hand in hand with information theft fraud.



How have data breaches impacted your industry?

"Account takeover activity is co-related to data breaches and hence impacts our business."

~ Manager, Small Business, Financial Services Organization

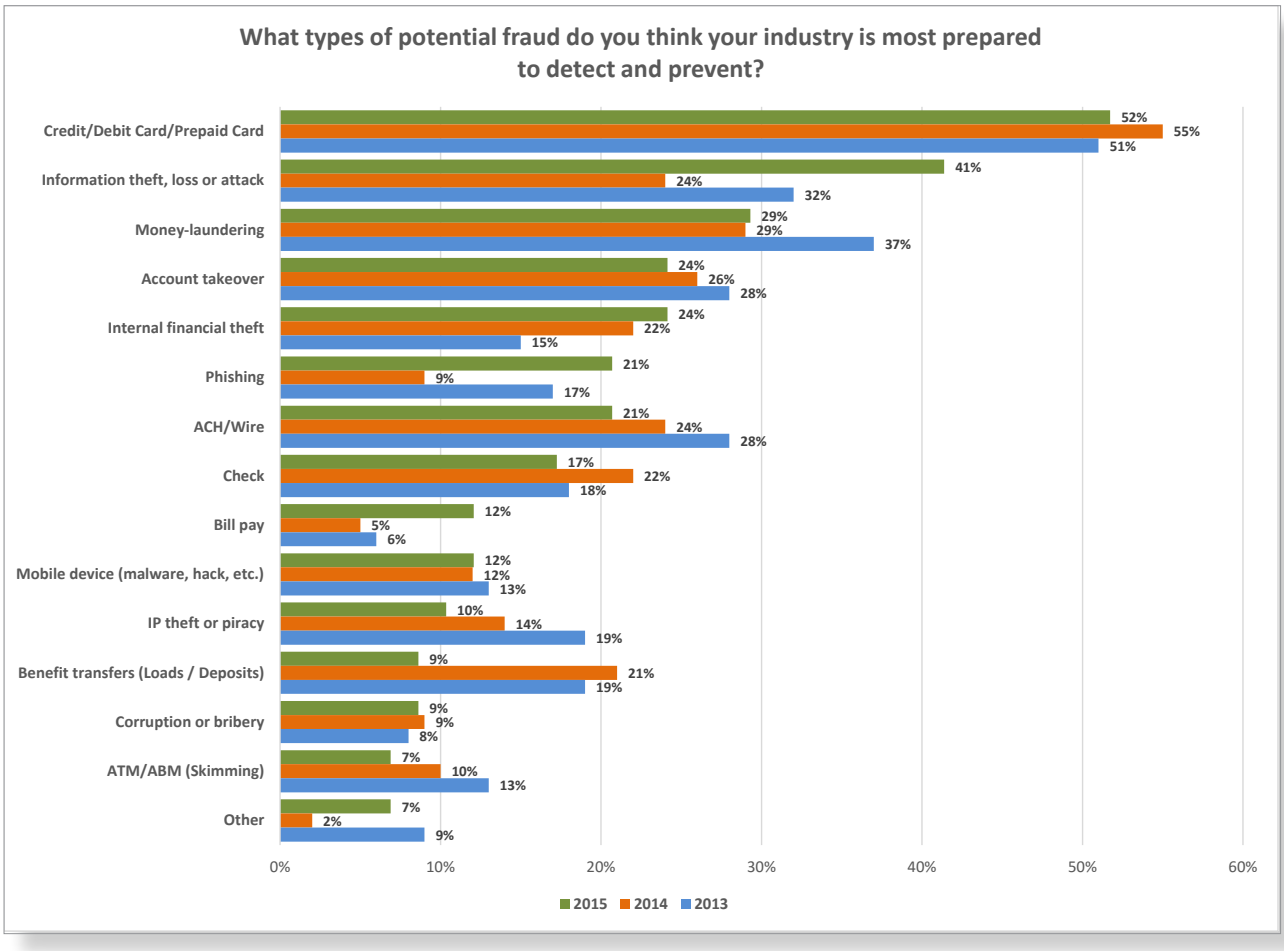
Phishing also saw a marked increase this year - from *16%* in 2014 to *27%* in 2015. Identity thieves are increasingly deploying sophisticated phishing email schemes in order to try and trick unsuspecting victims into releasing valuable information or clicking on fraudulent links. Other fraud tactics that had more moderate increases this year include money laundering *(22% in 2013, 16% in 2014 to 26% in 2015)* and internal financial theft *(6% in 2013, 2% in 2014 to 13% in 2015)*.

