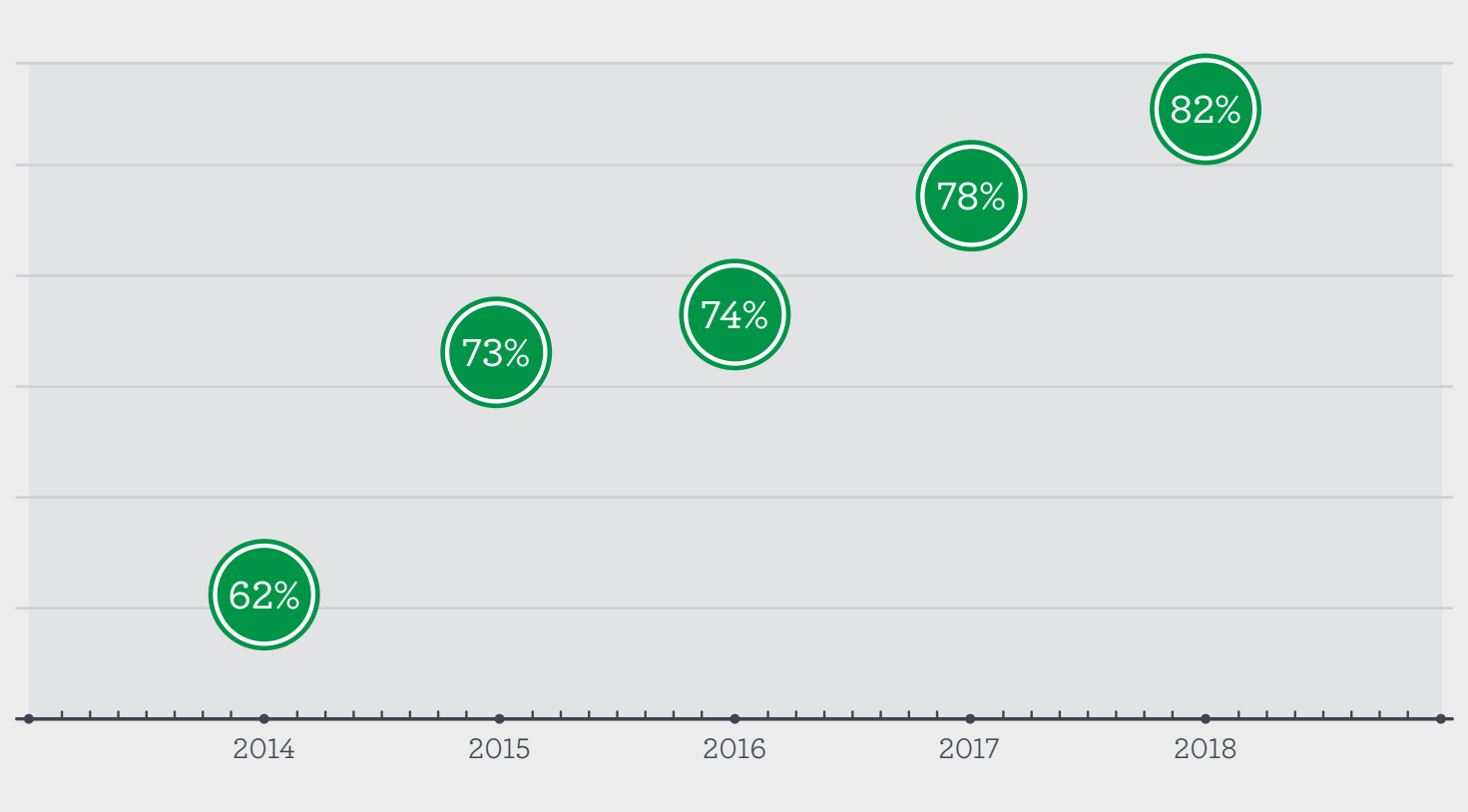
Payments fraud hits record of 82% in 2018

WELLS FARGO

Payments fraud continues to rise, and shows no signs of abating, with a record 82% of organizations hit by attempted or actual payments fraud in 2018, according to the 2019 AFP® Payments Fraud and Control Survey Report underwritten by J.P. Morgan.

Payments fraud has increased significantly over the past five years, surging 20% since the uptick in 2014.



Fraud sources and perpetrators

64%

64% of attempted or actual payments fraud attacks resulted from actions of an individual outside the organization.

