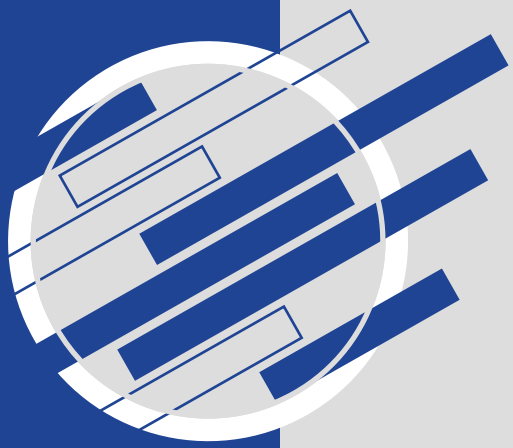
A Forrester Consulting
Thought Leadership Paper
Commissioned By Sift Science

April 2017

# Mitigating Threats Beyond Payment Fraud

## Address The Full Abuse Ecosystem To Win, Serve, And Retain Customers



FORRESTER®

# Table Of Contents




**Project Director:**
Rachel Linthwaite,
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®

Firms are not yet equipped to combat the mounting threat of nonpayment fraud and abuse.

70% of companies agree that the customer is most affected by fraud and abuse.

# Executive Summary

Whether or not to engage in digital relationships with customers is no longer an option for businesses looking to succeed today. Without a strong digital strategy, firms will undoubtedly get left behind. But the very nature of digital relationships has an impact on the ways in which customers and brands interact. Ultimately, the nature of fraud and abuse risk changes as customer interactions move increasingly online.

Most notably, the growing importance of digital content and community strategies raises the profile of nonpayment fraud. As firms move away from focusing strictly on commerce, they increase the risk and applications of fraud and abuse, introducing account takeovers, phony accounts, fake or malicious content, and the like into the mix. This change dictates an equal response from companies looking to mitigate risk. In order to succeed in a changing landscape, firms must realign priorities to account for the rising nonpayment threat and invest in predictive, agile solutions that automate processes.

In January 2017, Sift Science commissioned Forrester Consulting to explore how organizations are addressing online fraud beyond the realm of simple payments and credit card use cases. Forrester surveyed 150 fraud prevention and risk management professionals at digital businesses in the US to understand how they view the changing landscape of abuse as a result of this shift toward content and community.

### KEY FINDINGS

- **The nature and risk of fraud shifts as customer interactions go increasingly digital.** Fraud management is not just a loss problem; it's also a way to maintain good customer experiences. Unfortunately, companies are most vulnerable to the abuses that hurt the customer hardest and also happen to be some of the most common.
- **Firms are underprepared for the mounting nonpayment fraud threat.** Though firms note an increase in nonpayment abuses, they have yet to prioritize mitigating that risk over the risks associated with payment fraud. Tools and solutions adopted to combat the increasing threat are myriad, but they also come with their own set of shortcomings.
- **Automated, holistic approaches to fraud prevention lead to business benefits.** In order to win, serve, and retain customers, businesses must view the problem of fraud holistically. The key to gaining real business benefits is adopting predictive solutions that eliminate the need for manual oversight across all abuse types. The results will be lower spends, cut losses, and increased customer satisfaction across the board.



FORRESTER®

# Digital Relationships Change The Nature Of Fraud

In the age of the customer, organizations are competing for customers harder than ever before — and on a seemingly never-ending list of burgeoning channels. As organizations seek new digital approaches to customer engagement, they must also adjust to a shift in their risk profile.

The shift to digital relationships leads to a shift in risk profile.

Companies that don't invest in building digital relationships will fall behind. Investment in technology that drives digital customer interaction, such as payments, fraud management, and online communities, delivers customer value and drives revenue. Unsurprisingly, nearly a third of companies globally are allocating 15% of their revenue to these critical digital investments.[1] Those that do not invest in forging digital relationships with customers will lose to organizations that are focusing both time and budgets on this area.

This digital investment must, in turn, shape the business' security and fraud prevention investment and strategy. As more and more customers approach the business on digital channels, the business must also provide a pleasing customer experience during identity verification. The ultimate goal, then, is to have access and fraud management capabilities that at the very least do not hinder good CX, while simultaneously maintaining reasonable costs for investigation and analysis staffing.

