2022 LexisNexis® Risk Solutions

True Cost of Fraud™ Study

Supplemental Nutritional Assistance Program (SNAP)

Mobile and Web Channels Drive Bot and Fraud Attacks

LexisNexis® RISK SOLUTIONS

Background and Objectives

LexisNexis® Risk Solutions conducted a research study that can drive government segment revenue growth via thought leadership, particularly in the Social Services area with the Supplemental Nutrition Assistance Program (SNAP) as an initial target. This True Cost of Fraud™ Study for SNAP serves as a model framework by informing the level and impact of fraud on SNAP agencies, including the challenges, volume, and cost, as well as the resources that agencies utilize to detect and prevent fraud.

Fraud Definitions:

- Account takeover by unauthorized persons
- Fraudulent transactions due to identity fraud, SNAP benefits are exchanged for cash (trafficking – generally involving two parties — typically a household and a SNAP retailer)
- A household intentionally lies to the state to qualify for benefits or to get more benefits than they are supposed to receive

The LexisNexis Fraud Multiplier™ cost:

- Estimates the total amount of loss a firm incurs based on the actual dollar value of a fraudulent transaction

Methodology

LexisNexis® Risk Solutions partnered with KS&R, a global market research firm, to collect the survey responses for this research study.

- Data was collected online and by phone in August 2022 with a total of **74 completions** in the United States.
- Respondents included mostly senior executives responsible for fraud mitigation and decisions with SNAP.

Type		Region						
County	State	NERO	MARO	SERO	MWRO	MPRO	SWRO	WRO
49	25	15	9	9	18	12	4	7

States: Alaska, Arizona, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Montana, Pennsylvania, South Carolina, Texas, Utah, Vermont, Virgin Islands, Washington, DC

Counties from the 10 states (California, Colorado, Minnesota, New York, New Jersey, North Carolina, North Dakota, Ohio, Virginia, Wisconsin) that delegate to the county level:

Alameda, Albany, Anoka, Arapahoe, Arlington, Bergen, Boulder, Bronx, Buncombe, Burleigh, Burlington, Butte, Cass, Clermont, Cuyahoga, Dakota, Dane, Denver, Douglas, Durham, El Paso, Fairfax, Grand Forks, Hamilton, Hennepin, Henrico, Hudson, Kenosha, Kings, Milwaukee, Morris, Onondaga, Onslow, Pender, Ramsey, Richmond, San Bernardino, San Francisco, Somerset, St. Louis, Suffolk, Summit, Wake, Ward, Warren, Williams

LexisNexis® Risk Solutions was **not** identified as the sponsor of the research to reduce potential for brand bias.

Significant Differences

Statistical significance is determined by a set level of confidence sought in an estimate. Results are considered *statistically significant* if the observed difference is large based on sample size(s) and confidence level. This means the observed difference in the estimates is extreme enough to conclude with confidence *(usually 90% or 95%)* that the results would not have occurred by chance and a real difference between them exists. For this study with 74 completions at the total level, the sampling error is +/- 11.4% in order to highlight two findings as statistically different.

Directional significance, commonly referred to as practical significance, on the other hand, is when the magnitude of the difference is large enough to be meaningful given the situation, though not statistically different.

Comparing the two, note that *statistical significance* relates to **existence of a difference**, while *directional significance* refers to the **meaningfulness/magnitude of a difference**. No statistical test can determine directional significance, as it varies greatly depending on the area of study, issue at hand, etc., and instead, must be decided upon by those using the results. When reporting on directional significance, it is often helpful, especially when dealing with extremely large/small base sizes, to set a pre-determined threshold agreed upon in collaboration with the client and apply to all results.

A finite population correction may be applied to the margin of error when the sample size is at least 5% of the overall population. While this is the case for the total sample relative to the number of states and counties as we achieved just shy of 10%, the difference in significance testing outcomes for reporting is minimal. In an effort to simplify reporting and explanation for publication, the finite population correction is ignored.

Summary of Key Findings

#1: Digital transactions channels, particularly mobile devices and apps, are contributing to the cost of fraud across SNAP agencies.

Every $1 value of lost benefits through fraud actually costs SNAP agencies $3.72 based on additional costs related to labor and administrative activities. The cost of fraud is higher for agencies that have more mobile channel applications.

#2: Inadvertent household errors (IHEs) and suspicious cases not worked because of limited resources represent the majority of SNAP fraud losses. Malicious bots and the mobile channel are influencing this.

Identity-related fraud represents over half of fraud losses. The mobile channel continues to be a challenge, with agencies that have an above average volume of mobile transactions also reporting a higher number of fraud attacks per month.

#3: Verifying household composition, identifying malicious bots, address verification, and identity verification are among a number of challenges SNAP agencies have with online and mobile channel applications.

Verifying identities is directionally more of a challenge with mobile channel applications compared to those via online.

#4: There is limited use of best-practice fraud mitigation methods involving a multi-layered solution approach and the integration of fraud solutions with cybersecurity and digital customer experience operations.

Key Findings 1

Every $1 value of lost benefits through fraud actually costs SNAP agencies $3.72 based on additional costs related to labor and administrative activities. The cost of fraud is higher for agencies that have more mobile channel applications.