58%

58% of companies reported that payments fraud originated via BEC.

22%

22% of companies experienced fraud perpetrated by third parties or outsourcers, such as a vendor, a 4% increase over 2017.

21%

21% of companies reported attempted/actual Account Takeover fraud, which includes malware and other methods, a jump of 13% year-over-year.

Business email compromise (BEC) is becoming the method of choice for fraudsters

BEC fraud is evolving and becoming more sophisticated, making it difficult to detect. A record **80%** of companies were targets of BEC scams in 2018, a significant jump from the 64% reported in 2015, and over half of the companies impacted suffered a financial loss.

Wire transfers remain a prime target for BEC scams, with **43%** of companies experiencing wire transfers BEC payments fraud in 2018. **33%** reported fraudsters used BEC scams to perpetrate ACH credits fraud, a huge increase from the 12% reported in 2017. Meanwhile, the number of companies reporting BEC via check payments dropped significantly from 34% to 20% in 2018.

Payments methods impacted by BEC

Wire transfers	43%
ACH credits	33%
ACH debits	21%
ACH checks	20%
Corporate credit cards (e.g., purchasing and fleet)	10%

Fraudsters are becoming more clever and sophisticated with their email techniques.

81% of respondents received emails from fraudsters posing as senior executives using spoofed email addresses directing a transfer of funds to the fraudsters' accounts.

44% received emails impersonating vendors directing payments, based on authentic invoices, to fraudsters' accounts.

33% received emails from fraudsters pretending to be third parties requesting changes to bank accounts and/or instructions.

Other types of email used in the attacks included:

- Emails from fraudsters who hacked senior executives and used legitimate outlook accounts
- Email impersonating HR department, directing employees to sign in using links
- Email requesting change in payroll bank information
- Faxes requesting revisions in bank instructions

Fraudsters are shifting their focus to ACH transactions to avoid detection

In 2018, the number of companies reporting ACH debits fraud climbed to **33%** in 2018, versus **28%** in 2017, while ACH credits fraud jumped from **13%** to **20%** year-over-year.

The number of organizations impacted by wire transfers fraud continues to rise with **45%** of companies reporting fraudulent wire transfers activity in 2018.

Financial impact in 2018:

43% of businesses said they suffered a financial loss as a result of some type of payments fraud.

54% of organizations reported financial losses as a result of BEC in 2018, marking the first time since AFP began tracking the data that a majority of businesses suffered financial losses due to BEC attacks.

57% of larger organizations (annual revenue of at least $1 billion) had losses as a result of BEC.

49% of smaller organizations (annual revenue less than $1 billion) suffered losses from BEC.

