October 2019

similityA PayPal Service PYMNTS.com

FRAUD DECISIONING PLAYBOOK

Keeping On-Demand PROFESSIONAL SERVICES FRAUD-FREE

– Page 7 (Feature Story)

FTC reports millennials are 25 percent more likely to fall for eCommerce fraud

– Page 11 (News and Trends)

How data lakes help fight fraud

– Page 16 (Deep Dive)

TABLE OF CONTENTS

ACKNOWLEDGMENT

The Fraud Decisioning Playbook is produced in collaboration with Simility, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

PYMNTS.com

WHAT'S INSIDE

KEEPING PACE WITH CYBERCRIMINALS IS SIMILAR TO A GAME OF WHACK-A-MOLE FOR ONLINE MERCHANTS.

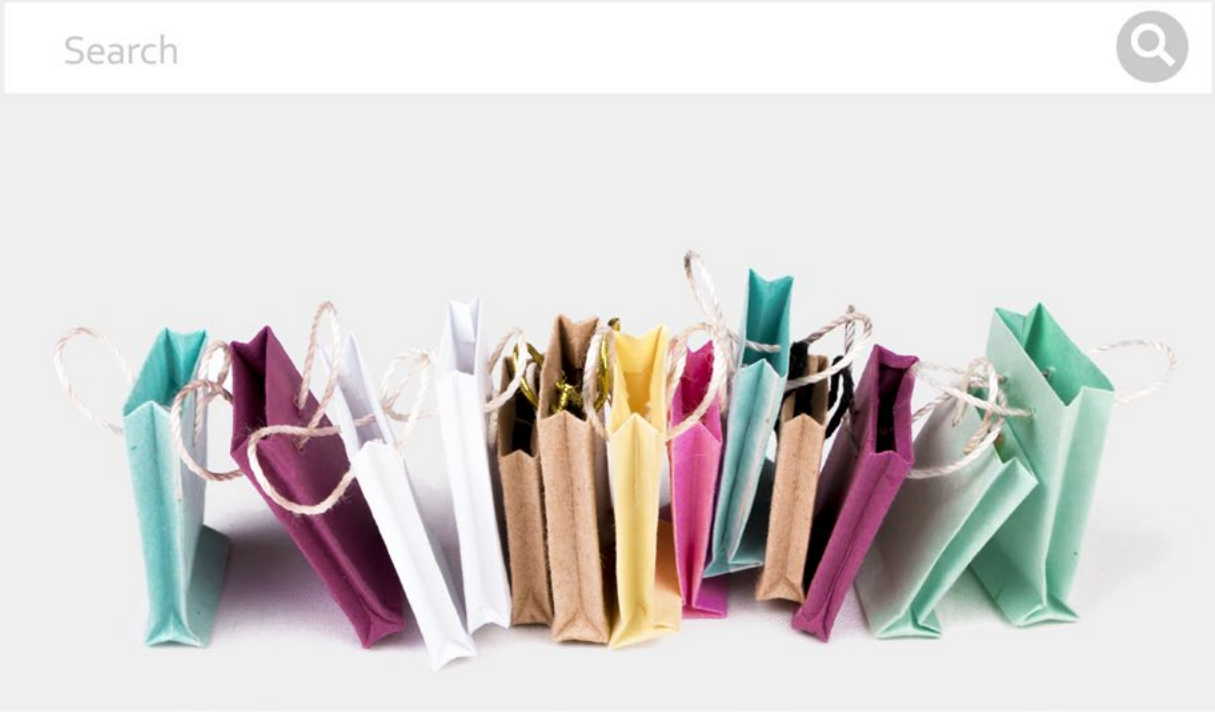
Fraudsters are getting more creative when impersonating legitimate customers and sidestepping authentication protocols, pressuring online merchants and marketplaces to adopt new anti-fraud strategies. Merchants and eCommerce companies must not only upgrade their systems after detecting fraud events, but also identify new threats and respond in real time.

Businesses need more than fraud solutions that can flag potential cybercriminals as they attempt to access sensitive information and effectively fight fraud. These merchants require solutions that can learn and evolve from each incident, allowing them to become more effective.

Cybercriminals can devastate companies' finances and deplete their resources by impersonating legitimate users, allowing bad actors to steal data or initiate transactions based on false pretenses. Research shows the increased availability of personally identifiable information (PII) is making such attacks easier: The number of exposed United States consumer records containing PII increased by 126 percent between 2017 and 2018. These crimes can also hurt companies' reputations and leave customers and investors paranoid about how data breaches could affect their interests. Compromised businesses may be held responsible for chargebacks associated with fraudulent purchases if stolen information is used for transactions that are later disputed.