## FRAUD MANAGEMENT IS CRITICAL TO CUSTOMER OBSESSION

86% of firms note creating/maintaining excellent customer experiences as a high or top priority.

The key to winning, serving, and retaining customers in the digital age is having exceptional, seamless customer experiences across all channels. Understanding this as a guiding principle for all internal teams, regardless of where exactly within the organization they sit, is critical to ensuring good CX. Risk management and fraud prevention professionals are far from exempt from this clarion call.

- **Customer experience is paramount.** Risk management and fraud prevention teams understand the importance of good CX as well as anyone else. Creating and maintaining excellent customer experience is a high or top priority for 86% of organizations we surveyed. These firms see that in order to truly call yourself customer obsessed, you must be led by your customers' needs and guided by their particular journey with your brand.
- **Fraud hurts the customer most.** The issue of fraud and abuse is a problem specifically because it hits companies where it matters most — their customers. Seventy percent of organizations cited customer privacy/safety/satisfaction as somewhat or strongly affected by fraud and abuse, topping company reputation (67%), revenue (56%), and relationship with regulatory authorities (49%). While ultimately, firms are looking to protect their bottom lines, fraud affects customers first, weakening their experiences and ultimately hurting both their relationship with and favorable impression of the firm's brand. The desire to mitigate fraud and abuse, therefore, is not simply financial; it's business critical.



FORRESTER®

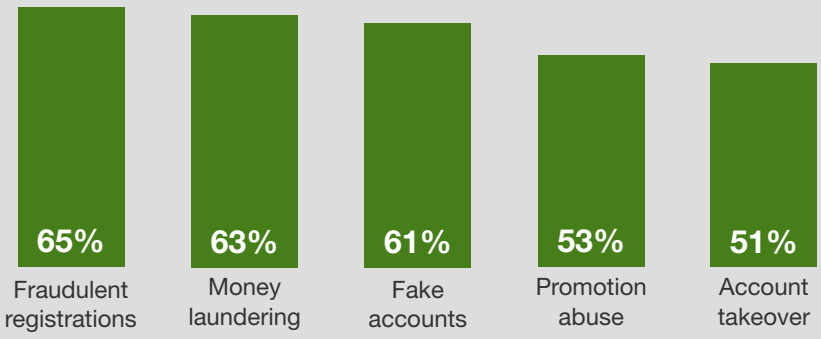
## BROADER DIGITAL RELATIONSHIPS BREED NEW ABUSES BEYOND PAYMENTS

Opening up increasingly more digital channels to customer interaction not only increases the risk of fraud but also opens the door to new abuses. Whereas previously, payments and credit card fraud were of primary concern, nonpayment abuses now have the potential to hurt businesses. And because they are new, they have the ability to cause real harm.

- **Nonpayment abuses are among the most common.** The results of this study make it clear that firms are experiencing new nonpayment types of abuse most frequently. Fifty-seven percent reported experiencing fake accounts, while 39% noted experiencing account takeover. However, just because nonpayment abuse is on the rise, does not mean that the problem of payment frauds is waning. Payment fraud with digital goods (51%), money laundering (49%), and payment fraud with physical goods (45%) are also among the most consistently faced abuses.
- **Companies are most vulnerable to abuses that harm customers most.** While nonpayment abuses are happening most frequently, firms have not yet found a way to successfully combat them. Those surveyed believe that some of the abuses to which they are most vulnerable are also the most common: fraudulent registrations (65%), fake accounts (61%), and promotion abuse (53%) (see Figure 1). This is a problem for firms that seek to put the needs of the customer first. All abuses that companies note they are the most vulnerable to are at the very best annoying and at the very worst destructive to the life of the consumer. Organizations admit that they are struggling to protect their customers from the kinds of fraud and abuse that can have a real, measurable impact on quality of life. This is a problem that must be solved if good CX is the goal.

**Figure 1**

**"How vulnerable do you believe your company is to each of the following types of ongoing fraud and abuse today?"**
(Sum of "highly" and "somewhat" vulnerable responses are shown)




Base: 150 US-based managers or higher in charge of risk management and fraud prevention for their 500-plus-employee organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Sift Science, February 2017

Nonpayment abuses are what firms are most vulnerable to and combat most frequently.