- While in-person is the single largest channel for SNAP application submissions and Electronic Benefits Transfer (EBT) card use, the online and mobile channels contribute to the cost of fraud.
- The volume of applications through the mobile channel is still emerging, though fraudsters have increased their focus on mobile devices and mobile apps during the past 12 months.

Distribution of Direct Fraud Costs

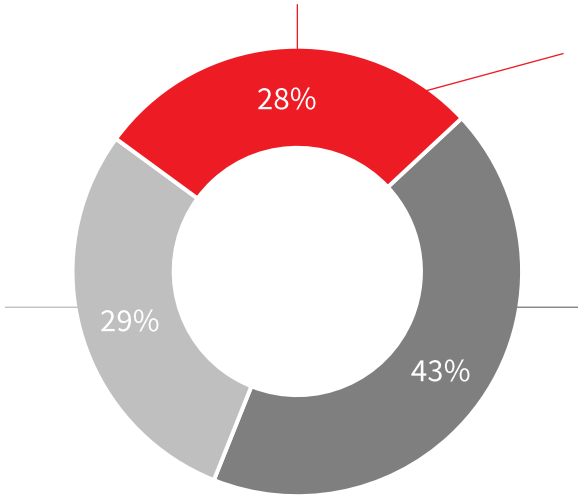
For every $1 value of benefits lost through fraud, it actually costs SNAP agencies $3.72.

This is based on the LexisNexis Fraud Multiplier, which demonstrates that the cost of fraud is more than just the lost value, but also additional costs. **Agencies that have an above average level of applications through the mobile channel have a higher cost of fraud ($4.40), with nearly half of costs related to internal labor.**

Distribution of Direct Fraud Costs

Overall
(N = 74)

Every $1 value of benefits lost is only 28% of the total cost of SNAP fraud



For the total cost of fraud, the value of benefits lost represents only 28%; there are additional costs that comprise another 72% of costs. Therefore, for every $1 value of benefits lost, it actually cost SNAP agencies 3.72.

And there are administrative costs that also contribute to the total (29%)

There are also internal labor costs that contribute to the total (43%)

Above average volume of mobile applications Fraud Multiplier = $4.40

48% of costs are attributed to internal labor

■ Internal labors costs ■ Administrative costs ■ Dollar value of benefits lost through fraud

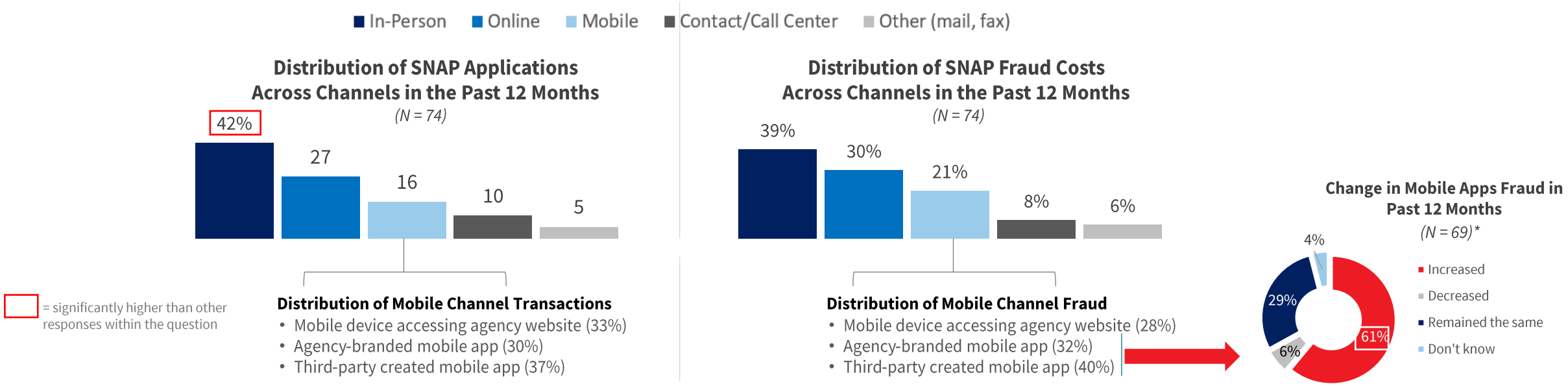
Survey Q5E: Adding to 100%, what percentage do each of the following direct fraud costs account for your total SNAP fraud losses during the past year?

Distribution of SNAP Applications and Fraud Across Channels

In-person is the single largest channel for submitting SNAP applications, though online applications represent just over one-quarter of these transactions and account for a similar level of SNAP fraud while mobile channel fraud is growing.

Mobile channel submissions are limited but are likely to grow given the increased use of mobile transactions in the larger market. Mobile apps account for the majority of submissions and fraud through this channel, with 61% of agencies that allow these types of transactions saying that fraud has increased through them during the past 12 months.