Staying ahead of new fraud threats requires firms to collect massive troves of data and analyze them for vulnerabilities and patterns that can provide actionable insights. Humans can only do so much, however, and manually reviewing such large volumes of information can be time consuming and fail to adequately protect against attacks. Data volume is expected to grow by 800 percent over the next few years, and as much as 80 percent of this information will be unstructured, making it even more challenging for businesses to determine which details are relevant.

Fraud decisioning solutions can help these firms better understand attacks and anticipate future schemes



by combining automation, Big Data analytics, machine learning (ML) and human insights to establish data-driven orchestration hubs, improve decisioning efforts and adapt to new fraud tactics. These tools can also protect against account takeovers (ATOs), new account fraud, transaction fraud, transfer fraud and mobile check deposit fraud.

Stopping such crimes is only half the equation, however. The other half requires smooth experiences for legitimate customers, meaning businesses must balance seamlessness and security. Fraud decisioning solutions must also have omnichannel operations as customers now interact with their favorite brands both in person or online via social media, mobile, apps and email. Employing strong mechanisms can help businesses spot fraudsters in real time without sacrificing seamless and secure user experiences.

The new Fraud Decisioning Playbook, a PYMNTS and Simility collaboration, will highlight the latest solutions changing how financial institutions (FIs), eCommerce merchants and others understand and respond to fraud-based threats. The monthly report will examine how these industries are embracing fraud decisioning solutions to reduce chargebacks, ATOs and false positives as well as deliver safer, more secure experiences for legitimate users.

THE LATEST FRAUD DECISIONING DEVELOPMENTS

Consumers of all ages are at risk of losing money to social media and online marketplace scams, but the U.S. Federal Trade Commission (FTC) found that the threat is highest for millennials. This group is 25 percent more likely to report fraud-related losses than those aged 40 or older and are particularly vulnerable to marketplace scams, losing $71 million to online shopping fraud over the past two years.

The FTC also highlighted that fraud is a growing problem for online dating and classified ad sites. These schemes involve fraudsters who pretend to be online suitors and

trick users into sending them money under false pretenses. Such scams cost U.S. consumers $143 million each year — more than any other type of fraud.

Consumers can also find their merchant loyalty rewards programs targeted by fraudsters. Recent data shows that ATOs have affected approximately 1.5 million individuals over the past year, with fraudsters opening new accounts in legitimate users' names and siphoning off funds and benefits from them. The trend highlights why merchants need to secure consumers beyond the transaction point of sale (POS) and why they should use artificial intelligence (AI) and ML to protect consumers at all stages of their journeys.

To learn more about the shifting fraud and security landscape, read the Playbook's News and Trends section (p. 11).

HOW HANDY STAYS AHEAD OF FRAUDSTERS

Online marketplaces must not only protect consumers from fraud, but also the professionals seeking employment via their platforms. In this month's Feature Story (p. 7), Oisin Hanrahan, CEO of on-demand professional hiring platform Handy, describes how the company relies on AI, ML and human insights to stay ahead of fraudsters.

DEEP DIVE: DIVING INTO DATA LAKES

Businesses from a wide variety of industries must handle troves of data as they continue to crack down on fraud. Making sense of such large volumes of information can be challenging, though, and firms must ensure that their systems are tapping into and analyzing the right kinds of data. This Playbook's Deep Dive (p. 16) highlights how data lakes — massive repositories of information — are becoming crucial to firms' anti-fraud strategies.

FIVE FACTS

1.5M

Share of individuals who have had new accounts opened in their names due to account takeover attacks

81%

Share of fraud victims in 2018 who said they interacted with a false ad last year

$400

Average amount millennial consumers lost per fraud incident

1.4M

Number of fraud reports the FTC received in 2018

80%

Expected share of unstructured data enterprises will process daily by 2025

Keeping On-Demand Professional Services **FRAUD-FREE**

feature story

FEATURE STORY

DIGITAL MARKETPLACES RELY ON TRUST TO THRIVE. CUSTOMERS WHO DO NOT FEEL THEY CAN SAFELY TRANSACT ON SUCH PLATFORMS ARE HIGHLY UNLIKELY TO RETURN TO THEM, PUTTING TREMENDOUS PRESSURE ON MERCHANTS TO PROVIDE EXPERIENCES THAT ARE BOTH SEAMLESS AND SECURE.