Those methods seeing a decline in prevalence this year include check fraud *(13% in 2013, 16% in 2014 to 6% in 2015)*, and surprisingly mobile device fraud *(11% in 2013, 13% in 2014 to 5% in 2015)*. It will be interesting to see the results in 2016 regarding mobile fraud given the level of investments that the majority of organizations plan to make on mobile over the next 12 months.

Survey Results & Analysis

Organizations Shift Their Focus in Order To Detect & Prevent Evolving Fraud Techniques

For a third year, organizations report that they are most prepared to detect and prevent credit, debit and/or prepaid card fraud receiving *52%* of survey responses this year *(51% in 2013 and 55% in 2014)*. While the number of organizations reporting the prevalence of information theft, loss or attack has risen, we also saw a large improvement in those that say they are more prepared to detect and prevent this type of fraud this year than in previous years *(32% in 2013, 24% in 2014 and 41% in 2015)*. However, with organizations reporting an increase in frequency of account takeovers, they also felt, in contrast, less prepared to detect and prevent account takeover activity *(28% in 2013, 26% in 2014 and 24% in 2015)*.

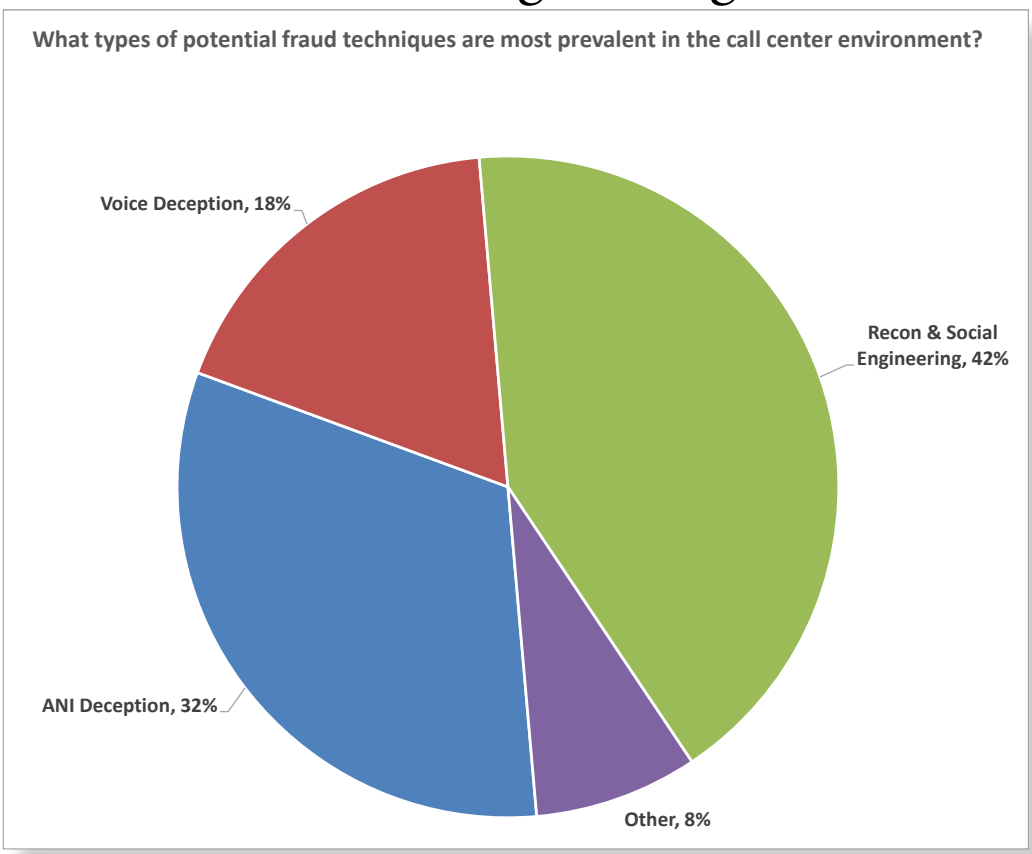


A few interesting trends include:

- Respondents feel more prepared to detect and prevent phishing attempts than in years past, particularly since 2014 *(17% in 2013, 9% in 2014, 21% in 2015)*
- Benefit transfer (loads/deposits) fraud has slowly increased in prevalence *(17% in 2013, 18% in 2014, 19% in 2015)*, however organizations don't feel as prepared to prevent this type of fraud *(19% in 2013, 21% in 2014, 9% in 2015)*
- Respondents are much more prepared to deal with bill pay fraud than in previous years *(6% in 2013, 5% in 2014, 12% in 2015)*
- Only *12%* of respondents report being prepared to detect and prevent mobile fraud. However, this has not changed much since 2013 *(13% in 2013, 12% in 2014, 12% in 2015)*
- ATM/ABM (skimming) fraud has declined in overall preparedness
- ACH/Wire fraud readiness has also declined

Survey Results & Analysis

Recon & Social Engineering Lead Call Center Fraud Schemes



As this year's fraud report survey results revealed, suspected call center fraud attempts have grown this year. When it comes to the types of call center fraud that respondents believe are most prevalent, recon and social engineering dominate, receiving *42%* of the response. ANI (Automatic Number Identification) deception (spoofing/apps, VoIP gateways, burner phones) *(32%)* and voice deception (disguise, distortion, additional noise) *(18%)* are other tactics that criminals employ to defraud the call center environment.

How do organizations that operate a call center gain the confidence that their representatives are speaking with a legitimate customer instead of a fraudster?

Fraud Trend

"Impersonation of a physician."

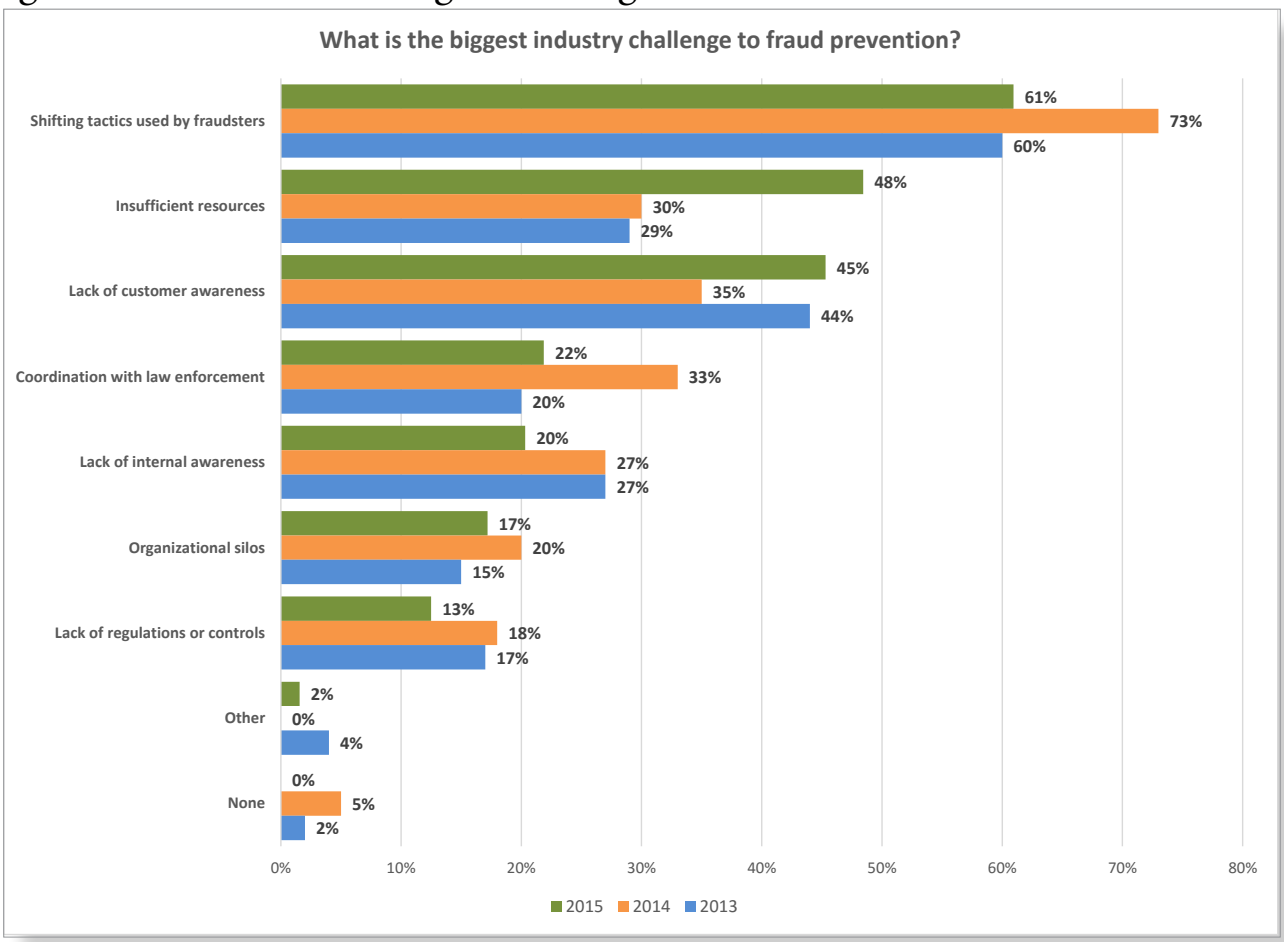
~ Director of Product Management, Large Enterprise. Healthcare Organization