Fraudulent registrations top the list, eclipsing payment fraud by over 10%.



FORRESTER®

# Firms Are Underprepared For Mounting Risk Of Nonpayment Fraud

Though fraud prevention and risk management professionals acknowledge the growing threat of nonpayment fraud, firms have not yet equipped themselves to deal with the problem. Priorities — and with them investments and attention — are still aligned with the payment frauds of yesterday. Adjusting that misalignment is necessary to combat the growing risk.

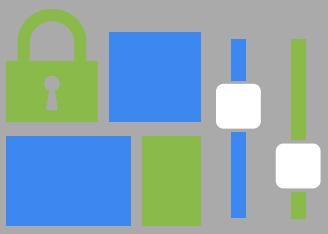
› **Fraud priorities are not aligned to the change in risk.** While firms admit that the greatest risk comes from fraudulent registrations (which are most commonly thought of in terms of identity theft) and fake account abuse (e.g., creating multiple fraudulent accounts using fake email addresses), payment fraud still receives more attention. Seventy-two percent of organizations weigh preventing/reducing payment fraud as a high or top priority, in contrast with only 62% of firms that feel the same about nonpayment fraud (see Figure 2). This misalignment is the core of the challenge for firms as they seek to protect both their customers and their bottom lines from the full gamut of abuses. If they continue to persist in prioritizing payment fraud over nonpayment fraud, the risk will continue to mount and results will not be favorable.

**Figure 2**

**72%** of organizations weigh preventing/reducing **payment fraud** as **a high or top priority**

**62%** of organizations weigh preventing/reducing **nonpayment fraud** as **a high or top priority**

Base: 150 US-based managers or higher in charge of risk management and fraud prevention for their 500-plus-employee organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Sift Science, February 2017



The gap between prioritization of payment fraud and nonpayment fraud is the core challenge for firms today.



FORRESTER®

› **The risk of nonpayment fraud is growing.** Again, survey results highlighted a gap between what firms perceive to be their reality and where they are prioritizing investment. Even while firms prioritize payment fraud today, they admit nonpayment abuses are the looming threat among fraudsters. Forty-five percent of firms agree that fraudulent registrations will increase in frequency over the next 18 to 24 months, compared with only 37% for payment fraud of digital goods. Furthermore, four of the next five types of abuse expected to increase are also of the nonpayment variety (see Figure 3). The issue then is clear: Firms realize the threat from nonpayment abuse is here and is only going to get worse if something isn't done about it.

› **Reputations are at stake.** Customer satisfaction is not the only issue at risk here. With 67% of organizations reporting that company reputation is affected by fraud and abuse at their organization, this under preparation for the growing threat may very well compound reputational risk over the next two years. When massive fraudulent or money laundering activity happens, regulations force companies to disclose this to the public, resulting in a potential lack of trust in the ability of said company to keep its information and money safe. The combined impact of customer satisfaction and reputation issues is enough to concern any business professional. But even that is not the whole story. Not surprisingly, half of firms (49%) also worry how fraud is harming their relationship with regulatory authorities. Beyond heads rolling from the C-suite, this creates a massive loss of goodwill and reputation for the organization. And, of course, ultimately all of this will hurt the business' ability to remain profitable: 56% worry that their revenue or business continuity will be affected by these mounting threats.

At the end of the day, if firms want to avoid detrimental impact to their customer base, reputation in the marketplace, and their bottom line, they must adjust internal priorities to account for the growing risk of nonpayment abuse.

## FIRMS USE MANY TOOLS TO COMBAT FRAUD BUT LACK STRATEGY AND RESULTS

Fraud prevention and risk management professionals are working to combat abuses in many ways. Using a variety of tools has served them well in the past, but adjusting to the growing risk posed by nonpayment fraud and abuse requires a different strategy — one that firms have not quite mastered yet.