The challenge is doubled for two-sided marketplaces that connect customers and service providers. These platforms must ensure that all parties are trustworthy, putting them in precarious positions as they work to build their user bases without alienating either side with their anti-fraud measures.

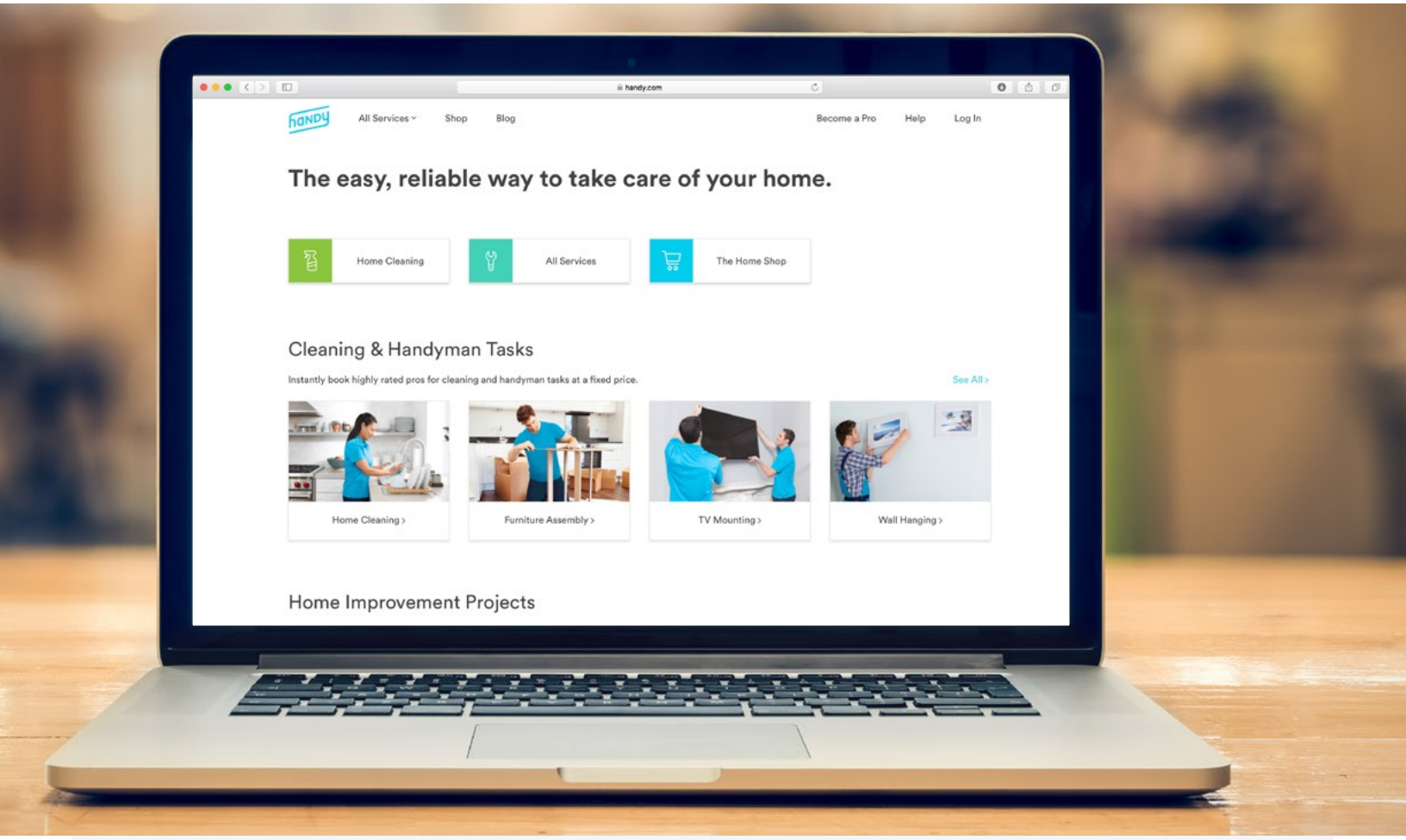
One such marketplace is on-demand professional services platform Handy, which connects customers with workers who can perform a multitude of household tasks, such as cleaning, furniture assembly and appliance installation. CEO Oisin Hanrahan recently spoke to PYMNTS about how the company combines AI and ML solutions and human insights to ensure its anti-fraud efforts do not interfere with legitimate users' experiences.