Distribution of SNAP Applications and Fraud Costs Across Channels in the Past 12 Months

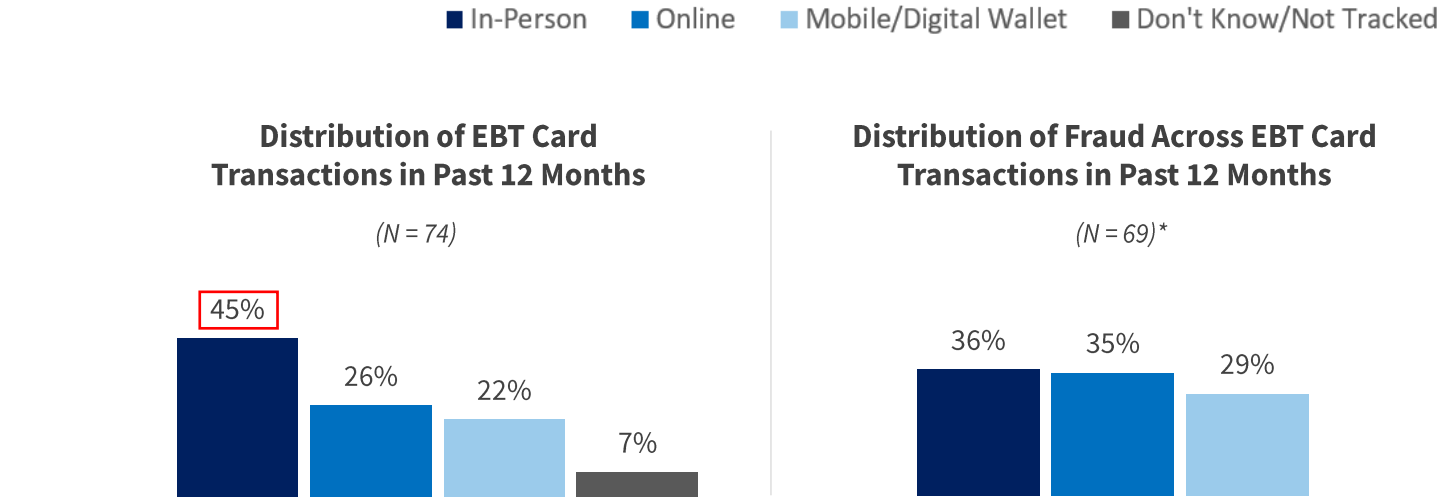


Survey Q1: Please indicate the percentage of SNAP applications submitted over the past 12 months across each of the following channels used by your agency.
Survey Q3: You indicated that approximately [INSERT # FROM Q1_4] % of your agency's total number of SNAP applications during the past 12 months were submitted through a mobile device. Of that [INSERT # FROM Q1_4] %, what is the distribution of applications through the following:
Survey Q8: Adding to 100%, please indicate the percent of fraud costs generated through each of the following channels currently used for SNAP applications (as a percentage of total annual fraud losses).
Survey Q11: For SNAP applications conducted through a mobile device or mobile app, what percentage do the following account for applications fraud?
Survey Q11B: Has fraud with applications through mobile devices or mobile apps increased, decreased or stayed during the past 12 months?

Distribution of EBT Card Transactions and Fraud Across Channels

In-person is also the single largest channel used for Electronic Benefits Transfer (EBT) transactions, though online and mobile use contributes to EBT card fraud just as much as in-person use.

Distribution of Electronic Benefits Transfer (EBT) Card Transactions and Fraud Costs Across Channels in the Past 12 Months



= significantly higher than other responses within the question

* Asked only of agencies that track EBT card transactions by channel

Survey Q4: Please distribute 100 points to indicate the approximate percentage that total transactions/purchases during the past 12 months were completed through the following methods.
Survey Q9: Adding to 100%, please indicate the distribution of fraud across the following types of EBT card transactions during the past 12 months.

Key Findings 2

Inadvertent household errors (IHEs) and suspicious cases not worked because of limited resources represent the majority of SNAP fraud. Malicious bots and the mobile channel are influencing this.

- SNAP agencies that experience an above average (>38%) distribution of fraud losses due to IHEs have a higher cost of fraud compared to the overall average.
- Identity-related fraud represents over half of fraud losses.
- The mobile channel continues to be a challenge, with agencies that have an above average volume of mobile transactions also reporting a higher number of fraud attacks per month. They are also more likely to have indicated an increase in bot attacks during the past 12 months.

Key Finding 2

Distribution of SNAP Fraud Losses

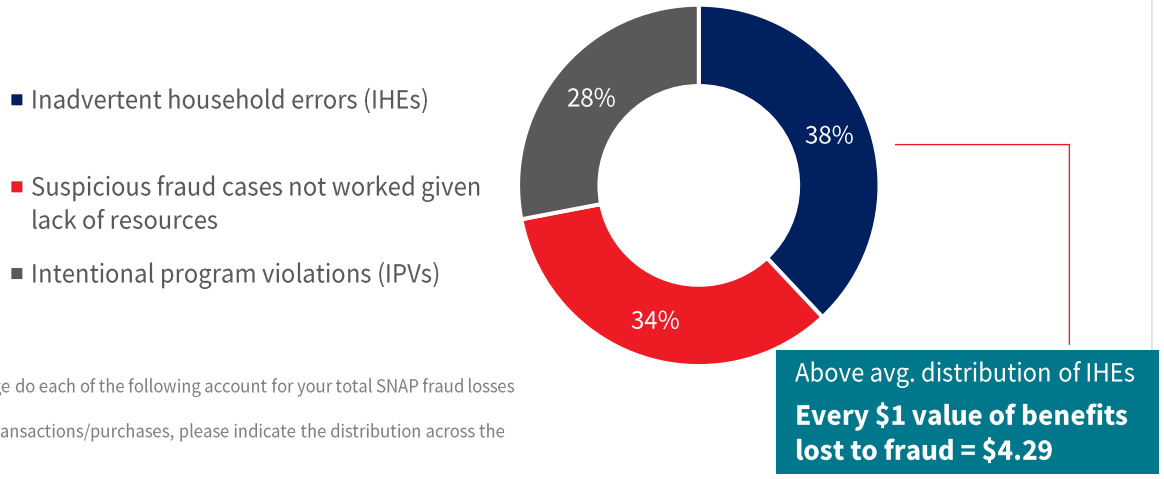
A majority of SNAP application fraud losses are either suspicious cases not worked on given lack of resources or inadvertent household errors (IHEs) that have not been formally designated as an intentional program violation but could be provable or reasonably be assumed as fraud.