› **Firms are expanding fraud management capabilities but misaligned to greatest risk.** The most basic fraud prevention measures currently enjoy the most widespread use and will see the greatest expansion: Seventy-eight percent of firms have a security or network operations center, with 35% of those firms also planning to expand those centers. Similarly, 72% of companies have employee cybersecurity training; again, 35% of those companies intend to expand the trainings going forward. While this is all well and good as the basis for a fraud prevention system, it does not go far enough. The more powerful technologies that

**Figure 3**

**INCREASING ABUSES**

**Most anticipated abuses to increase within 18 to 24 months**


**Other abuses expected to increase**

- **29%** Fake or malicious content
- **26%** Account takeover
- **25%** Friendly fraud
- **25%** Fake accounts
- **23%** Promotion abuse

Base: 150 US-based managers or higher in charge of risk management and fraud prevention for their 500-plus-employee organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Sift Science, February 2017



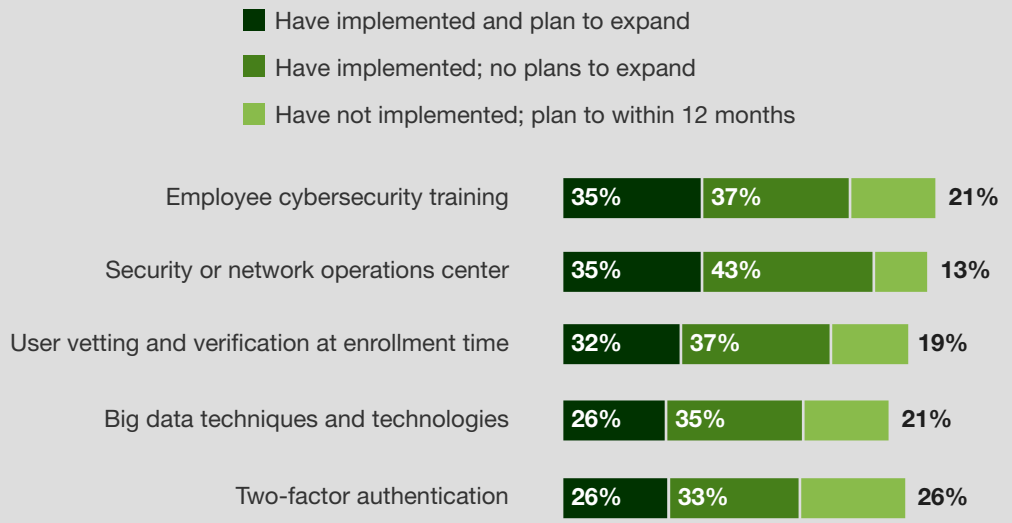
FORRESTER®

comprise big data techniques and two-factor authentication are used far less frequently and are only expanding at a quarter of firms (26%). Meanwhile, user vetting and verification at enrollment time — which has the potential to greatly reduce the most commonly experienced types of nonpayment fraud — could also stand greater expansion, but less than a third of firms (32%) have already implemented it (see Figure 4). The essential issue here is that firms are still attempting to mitigate specific threats, instead of thinking holistically about the entire fraud and abuse ecosystem. If these organizations wish to succeed in the digital age, they must develop trust and safety measures that account not just for the payments fraud of yesterday but also the nonpayment abuses that are here today, as well as the threats lurking around tomorrow's corner.

› **Current tools fall short.** Even as firms attempt to mitigate fraud through the adoption of various tools, they still encounter issues. Those surveyed struggle primarily because aging tools can't recognize new fraud patterns as they emerge (cited as a challenge by 68%). This inability to keep up with the ever-changing nature of fraud, when coupled with the lack of flexibility to allow for real-time adjustment (61%), poses a real problem for companies. The nature of digital customer relationships is constantly evolving, and with this comes opportunities for fraudsters to wreak havoc. If the tools currently in place can't pick up on new or different fraud patterns and can't learn from these new patterns, companies must resort to manual oversight, which is more time consuming, expensive, and prone to human error. Not surprisingly, then, the high ongoing transactional cost required of management is also a key problem (67%). These pain points highlight the need for automated tools that can optimize efficiency and employ machine learning.

**Figure 4**

**"Which of the following statements best reflects the current state of your company's adoption of fraud prevention measures?"**




Base: 150 US-based managers or higher in charge of risk management and fraud prevention for their 500-plus-employee organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Sift Science, February 2017



FORRESTER®

# Protect Customers With Automated Tools Powered By Big Data

As their challenges suggest, firms are struggling with a lack of automation when it comes to fraud detection and mitigation. Though they utilize a host of tools, they have yet to hone in, it seems, on just the right ones.