By improving a call center's identity verification and fraud prevention platform, organizations are able to strike a balance between operational efficiency and fraud prevention. They can then tailor a system fit for their business needs and instantly process verifications without losing productivity or lengthening call times. This will allow them to ensure that the legitimate customers are quickly and accurately identified, while also employing dynamic fraud prevention and multi-layered verification processes to fight fraud.

Being able to detect, deter and eliminate fraud is an essential priority for any organization. And, as more and more criminals turn to call centers to defraud businesses, enhanced call center solutions are needed to prevent fraudsters impersonating customers from being able to access products and services. Moreover, systems that are able to verify that customer calls are in session will increasingly become important in order top stop ANI spoofing tactics and also lessen the time needed to approve legitimate customers.

Survey Results & Analysis

Shifting Fraud Tactics a Challenge. Growing Concerns About Fraud Prevention Resources.



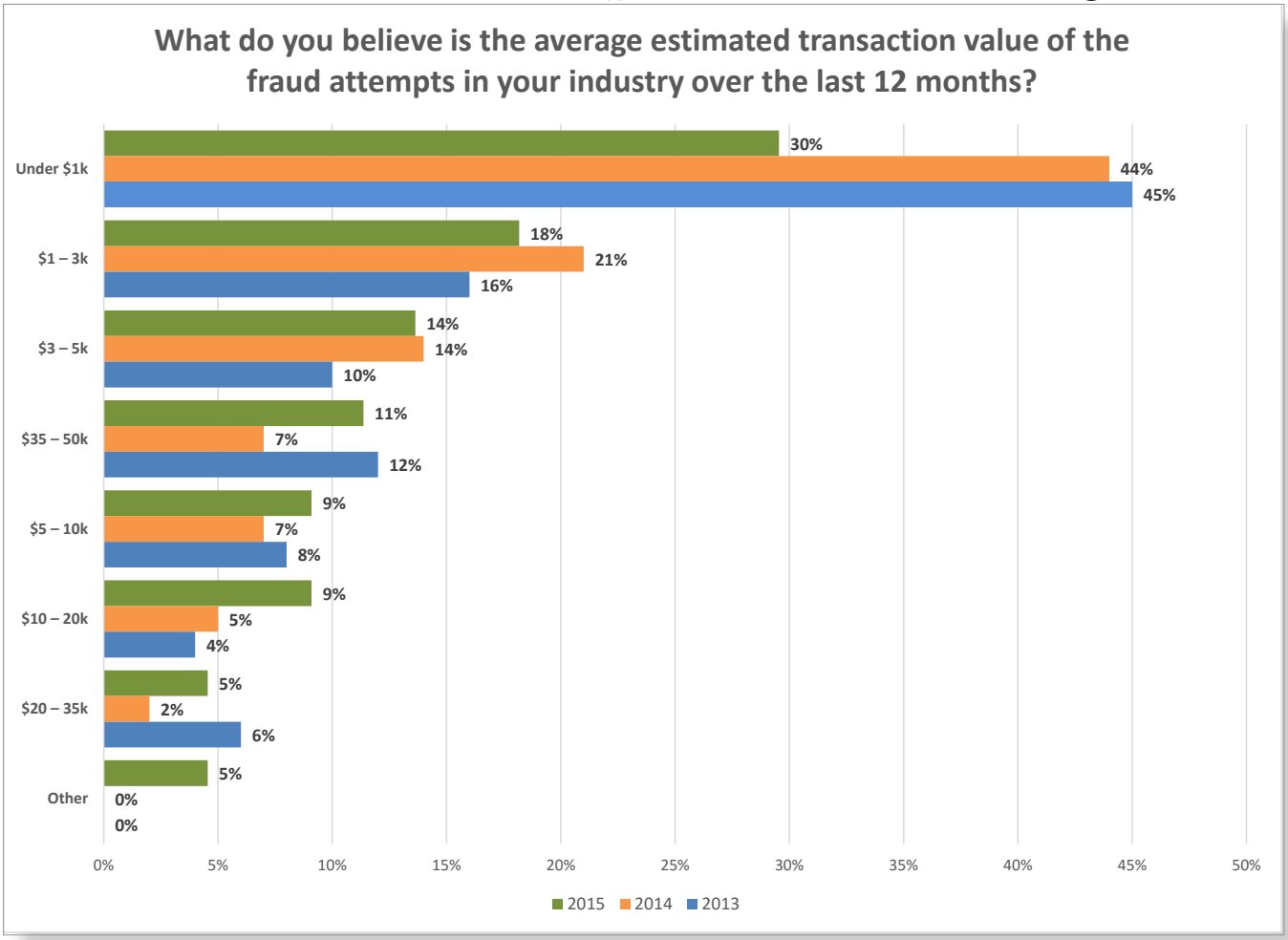
Shifting tactics used by fraudsters continues to be the top challenge for organizations in their fraud prevention programs, although this has declined since last year - from *73%* in 2014 and *61%* in 2015. Due in large part to advances in technology, especially with the continued growth of the online marketplace, businesses have to constantly fight fraud in order to protect their own interests as well as their customers' privacy. Improved identity verification and fraud prevention techniques make it easier for organizations to keep fraud out while, at the same time, improving the overall customer experience.

Interestingly, the challenge of insufficient resources grew drastically this year - from *30%* in 2014 to *48%* in 2015. As fraud challenges continue to grow and evolve, it seems that respondents are concerned about whether they have enough resources available to remain at the forefront.