EBT card-related fraud losses are distributed similarly across various factors, including card not present, counterfeit or doctored cards and stolen/card theft. SNAP agencies that experience an above average (>38%) distribution of fraud losses due to IHEs have a higher cost of fraud compared to the overall average.

Distribution of SNAP/Electronic Benefits Transfer (EBT) Card Fraud Losses

Distribution of SNAP Fraud Losses by Activity

(N = 74)



Distribution of EBT Card-Related Fraud Losses

(N = 74)

Survey Q5C: Adding to 100%, what percentage do each of the following account for your total SNAP fraud losses during the past year?
Survey Q10: For fraud losses related to EBT transactions/purchases, please indicate the distribution across the following types of card fraud.

LexisNexis® RISK SOLUTIONS

Key Finding 2

Distribution of SNAP Fraud Losses

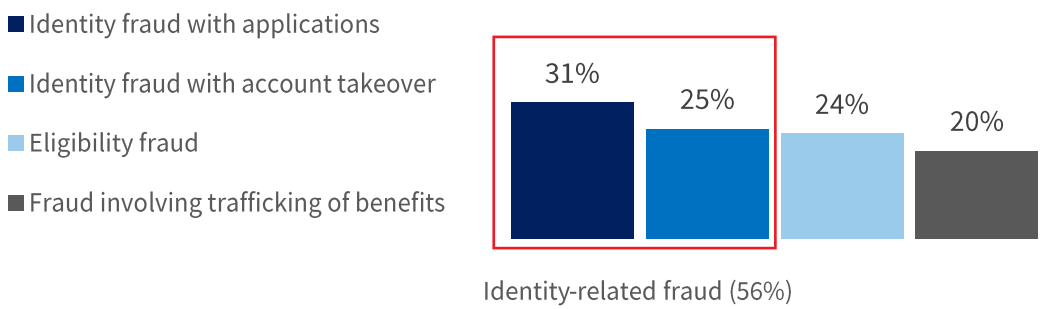
Identity-related fraud accounts for over half of SNAP fraud losses. Automated malicious bot attacks have increased.

As shown later, the rise of malicious bot attacks is a driver of identity verification challenges for roughly half when assessing the risk of online and mobile channel applications. Directionally, those with an above average volume of applications through the mobile channel areeven more likely to indicate an increase in bot attacks from last year.

Distribution of SNAP Fraud Losses by Activity and Fraud Type

Distribution of Fraud Losses by Fraud Type

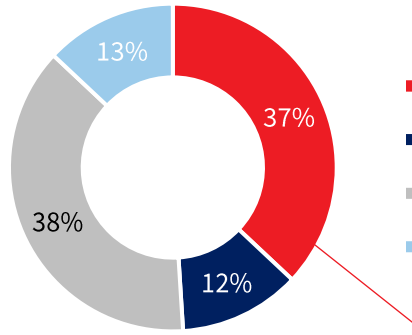
(N = 74)



Automated Bot Attacks – Trends

(N = 52)

Compared to last year, bot attacks have…



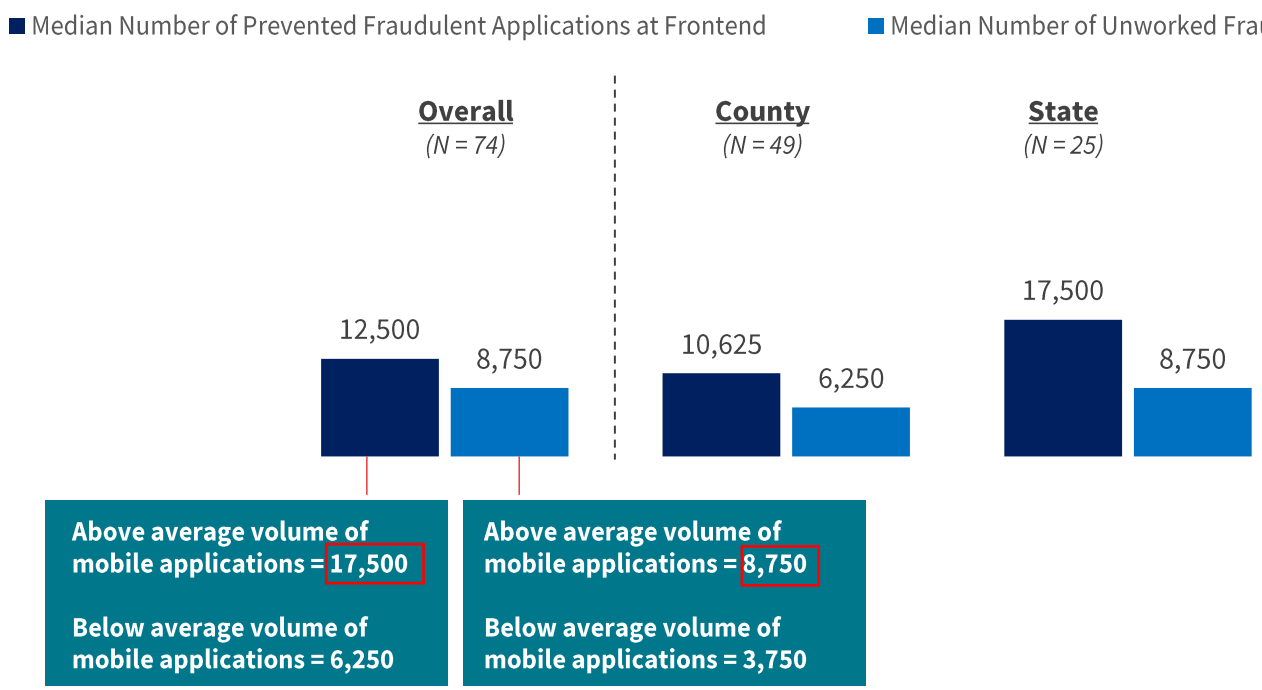
Above average volume of mobile applications (45% say increased Bots)