"There are ever more ways in which funds are flowing digitally, and that creates an opportunity for fraudsters to behave in ways that are detrimental to legitimate customers," he said. "I hope ... that we can continue to drive toward this world where we can identify individual actors with very high levels of certainty."

WALKING THE SECURITY-SEAMLESSNESS LINE

Vigilance against fraudsters begins with the onboarding process, according to Hanrahan. Customers and professionals who use Handy's platform must provide data that it can use to enhance interactions and build trust upfront.

"When you're onboarded to the platform, we ask you a number of questions and do a pretty deep regression analysis to figure out how your answers to questions are likely to lead to a great experience," he said.



The onboarding process uses AI and ML to review data like Social Security numbers and facial recognition technology to compare selfies with government-issued forms of identification. The platform also runs customers' background checks and processes credit cards through a predictive analytics system to gauge fraud risks. Handy requires two-factor authentication (2FA) methods such as text messages or email responses to verify certain activities, including sudden changes to credit card numbers, home addresses or — in the case of professionals — the bank accounts in which their funds are deposited.

These measures are necessary to protect both sides of Handy's platform, but Hanrahan said the challenge is in making sure its anti-fraud efforts are not cumbersome for legitimate consumers looking to hire professionals.

"If we were to go and insist that every customer that comes to our site would do the same photo verification that a pro would do, that would obviously be too extreme," he said. "It's a matter of figuring out how you put in place the right balance to maintain a seamless customer experience."

GETTING PREEMPTIVE ABOUT FRAUD

Handy protects its platform by underwriting transactions, which ensures customers are not liable for fraudulent payments made with stolen credit cards and that professionals are paid for their jobs. The latter are also guarded against false reviews because the platform enables only users who have hired and paid for services to share their experiences online.

Handy's role as an underwriter requires it to determine how fraud affects its bottom line and how much activity should trigger a response. It also relies on a team of contractors to analyze the platform for patterns and uncover vulnerabilities.

"The last part is to say, 'How can we preemptively spot these things before they actually come to fruition?'" he said. "To do that, we engage with folks to really dig in on the platform and try and identify vulnerabilities in advance."

The company's solutions combine several data fields to determine if new fraud patterns are emerging. These solutions use AI and ML tools to review individuals' behaviors, identify trends over time and engage with its team of data scientists to understand important correlations. Hanrahan noted that advanced learning tools help new users onboard smoothly, but human beings will still be necessary to provide support and ensure seamless user experiences.

"I think we're always going to need humans to figure out certain parts of the decision tree and certain parts of where to draw the boundary between putting friction in the customer experience, what that friction looks like [and] what's the most creative way to put that friction in place to remove fraud," he said. "I think it's a balance of both in the long term."

Digital marketplaces that enable users to electronically exchange funds require several layers of protection. AI and ML tools can help quickly review trends, but human insights are necessary to make solutions more effective at catching fraudsters and ensuring seamless experiences for legitimate users. These security layers are a must in a market that relies on trust, and ensure that home professionals and consumers can transact with peace of mind.

UNDER THE HOOD

Oisin Hanrahan, CEO of on-demand professional services marketplace Handy, explains how the platform identifies potentially fraudulent activities.

"First, [we need] to look at individual examples, [such as] the tracking of individual users where we know there is a loss or where we know there is anomalous behavior, and tracking that individual's behavior throughout the transaction flow. The second is looking at these in aggregated trends — [at] trends that are changing through time — [such as] the percentage of users logging on [using] more than one device [or] the percentage of devices with more than one user. You can look at aggregated trends, and through time — if they're changing — you know if there's some change to consumer behavior or change to fraud risk. Then the third is to engage with [a] data science team and have them really go through this [with] a different lens, to look at correlations between user patterns and fraud or different trends … and to figure out how we can take action."