- **Firms can stand to win by automating detection.** Manual oversight is still playing a big role in detection. In fact, a combination of manual oversight and software is the prevailing tactic in 35% of firms for fraudulent registration and digital good payment fraud alike. And manual oversight alone is still used to varying degrees depending on the type of abuse. This is particularly true for detecting fake or malicious content (18%), friendly fraud (15%), and account takeover (13%). Detecting nonpayment abuses, it seems, is particularly labor intensive. These survey results show that firms are still quite far away from full automation when it comes to detecting and mitigating fraud. This leads to increased costs, inefficiencies, the potential for missed abuses or false positives, and the inability to keep up with the ever-shifting nature of these threats. Clearly, there is much to gain for these firms by turning to automation.
- **Investigation by eyeballing is not an option.** To succeed, organizations must adopt solutions that solve these key challenges. Specifically, firms crave robust tools that allow for better reporting and auditing (49%), provide a multilayered and integrated platform (42%), and, of course, provide automated processes and decisions (41%). Solutions powered by big data analytics are also important to many respondents. Companies believe that these enhanced investigative and user capabilities, when coupled with the ability to automate processes and decisions, is critical for being able to overcome the mounting risks. But it is also interesting to note that 29% of those surveyed indicated a desire for supervised machine learning-based algorithms. This is important, as it could help assist firms with their key challenge of not being able to detect new fraud patterns. Shifting to machine learning-based techniques powered by big data has the potential to take the guesswork out of mitigation, with tools that learn from the scores of data available and can flag different patterns of abuse when they arise.

## BIG BENEFITS ARE WON THROUGH HOLISTIC FRAUD PROTECTION

› **The main benefits of fraud mitigation are shared across categories.** When it comes to mitigating both types of fraud, firms believe the main business benefits will be financial. Cutting losses due to fraud and spending less on fraud investigations rise to the top of the expected benefits list overall (see Figure 5). The stakes to ensure the fraud problem is being handled properly is therefore of critical importance. Not only are customer satisfaction and company reputation on the line, but the ability to successfully decrease instances of abuse will directly lead to economic efficiencies.

› **Firms realize second-tier benefits with a holistic solution.** When we asked firms about the business benefits of mitigating nonpayment and payment abuse, we found that better ROI on marketing investments and improved customer satisfaction were the third and fourth most commonly expected gains for both. A robust solution able to tackle the two risks in tandem, therefore, will add to the bottom line. Because of how important maintaining good CX is for companies, this last benefit is nothing to scoff at. Being able to improve customer satisfaction while cutting losses, eliminating unnecessary spends, and receiving better returns on investments being made in marketing indicate that fraud prevention is an important business challenge. And mitigating fraud and abuse — particularly those instances that stand to cause the most damage — is an opportunity for businesses to continue to win, serve, and retain their customers.

Firms need powerful, flexible, automated solutions to enjoy the big business benefits of fraud mitigation.

**Figure 5**

**"What do you expect to be the business benefits of mitigating nonpayment/payment fraud abuse?"**


Base: 150 US-based managers or higher in charge of risk management and fraud prevention for their 500-plus-employee organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Sift Science, February 2017

Holistic solutions that reduce abuses across categories allow firms to realize benefits in top areas of business importance.



FORRESTER®

# Key Recommendations

To account for the growing and changing risks that fraud and abuse pose, firms must shift from a narrow focus on payments and credit cards to a more holistic focus on trust and safety. By accounting for the full ecosystem of potential threats, companies will better protect themselves and their customers and ultimately win in the end.

Forrester's in-depth survey of risk management and fraud prevention professionals yielded several important recommendations:

**Make the business case for fraud management.** Ensuring executive support is critical. In order to secure buy-in, create a direct connection between business objectives and fraud management to show to executive stakeholders and gain support.

**Involve marketing and line-of-business stakeholders in fraud management.** If you can't effectively manage fraud, business growth will be hampered. Partners and internal stakeholders outside of typical risk management and fraud prevention roles need to understand this for the firm as a whole to be successful in the endeavor.

**Think big picture when it comes to fraud prevention.** When combating fraud and abuse, firms must think about not just payments but also the entire customer journey life cycle. Onboarding, registration, authentication, payments, and transactions, as well as self-service, must all be taken into consideration to create an effective, holistic mitigation strategy.