Survey Q6: Approximately, how much of your fraud losses would you attribute to each of the following types of fraud?
Survey Q15A: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks?
Survey Q15B: How does this compare to the same time last year? Would you say the percent of monthly automated malicious bot attacks has:

Median Volume of Fraudulent Applications

SNAP agencies that have a higher, above average volume of applications submitted through the mobile channel are dealing with more fraud attacks per month, including those that are unworked due to limited resources.

Median Volume of Fraudulent Applications per Month



= significantly higher than other responses within the question

Survey Q13: In a typical month, approximately how many fraudulent applications are prevented at the front-end by your agency?
Survey Q14: In a typical month, approximately how many fraudulent applications are unworked/not prosecuted at your agency?

Key Findings 3

Verifying household composition, identifying malicious bots, address verification, and identity verification are among a number of challenges SNAP agencies have with online and mobile channel applications.

- Verifying identities is directionally more of a challenge with mobile channel applications compared to those via online.
- Those experiencing increased bot attacks are directionally more likely to rank verification of household composition as an online and mobile channel challenge.

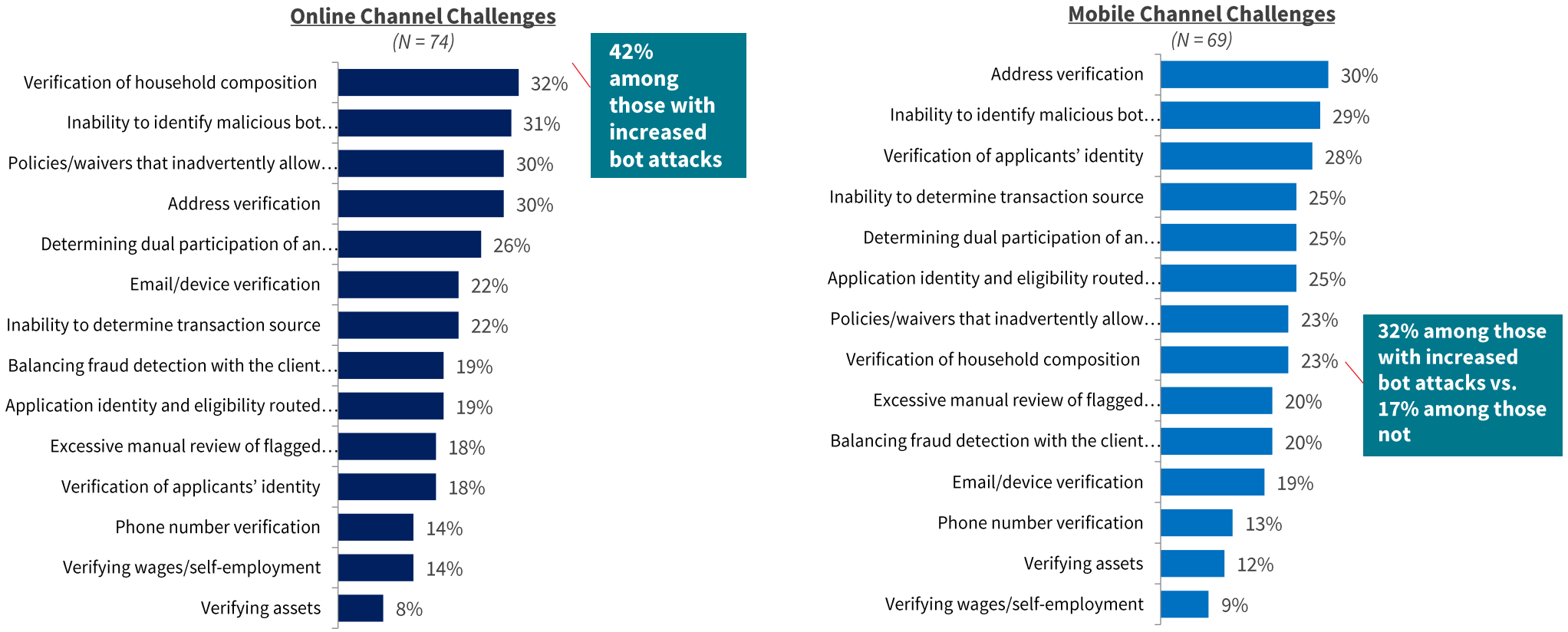
Key Finding 3

Top Online and Mobile Applications Fraud Challenges

There are many similar fraud detection challenges between online and mobile channel applications, including identifying malicious bot attacks. Verifying applicants' identity is directionally more challenging with mobile channel applications.