NEWS&TRENDS

MARKETPLACE FRAUD

TRADE GROUP ACCUSES AMAZON OF DEALING IN COUNTERFEIT GOODS

A group of big-name fashion retailers is recommending that five Amazon-backed websites from different global markets be added to a U.S. government watch list that tracks copyright infringement. The group is known as the American Apparel & Footwear Association (AAFA) and represents over 1,000 brands, including Adidas, Gap and Target. AAFA is recommending that Amazon's U.K., Canadian, French, German and Indian websites be added to the government's annual list of Notorious Markets. Adding these sites to the list could leave them vulnerable to trade sanctions, however. AAFA noted in a letter to the agency that outlines recommendations for U.S. trade policies that these sites' users can be become sellers with ease, making it difficult for consumers to understand from whom a purchase is being made. Should the U.S. government pursue this course of action it could pressure Amazon to take tougher measures against counterfeit materials.

CONSUMERS ARE MORE VULNERABLE TO ONLINE SCAMS THAN PHONE SCAMS

Amazon's counterfeit issues are part of a larger problem with online scams, according to a new report from *The Wall Street Journal*. The report found that consumers are more likely to fall victim to social media and online marketplace scams than phone scams. A recent study by the Better Business Bureau (BBB), the Financial Industry

Regulatory Authority and the Stanford Center on Longevity interviewed 1,408 fraud victims in 2018 and found that a majority of consumers are more likely to fall prey to scams on legitimate websites and social media channels. The survey found 81 percent of customers reported interacting with scam ads, and 53 percent of this group lost money in such cases. Social media is especially problematic, with 91 percent of survey respondents indicating they could not detect fake advertisements. Only 11 percent of respondents lost money to phone-based scams, however.

MIVA, KOUNT COLLABORATE ON ONLINE MERCHANT PROTECTION

A recent partnership between eCommerce solution provider Miva and digital fraud protection solution provider Kount will use AI to help merchants guard against potential fraudsters. The partnership will integrate the latter's AI-powered fraud protection solution with the former's flexible eCommerce platform, enabling online sellers to boost their revenues by accepting additional legitimate orders and reducing merchants' risk of losses due to fraud or manual review. The service notifies users of fraud's likelihood, automatically rejects high-risk transactions and reviews suspicious orders. It can also determine the availability of additional configurable application programming interface (API)-powered automation options. The collaboration will help merchants avoid chargebacks and false positives as well as eliminate friction for legitimate users.

HIDDEN FRAUD SPELLS BIG MARKETPLACE LOSSES

Merchants frequently provide free introductory offers to attract new customers, but fraudsters are exploiting these opportunities by pretending to be legitimate users. Two-sided sharing economy marketplaces are especially vulnerable, with some service suppliers exploiting these deals to boost their bottom lines. Ridesharing marketplaces often offer free rides to first-time users, for example, and fraudsters driving for such services can utilize Google or voice over internet protocol (VOIP) systems to generate fake phone numbers and use them to book first-time rides. Rideshare platforms are still required to pay these drivers even though there are no legitimate customers involved.

Jon Prideaux, CEO of mobile payment platform Boku, noted during a recent conversation with PYMNTS' Karen Webster that these attacks can compromise merchants' performances. Boku's solutions can verify whether a mobile number belongs to a legitimate device or was created by a VOIP system, he noted, adding that closing these loopholes is essential to helping merchants mitigate fraud losses.

LOYALTY PROGRAM FRAUD ON THE RISE

Merchants' loyalty programs are increasingly being targeted by bad actors. A recent report found that fraud in the space increased by 89 percent in the past year, revealing that cybercriminals' attacks are targeting

consumers' loyalty accounts and merchants' return policies as well as POS transactions.

Fraudsters are increasingly relying on ATOs, and the study found that 1.5 million individuals whose accounts were compromised had new ones illegitimately opened in their names. Bad actors then transferred funds from victims' legitimate accounts into the fake ones. These illicit activities show that merchants must adopt solutions to continuously and autonomously review customers' journeys and tackle loyalty fraud.

THE HIGH COST OF FRAUD ON MERCHANTS' BOTTOM LINES

Fraud can cost merchants more than just funds. The True Cost of Fraud study published by LexisNexis Risk Solutions concluded that merchants pay roughly $3.13 to deal with chargebacks, fees, merchant redistribution, investigations, legal efforts and IT security issues for each dollar lost to retail fraud. Mid-sized and large retailers that sell digital goods are particularly vulnerable, experiencing 3,085 fraud attempts per month and paying $3.40 for every dollar lost to mobile commerce fraud. Fraud volumes are also significantly higher among merchants that accepted payments via mobile apps or "bill to phone" features. The findings were based on input from 700 risk and fraud executives from retail and eCommerce businesses.