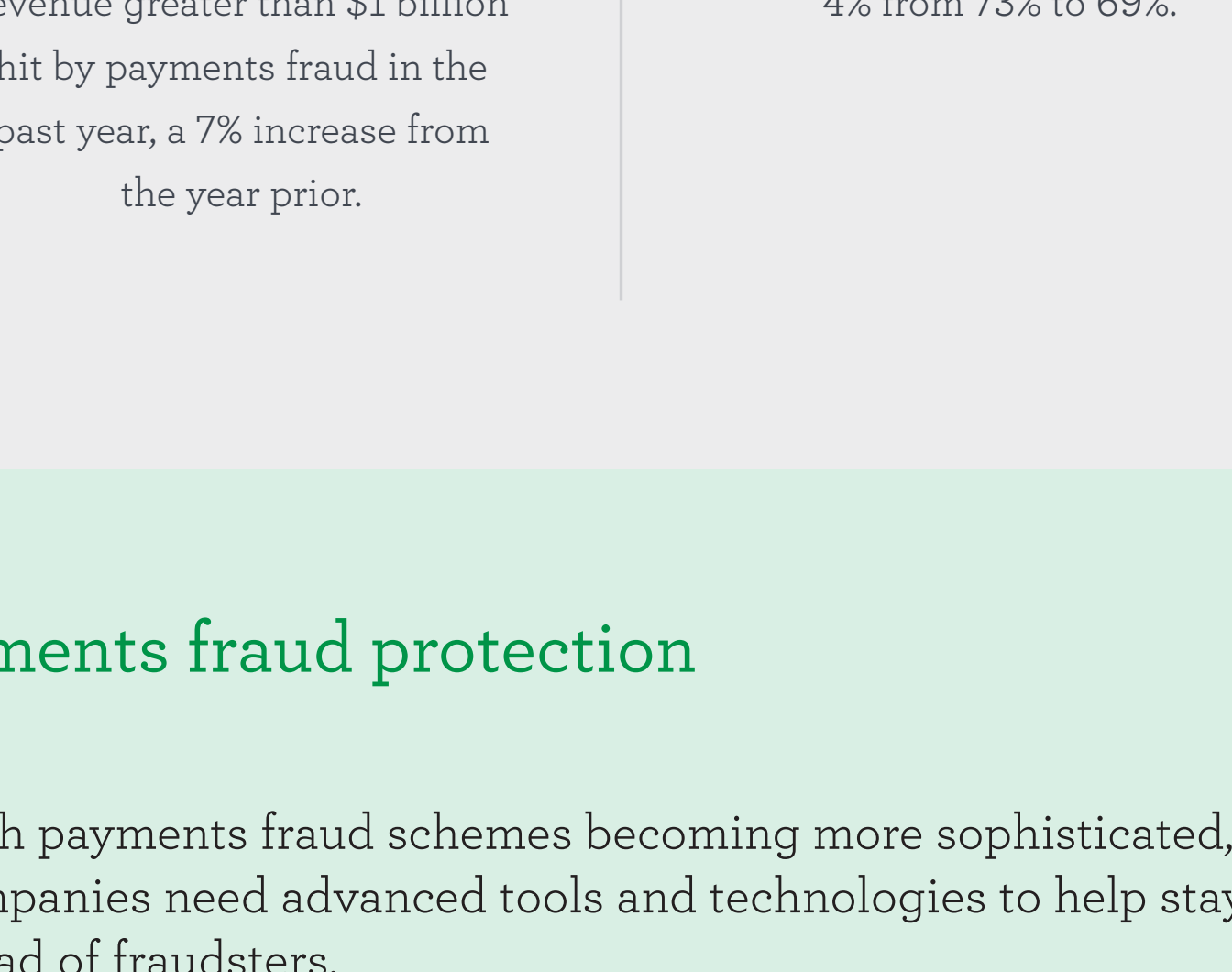
$12.5 billion[1]

in global financial losses due to BEC

between October 2013 and May 2018

1. Federal Bureau of Investigation

Which companies were impacted by fraud?



Large companies were severely impacted with a record-setting 87% of large companies with revenue greater than $1 billion hit by payments fraud in the past year, a 7% increase from the year prior.

Companies with revenue below $1 billion experienced fewer fraud attempts in 2018, down 4% from 73% to 69%.

Payments fraud protection

With payments fraud schemes becoming more sophisticated, companies need advanced tools and technologies to help stay ahead of fraudsters.

BEC fraud protection

76% of companies are adopting stronger internal controls that prohibit payment initiation based on emails or other less secure messaging systems.

76% are educating their staff about the threat of BEC and how to recognize phishing attempts.

68% of companies are implementing policies for providing appropriate verification of any changes to existing invoices, bank deposit information, and contact information.

65% are adopting at least a two-factor authentication or added layers of security for access to company network and payments initiation.

Security credential protection

76% of organizations perform daily reconciliations to protect against attacks on security credentials.

56% ensure disaster recovery plans include the ability to continue with strong controls.

48% restrict company network access for payments to only company-issued devices.

10% dedicate a PC for payment origination, with no links to email, web browsing, or social networks.

ACH fraud protection

Companies are implementing various tactics to protect against ACH fraud.

65% of companies reconcile accounts daily to identify and return unauthorized ACH debits.

63% block all ACH debits except on a single account set up with ACH debits filter/ACH positive pay.

37% block ACH debits on all accounts.

Check fraud protection

88% of companies used positive pay to protect against check fraud.

72% of organizations used segregation of accounts as a check fraud protection tool.

The BEC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions.

Between December 2016 and May 2018, there was a

136% increase[1]

in identified global exposed losses.

1. Federal Bureau of Investigation

The scam has been reported in all 50 states and in 150 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 115 countries.

Domestic and international exposed dollar loss:

$12,536,948,299[1]

Domestic and international incidents:

78,617

1. Federal Bureau of Investigation

"It is alarming that the rate of payments fraud has reached a record high despite repeated warnings. In addition to being extremely vigilant, treasury and finance professionals will need to anticipate scams and be prepared to deter these attacks."

— AFP President and CEO Jim Kaitz