Lack of customer awareness appeared to have improved in 2014, reaching a low of *35%* of the response. However, this year this challenge rises again to *45%*. While customers may be aware of fraud in general, fraud tactics are changing at a higher rate than customers are aware of. This is a challenge for businesses that must implement fraud prevention solutions that also do not add bothersome friction to the overall user experience. On the contrary, lack of internal awareness as decreased this year *(27% in 2013 and 2014 to 20% in 2014)* signifying that businesses are well aware that fraud is an issue that needs to be dealt with.

Survey Results & Analysis

Small Dollar Fraud Attempts Give Way to Larger Sums



According to survey respondents, small dollar fraud, or rather, suspected fraud attempts with an average estimated value of under $1,000 decreased substantially this year *(45% in 2013, 44% in 2014 to 30% in 2015)*. However, while small dollar fraud still receives the highest percentage of responses overall, it does give way to an increase in larger summed fraud. Particularly, suspected fraud with an average estimated value of $10,000 - $20,000 saw an increase from *5%* in 2014, to *9%* in 2015. Additionally, those that responded "other" in our survey this year reported seeing suspected fraud attempts of "over a million dollars" and "more than $50,000".

Fraud ranging from $1,000 - $3,000 still comes in second with fraud ranging from $3,000 - $5,000 follows close behind. However, no matter the value of suspected fraud attempts, it is clear that businesses need to put the necessary programs in place to verify the identity of their customers in order to prevent criminals from conducting fraudulent transactions.

How have data breaches impacted your industry?

"Tighter controls have been implemented across the board because of big name data breaches."