MILLENNIALS MOST VULNERABLE TO eCOMMERCE SCAMS

A new report from the FTC found that millennials are more at risk of being victimized by eCommerce, social media and online marketplace fraud than other generations. The study showed that millennial consumers were 25 percent more likely to report losing money to fraud than those who were aged 40 or older, and they were also likelier to report losing funds through false check schemes, fraudulent investment or job opportunities or scams that promised to fix debt-related issues.

Millennials tend to lose less money during fraud events than consumers from other generations at an average of $400 per incident. The former have lost $71 million to online shopping-related fraud over the past two years, however.

SEGASEC DEBUTS NEW ATO THREAT DETECTION SOLUTION

Security software firm Segasec debuted a new anti-fraud feature that helps online brands protect themselves from fraud and phishing attacks. It provides early detection

measures that can identify potential ATOs before customers' accounts are compromised and without alerting the fraudsters involved. The solution enables Segasec to detect fake websites and preemptively secure customers' digital accounts, and it comes as the FTC reported 1.4 million fraud incidents last year. The feature is being beta-tested among select FIs and consumers.

CRACKING DOWN ON CATFISHING

Recent FTC data revealed that romance fraud — in which cybercriminals use online dating platforms to trick members into sending them money — is the most common type of fraud in the U.S. Fraudsters based in Malaysia and Nigeria were recently exposed in a high-profile incident that saw them preying on online dating site members. The FTC reports that such scams cost consumers $143 million each year — more than any other fraud type. Online dating and classifieds platforms can tackle romance fraud by using ML-based tools to detect suspicious patterns and investing in solutions to detect social engineering schemes that target dating site users.

PAYMENT NEWS

NEW RADPAY DIGITAL WALLET FEATURES FRAUD RESISTANCE

Decentralized global payment processing company Radpay recently debuted a digital wallet that connects with mobile phones, wearables and other consumer technologies, enabling its payment capabilities via debit or credit cards. The new service can also be used for in-store payments and cracks down on card-not-present (CNP) fraud by increasing identity and transaction validation steps. A news release noted that global card fraud costs businesses more than $30 billion annually, and overall global spending on fraud detection and prevention is expected to reach $24 billion by 2024.

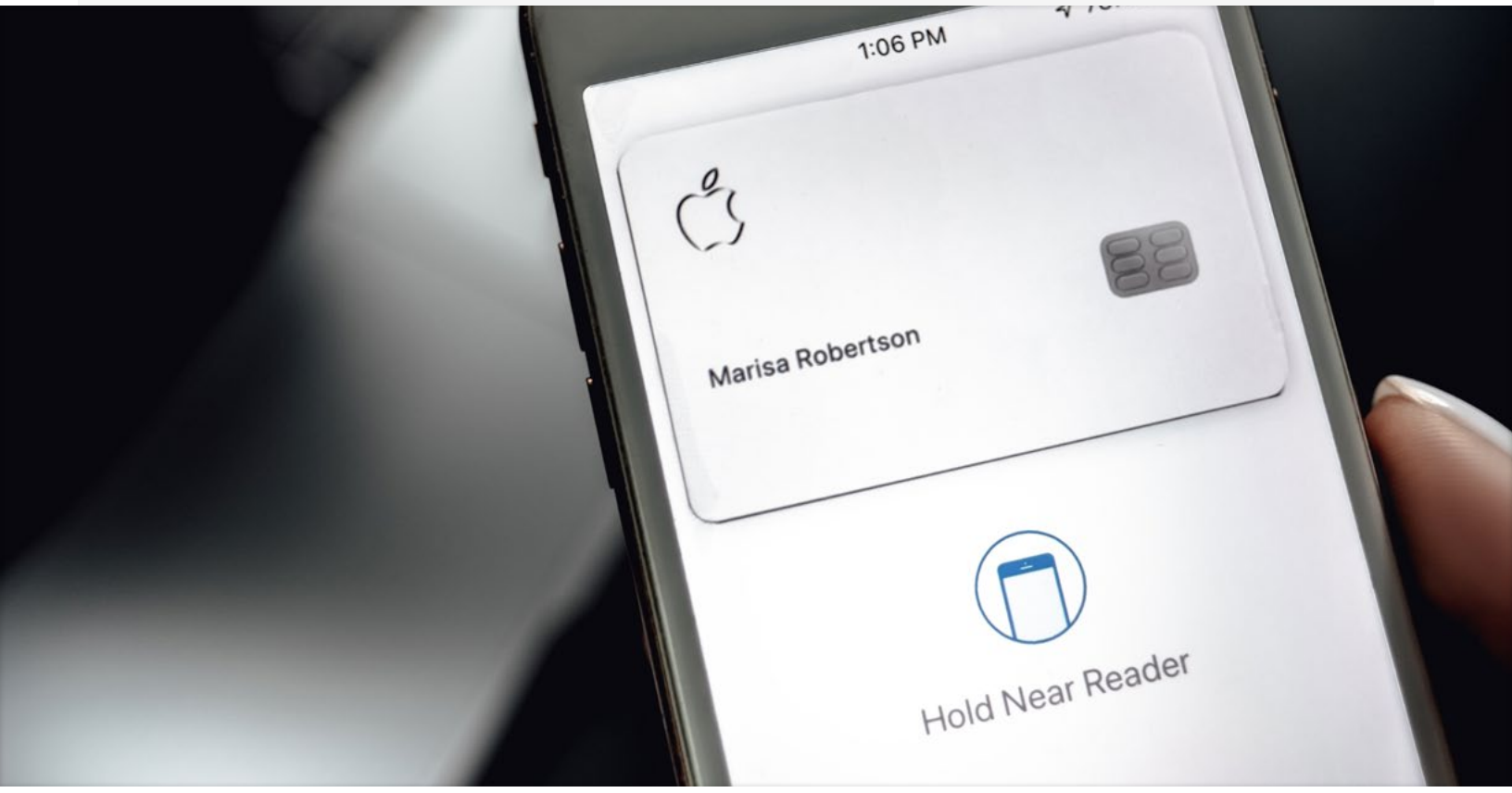
GOOGLE PAY USERS IN BRAZIL CAN PAY WITH DEBIT CARDS