**Look beyond tools.** Tools in and of themselves won't solve the fraud and abuse issue. Organizations need to have governance and processes that cover all transactions and channels before settling on the right tools for the job. Once the framework is in place, then a tool to cover these channels is a must, but skipping the first step is not an effective way to get ahead.

**Don't get more tools; get the right tools.** Firms need to make sure that the tools they employ can cover both nonpayment transactions and nontraditional (e.g., mobile, chat, chatbot) channels with specific risk scoring models.

**Lean heavily on data.** Reliance on as much data and/or big data in a fraud management tool as possible only helps fraud rates. Organizations must prepare to feed clickstream navigational analysis, sensor data from mobile devices, and series of past transactions into their big data-based risk scoring model to stay ahead.

**Understand that old school approaches won't work.** Do not attempt to solve tomorrow's issues with yesterday's methods. Manually managing rules for risk scoring is slow, costly, and inaccurate. Instead, use solutions that offer machine learning and AI-based automation of risk scoring. The solution should also be capable of learning from investigator feedback and have a constantly updated risk scoring model. Only then will organizations be able to keep up with the ever-changing fraud and abuse risk.



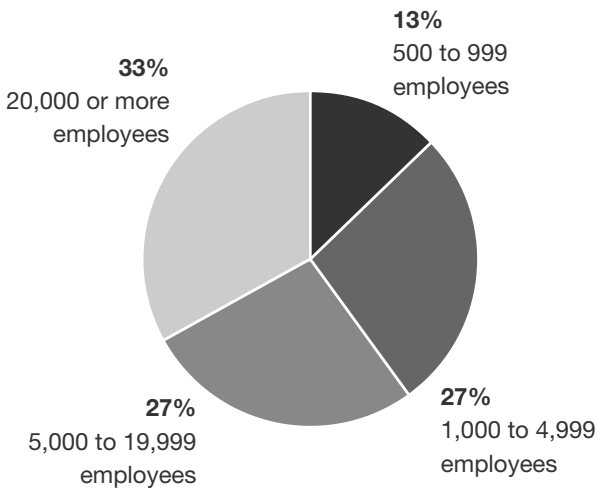
FORRESTER®

# Appendix A: Methodology

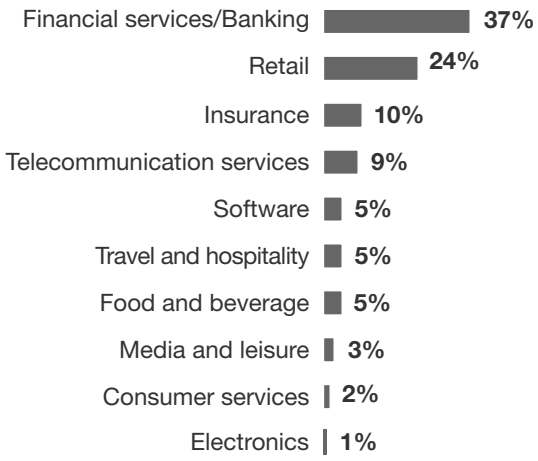
In this study, Forrester conducted an online survey of 150 500-plus-employee organizations in the US to evaluate how firms are addressing online fraud beyond the realm of payments. Survey participants included decision makers in fraud prevention and risk management roles. Questions provided to the participants asked how the growing importance of content and community strategies is affecting the nature of fraud risk. Respondents were offered an 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: Demographics/Data

**Company size**




**Industry**




**Areas selected as "very involved"**



Base: 150 US-based managers or higher in charge of risk management and fraud prevention for their 500-plus-employee organization (percentages may not total 100 because of rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of Sift Science, February 2017



FORRESTER®

# Appendix C: Supplemental Material

**RELATED FORRESTER RESEARCH**

"Stop Billions In Fraud Losses With Machine Learning," Forrester Research, Inc., April 6, 2015

"Big Data In Fraud Management: Variety Leads To Value And Improved Customer Experience," Forrester Research, Inc., October 16, 2013

"Best Practices: Effective Enterprise Fraud Management," Forrester Research, Inc., March 31, 2015

# Appendix D: Endnotes

[1]Source: "Build Your Digital Transformation Business Case Around The Customer And Revenue Growth," Forrester Research, Inc., February 22, 2017.