Those experiencing increased bot attacks are directionally more likely to rank verification of household composition as an online and mobile channel challenge.

Top Online and Mobile Channel Applications Fraud Challenges *(% Ranked in Top 3)*

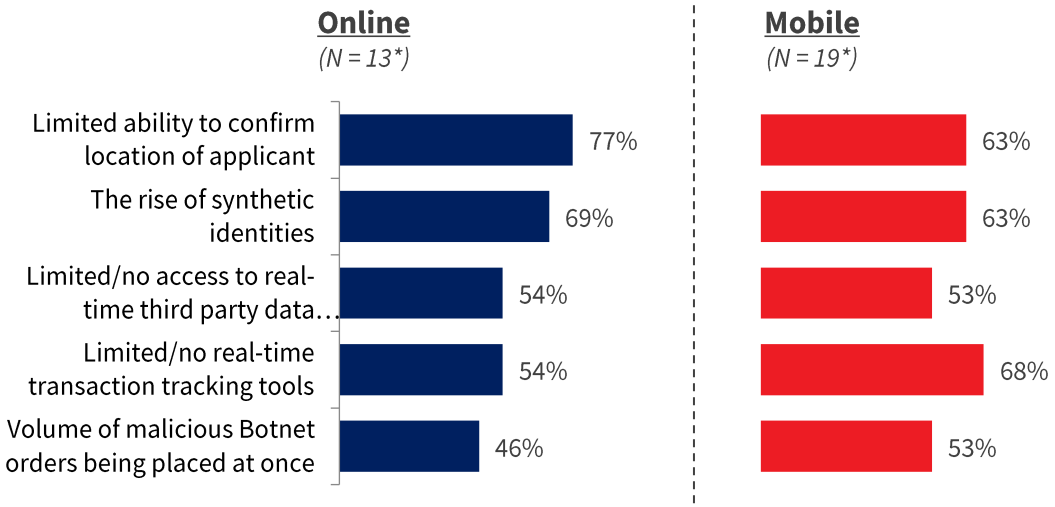


Survey Q12A: Please rank the top 3 challenges related to fraud when the application process is submitted online through your agency's website (via a PC).
Survey Q12B: Please rank the top 3 challenges related to fraud when the application process is submitted through a mobile device or mobile app.

Top Factors Challenging Customer Identity Verification

Confirming location of applicant, the rise of synthetic identities, malicious bot attacks and the need for real-time data are challenges with identity verification.

Top Factors Making Customer Identity Verification a Challenge *(% Ranked in Top 3)*



*No segment analysis because of small sample size

Survey Q12C: Please rank the top 3 factors that make customer identity verification a challenge when SNAP applications are submitted through your agency website (via a PC).
Survey Q12D: Please rank the top 3 factors that make customer identity verification a challenge when SNAP applications are submitted a mobile device or mobile app.

Key Findings 4

There is limited use of best-practice fraud mitigation methods involving a multi-layered solution approach and the integration of fraud solutions with cybersecurity and digital customer experience operations.

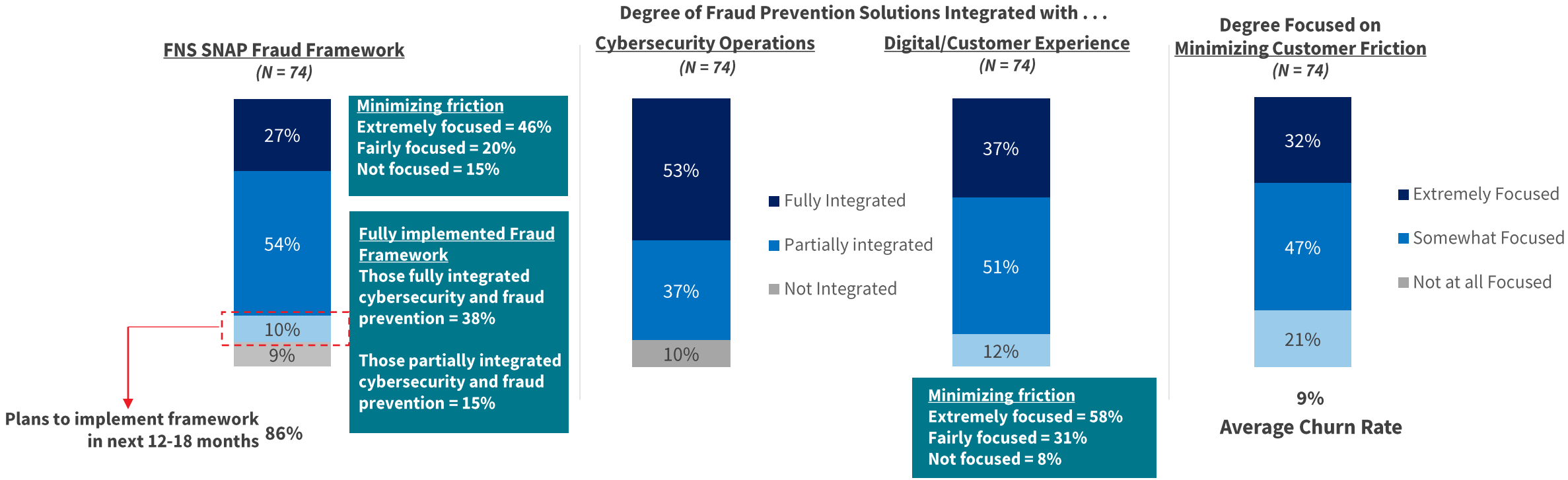
- Few agencies have fully implemented the USDA Food and Nutrition Service (FNS) SNAP Fraud Framework, though over half have partially done so.
- FNS SNAP Fraud Framework, though over half have partially done so.
- The use of fraud mitigation solutions is limited, particularly those that assess digital identity attributes to address challenges with online and mobile channel fraud detection challenges.