Google recently launched a Google Pay-enabled debit card to help Brazilian consumers make online purchases. Joao Felix, who heads Google Pay's operations in Latin America, told Reuters the country has 60 million debit card users and 50 million credit card users. Google said it will not charge issuers, processors or retailers to utilize the system, and Banco Bradesco, Banco do Brasil, Elo, iFood, Itau Unibanco Holding, Mastercard, Rappi and Visa will allow their clients to use the debit card function. The move is expected to fuel debit card usage nationwide.

The news comes as heightened fraud activities in Brazil have prompted many online retailers to accept only credit. It also follows a June announcement that Google Pay will support PayPal, thus enabling merchants to accept payments made via the latter.

DID APPLE'S APPLE CARD GET HACKED?

A recent report indicates that Apple's new payment card solution could have been compromised. The technology giant's Apple Card acts as both a physical and virtual card, has no credit card numbers or card verification value (CVV) code and does not require a signature. These features are intended to make the solution more secure than the average credit card, but the blog 9to5Mac reported that one reader had his Apple Card cloned. The reader claimed that his card was used to make an online purchase with a virtual number on behalf of his daughter's school, though such activity could instead indicate that the school's payment system was compromised.



DEEP DIVE

HOW DATA PROVIDES BUSINESSES WITH COMPETITIVE ANALYTICS

U.S. businesses are constantly battling to stay ahead of fraudsters, and 80 percent of IT business leaders expect cyberattacks or critical breaches to occur on their watches within the year. Data holds the key to helping modern enterprises develop effective anti-fraud strategies. Many businesses are sitting on massive troves of it, but they are also facing down the three "V's" of data complexity — velocity, variety and volume — which can make tackling fraud even harder.

Fraud solutions are needed to help firms understand the meaning behind increasingly complex data sets. These solutions use Big Data analytics and ML to help businesses better detect fraud and reduce the risks of financial losses. Such insights can also help firms improve customers' experiences and lower operational costs.

Businesses that do not implement fraud solutions risk underutilizing the data they have and overemphasizing ineffective anti-fraud strategies. These businesses' strategies are often hamstrung by legacy fraud solutions that rely on data warehouse technology. Such warehouses store data from various sources but often lack the flexibility to consider new types, collect additional sources or modify queries.

Data lakes offer an alternative that could help businesses update their anti-fraud solutions. They store and collect data in large depositories, but, unlike data warehouses, they can also provide structure and meaning to information that might not be obvious. Firms can use AI and ML tools to glean insights from data lakes, allowing them to analyze new fraud threats and determine how best to respond. The following Deep Dive uncovers how data lakes are causing a sea change in the fight against fraud.