~ Director, Medium Enterprise, Healthcare Organization

IDology Data & Analysis

New Geographic Regions Emerge as Centers of Suspected Fraud

The IDology fraud team, on a daily basis, examines new and emerging fraud trends. In last year's fraud report, we found that a significant amount of the suspected fraud appeared to be centrally located within a few geographic regions. In 2014, these regions primarily consisted of South Florida, North West Georgia, and New York/New Jersey. While all of these regions remain at the top of the list, this year, a few new regions also emerged as centers of suspected fraudulent activity. These cities include Detroit and Grand Rapids, Michigan; San Francisco, Bakersfield and Adelanto, California; Chicago, Illinois; Houston and Dallas, Texas; and Tuscaloosa, Alabama.

While other cities throughout the East and West Coast have pockets of suspected fraud activity, fraudsters appear to have concentrated in these particular regions. However, fraudsters are constantly evolving, so it is important to monitor suspicious activity and have solutions that enable configuration changes on demand to adjust to changing threats.

Protecting customer privacy involves more than making sure that your customers' data remains intact. It is also in your ability to detect potential fraud as it emerges. Likewise, with the rapid growth of mobile technology, you must also be able to employ solutions that prevent emerging mobile fraud tactics while also eliminating friction in account opening, enabling quicker mobile account access and better securing mobile interactions. At IDology, we help organizations evaluate risk based on identity, activity, device and location based attributes combined with collaborative fraud prevention tools that enable customers to quickly spot and stop fraud. Dynamic decisioning enables the legitimate customer to pass with minimal friction while the fraudster misusing customer data is stopped or escalated to higher levels of verification.

As a leading voice in the fight against fraud, IDology is constantly innovating in order to stay ahead of the fraudsters and help you protect data and privacy while providing a positive experience that gives your customers a higher level of confidence and security.

IDology Customer Feedback

Top Benefits Include Compliance, Manual Review Reduction, Implementation and Decrease in Fraud.

At IDology, we earn our success everyday by helping customers build their business. We are a customer-driven organization and our goal is to serve with innovative solutions and build strong personal relationships where our customers look to us for domain expertise and assistance in applying our solutions.

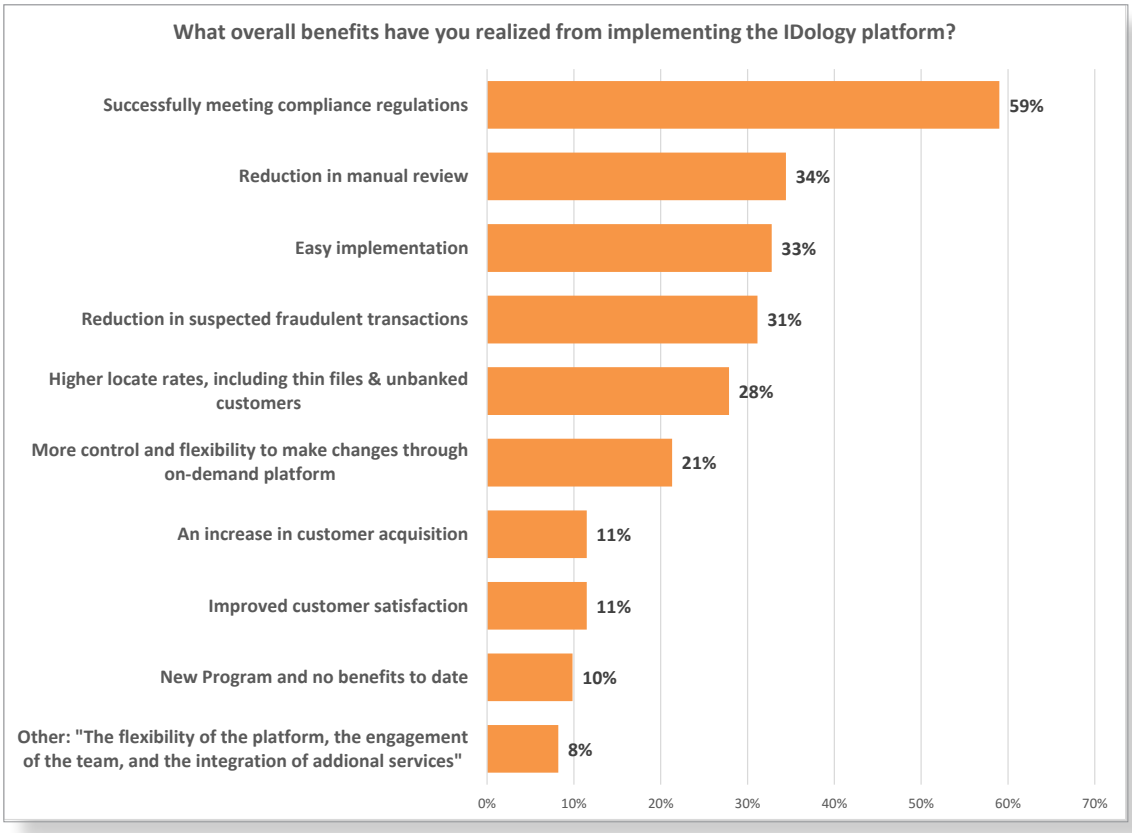
Successfully meeting compliance regulations *(59%)*, reduction in manual review *(34%)* and ease of implementation *(33%)* top IDology's customer list of benefits. Reduction in suspected fraudulent transactions received *31%* of the response and higher locate rates, including thin files and unbanked customers received *28%*.