FNS SNAP Fraud Framework and Other Best Practice Approaches

Many agencies are still in the process of implementing the SNAP Fraud Framework, though agencies are moving towards this. Half of participating agencies have integrated their cybersecurity operations with their fraud prevention efforts.

Fewer have fully integrated their digital/customer experience with fraud prevention efforts as a majority are less than extremely focused on minimizing friction. Those that are extremely focused on minimizing customer friction are more likely to have implemented these best practice approaches.

FNS SNAP Fraud Framework and Other Best Practices Implementation



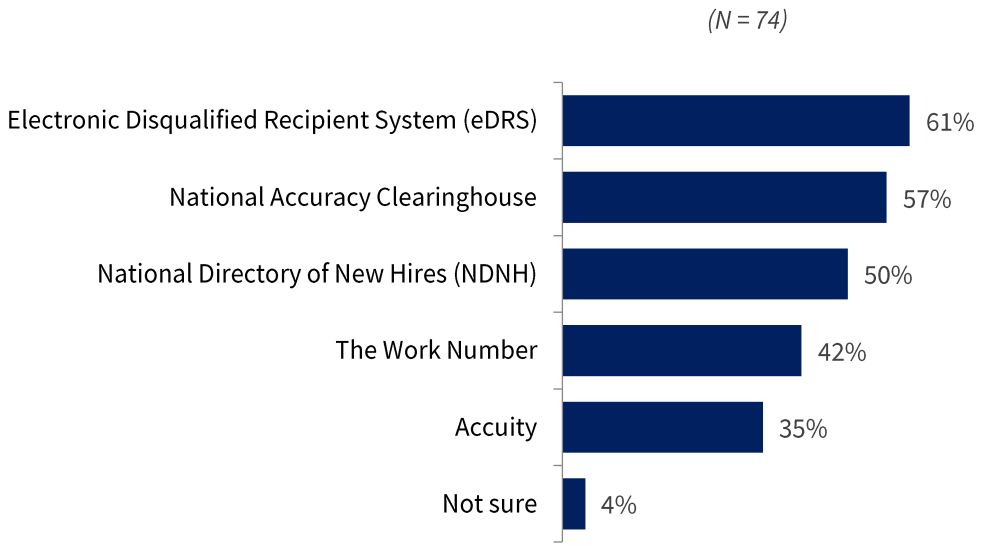
Survey Q16A: Has your agency implemented recommendations from the FNS SNAP Fraud Framework?
Survey Q16B: Does your agency have plans to implement the FNS SNAP Fraud Framework during the next 12 – 18 months?
Survey Q18: To what degree has your agency integrated its cybersecurity operations with its fraud prevention efforts?
Survey Q19: Approximately, what is your agency's typical rate of churn (i.e., the number of clients that are denied and reapply within the same eligibility period)?
Survey Q19B: To what degree is your agency focused on minimizing customer friction when a SNAP application is completed online (via a PC) or through a mobile device or mobile app?
Survey Q20: To what degree has your agency integrated its digital/customer experience operations with its fraud prevention efforts?

Providers Helping to Detect and Mitigate SNAP Fraud

An Electronic Disqualified Recipient System (eDRS) is mentioned by many participating agencies as a source of fraud detection information. The National Accuracy Clearinghouse and National Directory of New Hires (NDNH) are similarly mentioned.

Fewer have fully integrated their digital/customer experience with fraud prevention efforts as a majority are less than extremely focused on minimizing friction. Those that are extremely focused on minimizing customer friction are more likely to have implemented these best practice approaches.