STRUCTURED VERSUS UNSTRUCTURED DATA

Comprehending how data lakes function requires understanding how the data stored in them works. Data falls into two categories: structured and unstructured. The

former refers to information kept in businesses' databases that has readily discernable meaning. It is estimated that businesses use less than half of the structured data available to them, even though it is already sorted and organized for use.

Unstructured data is more elusive and refers to the contextual information stored outside most businesses' internal systems that gives meaning to structured data. Understanding how unstructured data can be analyzed for actionable insights is necessary to determining how it functions in data lakes.

AI and ML systems often struggle to determine the meaning and sentiment behind messages. Understanding unstructured data such as photos, images, videos, text messages, social media posts, PDFs, text documents and emails can be particularly challenging for such systems. Data lakes can collect and processes this information — as well as other details like server logs, individual device data and international blacklists — to enable advanced learning tools to more comprehensively analyze data.

Most companies looking to fight fraud are failing to tap into this information. Some sources estimate that modern businesses use as little as 1 percent of their unstructured data, meaning many do not consider context when scanning for fraud. Unstructured data is projected to account for approximately 80 percent of the data enterprises process on a daily basis by 2025, however, indicating that firms face a significant gap in the amount of data they use and the high volume that will be available to them.

ROLE OF HUMAN ANALYSTS

Human analysts are often the most adept at detecting contextual particularities inherent in unstructured data. Such information usually consists of written and spoken language, the nuances of which algorithmic tools like AI and ML have difficulty understanding.

Using human employees to assess each transaction for potential fraud can drain funds and deplete resources, leading most modern companies to rely on digital tools to power large-scale anti-fraud initiatives. This means they fail to adequately invest in technologies capable of parsing unstructured data, and many possess core operating systems that cannot even store such information.

This is a problem that can be easily remedied. There are a host of technologies that can help businesses make sense of syntactic and grammatical data, but firms must first invest in technologies to store it. Data lakes are therefore crucial to enabling comprehensive data and analytics strategies. These repositories are capable of storing not only structured and unstructured data, but also semi-structured data, which exhibits characteristics of both previous forms.

Insurance providers have been particularly quick to adopt data lakes and other tools that tap into businesses'

unstructured data reserves, as the success of the insurance business model hinges on providers' abilities to detect and thwart fraudulent claims. These insurers collect unstructured data in data lakes and apply special tools to sift through it.

Some of the more common tools include decision logic and language processing functions. These solutions power a sophisticated form of text mining that allow insurers to scan text stored in data lakes for key words indicating fraud and even examine handwritten claims to assess their validity.

The applicability of data lakes, text mining and other decision logic- and language processing-based functions extends beyond the insurance and financial services sectors. Strategies that rely on both structured and unstructured data have been so successful that U.S. agencies now regularly employ them. The Department of the Treasury utilizes a cloud-based solution called the Workplace.gov Community Cloud (WC2), for example, which provides it with data analysis capabilities far beyond those offered by its previous system. The WC2 can not only collect audio files, but also transcribe them and even provide sentiment analyses based on their content.

The collection and analysis of contextual data is particularly important as more consumers' PII is compromised via targeted scams and large-scale breaches. Some estimates claim that as much as 34 percent of U.S. consumers had their PII compromised in 2018 alone, and half of all consumers can find their birthdates, passwords, credit card details or even their Social Security numbers floating on the dark web. This means fraudsters have plenty of resources available as they attempt to access accounts and steal money.

Checking the PII businesses gather from their customers is often not enough to root out fraudsters and having plans in place to collect and analyze contextual data is crucial to firms' anti-fraud efforts. Most businesses have a long way to go before they are fully equipped to combat fraudsters, but the path they must follow is clear. They must learn to store, analyze and utilize their unstructured data, and data lakes are the first step in this journey.

Businesses must contend with the three V's of data, but the right AI and ML tools can add two more V's that can aid them: visibility and value. Data lakes and AI tools can provide enterprises with greater transparency, and insights into their data can help convert unstructured data into actionable intelligence.

ABOUT

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Simility's portfolio includes real-time risk and fraud-decisioning solutions that take data-first approaches to detecting fraud vulnerabilities. The solutions combine AI and Big Data analytics to help businesses address fraud challenges as well as reduce frictions and build trust in their brands. To learn more, visit www.simility.com.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at frauddecisioning@pymnts.com.

DISCLAIMER

The Fraud Decisioning Playbook may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.