Other benefits that are important to note are more control and flexibility to make changes through an on-demand platform *(21%)*, improved customer satisfaction *(11%)* and an increase in customer acquisition *(11%)*. While stopping fraud, streamlining processes and meeting compliance are important, ultimately, your goal is to grow your business and drive revenue. With the IDology solution, customers are able to acquire more customers and improve overall satisfaction.

Fraud Trend:

"People that build computer software that mimics mobile phones and mobile fingerprint to circumvent security and fingerprinting checks."

~ Chief Operating Officer, Small Business, Media & Entertainment Organization



Here is what IDology customers had to say...

Financial Services:

"The largest business impact has been the ability to pro-actively identify potential high risk fraud/bad actor incidents."

~ Founder, Small Business, Financial Services Organization

"With IDology, we can increase our ability to verify identities without requiring them to submit documents to us."

~ Chief Operating Officer, Small Business, Financial Services Organization

"Increased ability to quickly identify high fraud area applications and shut down applications from identified areas. Lower fraud lost expense. Lower application processing costs."

~ President, Medium Enterprise, Financial Services Organization

"IDology's platform helps us get users through our funnel quicker than our previous provider."

~ Analyst, Medium Enterprise, Financial Services Organization

"Our client's can meet regulatory requirements and have the ability to add fraud controls at will."

~ Analyst, Medium Enterprise, Prepaid Organization

"You guys do a better job finding lesser banked folks, hands down."

~ Vice President, Risk & Compliance, Fortune 500, Financial Services Organization

"Ability to implement changes without internal development resources. Creation of a peer group network for sharing of experiences and best practices."

~ Chief Compliance Officer, Medium Enterprise, Financial Services Organization

"Peace of mind when it come to customer sign-ups."

~ Managing Member, Small Business, Financial Services Organization

"IDology helps us effectively manage and prevent fraud at on-boarding ."

~ Head of Compliance, Small Business, Financial Services Organization

IDOLOGY

Banking:

"IDology is more innovative and adaptable to our industries needs. IDology will readily engage in testing new products/tools to assist with IDV and CIP."

~ Manager, Banking Organization

"Our customers are more confident that they are protecting their customers."

~ Analyst, Banking Organization

Healthcare:

"We are able to let end clients create their own accounts on customer websites. This limits the customer interaction and greatly speeds up the request process."

~ Analyst, Medium Enterprise, Healthcare Organization

"Easier identification of healthcare providers."

~ Director of Product Management, Large Enterprise, Healthcare Organization

Retail:

"Meets compliance regulations such as OFAC."

~ Director, Large Enterprise, E-Commerce Organization

"It helps move things along to verify information."

~ Analyst, Small Business, Retail Organization

Fraud Trend:

"Individuals who have stolen identities, and apparently been able to open bank accounts in the victim's name.

~ Vice President, Small Business, Financial Services Organization

Gaming:

"Naturally preventing fraud in effect prevents loss of revenue and protects customers as well as protects ourself."

~ Analyst, Small Business, Gaming Organization

"We are able to meet our regulatory compliance requirements within the Lottery industry."

~ Manager, Large Enterprise, Gaming Organization