Sourcing Information from Providers to Detect and Mitigate SNAP Fraud

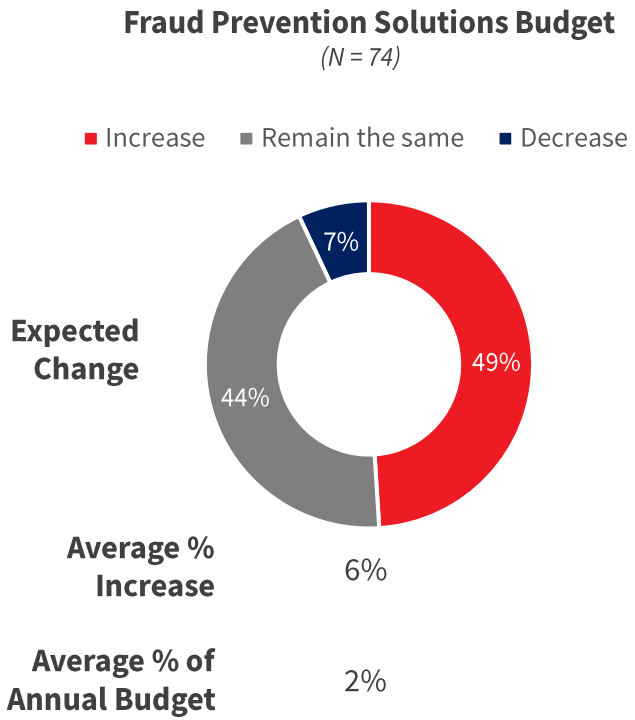


Survey Q17B: Does your agency participate in/source information from any of the following in order to detect and mitigate SNAP fraud?

Fraud Prevention Solutions Cost

The amount of budget dedicated to the detection and mitigation of fraud is 2% on average, with nearly half of participating agencies expecting this to increase next year by an average of 6%.

Fraud Prevention Solutions Budget



Survey Q5D: Approximately, what percent of your annual budget is dedicated to the detection and prevention of fraud?
Survey Q5F: Do you expect the amount you spend on fraud prevention solutions to increase, remain the same, or decrease in the next year?

Key Finding 4

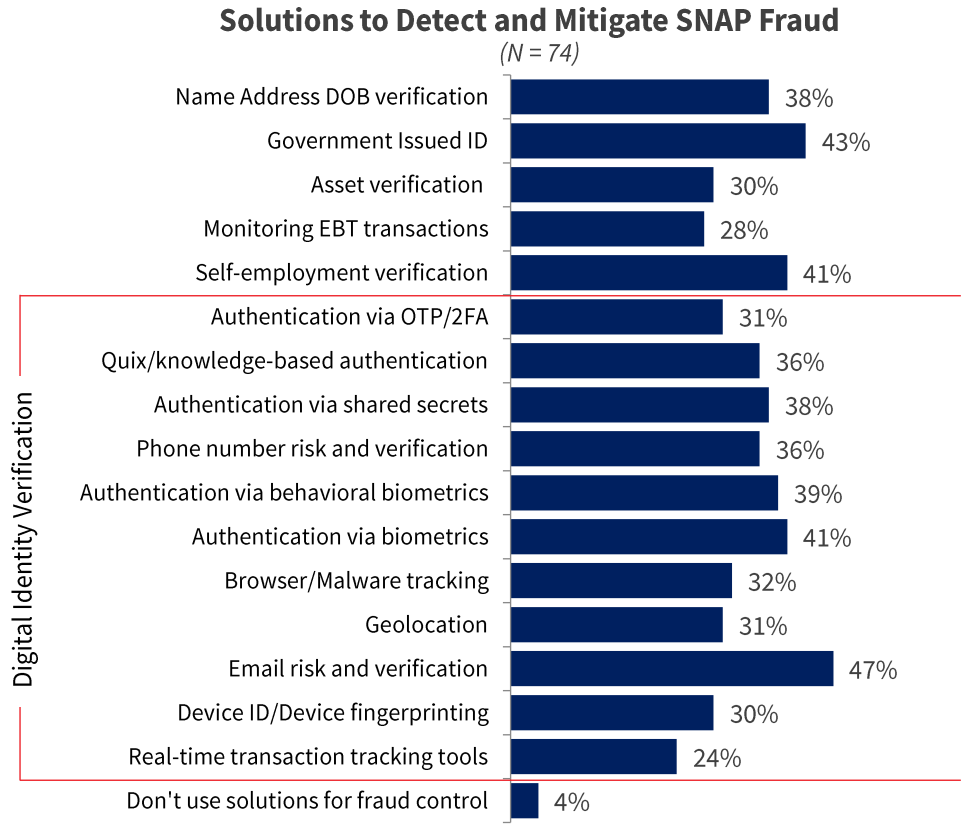
Fraud Prevention Solution Use

Overall, there is limited use of digital identity solutions that specifically support fraud detection in the online and mobile channels.

These types of solutions are designed to assess both individual and device risks (E-mail Risk Verification, Geolocation, Device ID, Biometrics and Behavioral Biometrics) and risk of the transaction (Real-Time Fraud Detection), which provide fast, seamless, and "behind the scenes" fraud detection that reduces customer efforts and delays while more effectively distinguishing synthetic identities and malicious bots.

Fraud Prevention Solutions Budget & Use

In other LexisNexis® Risk Solutions True Cost of Fraud™ studies, findings have shown that organizations which use a multi-layered solutions approach involving both traditional and digital identity verification solutions along with integrating cybersecurity and the digital customer experience with these solutions experience a lower cost of fraud and greater effectiveness at detecting and mitigating fraud.



Survey Q17: Which solutions does your agency currently use to detect and mitigate fraud associated with SNAP applications/eligibility, account login and/or trafficking of benefits?

= significantly or directionally higher than same response in other segment

For more information, please visit

https://risk.lexisnexis.com/GovFraud

or call 1-888-216-3544

About LexisNexis Risk Solutions
LexisNexis® Risk Solutions (lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.