PulseReport
GATEPOINT RESEARCH

Strategies to Prevent Attacks on Commercial Accounts

ACI payment systems

Summary Results • November 2013

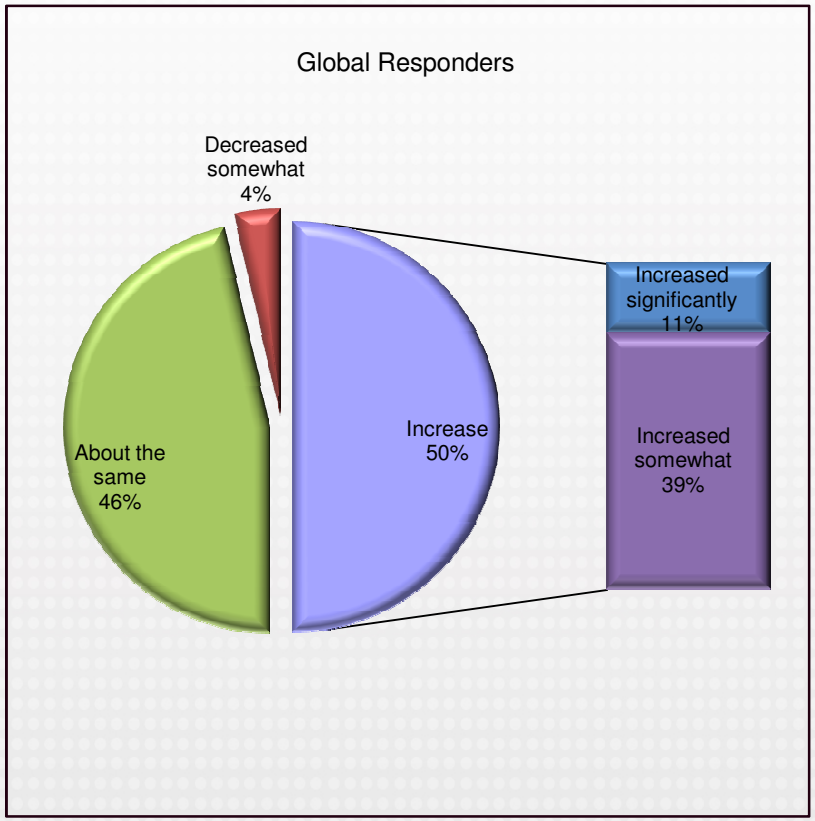
Program Overview

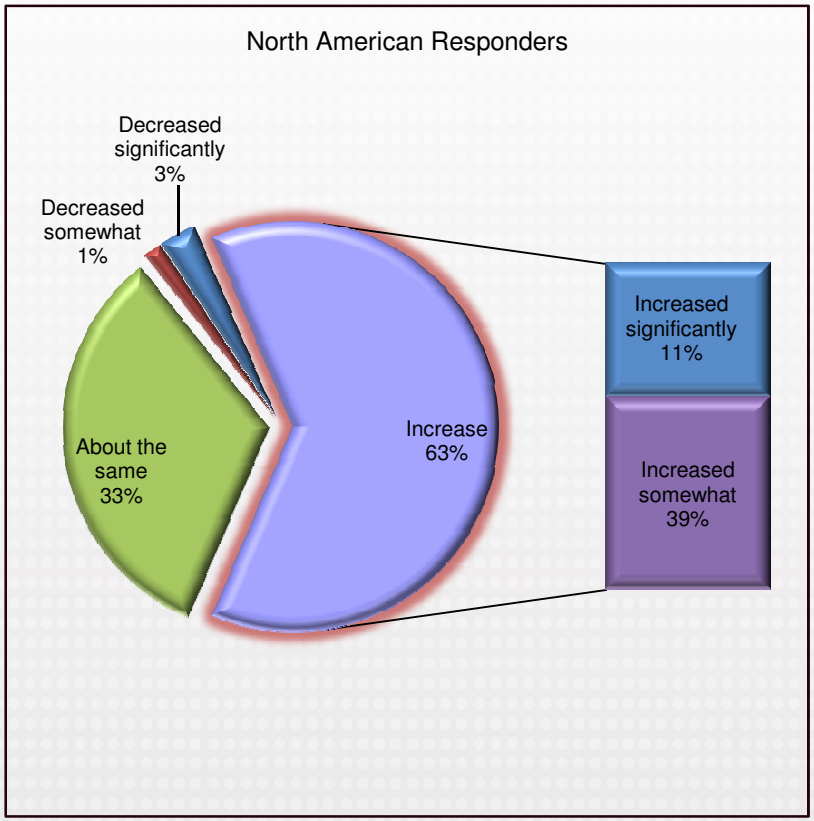
- In Q4 2013, Gatepoint Research invited selected executives from the financial services industry to participate in a survey themed *Strategies to Prevent Attacks on Commercial Accounts.*
- Candidates were invited via email and 100 executives participated, 70 from North America and 30 globally.
- Survey participants were senior finance, fraud and operations decision makers - 76% held titles of Director or above. Of those, 50% were VPs and 3% were CxOs.
- 100% of responders participated voluntarily.

Observations and Conclusions

- More North American responders perceive an increase in online account takeover of commercial accounts than their global counterparts (63% vs. 50%).
- Global responders are generally less concerned than their North American colleagues about the negative impacts from online account takeovers and ACH fraud.
- North American responders concentrate most on device protection such as device ID, secure browsing, and malware protection (84%); global responders concentrate most on payment specific transaction monitoring (89%) and online session anomaly detection (82%).
- While responders as a whole are confident in their fraud-fighting tools, they also admit they are not satisfied with cross-channel fraud monitoring and online session anomaly detection.
- When asked if they've experienced commercial account fraud, the global market admitted higher incidence of attempts – 54% have experienced it in the last 12 months, versus 40% in North America.
- Experience of commercial account fraud losses is much higher globally than in North America – 43% versus 14% in the last 12 months.
- 18% of responders admit to being only mostly or partly compliant with current security regulations.
- When buying a new fraud mitigations solution, North American responders worry most about cost, integration, and vendor credibility. Globally, vendor credibility also tops the list.

What is your perception of the rate of online account takeover attacks on commercial accounts over the past 12 months?

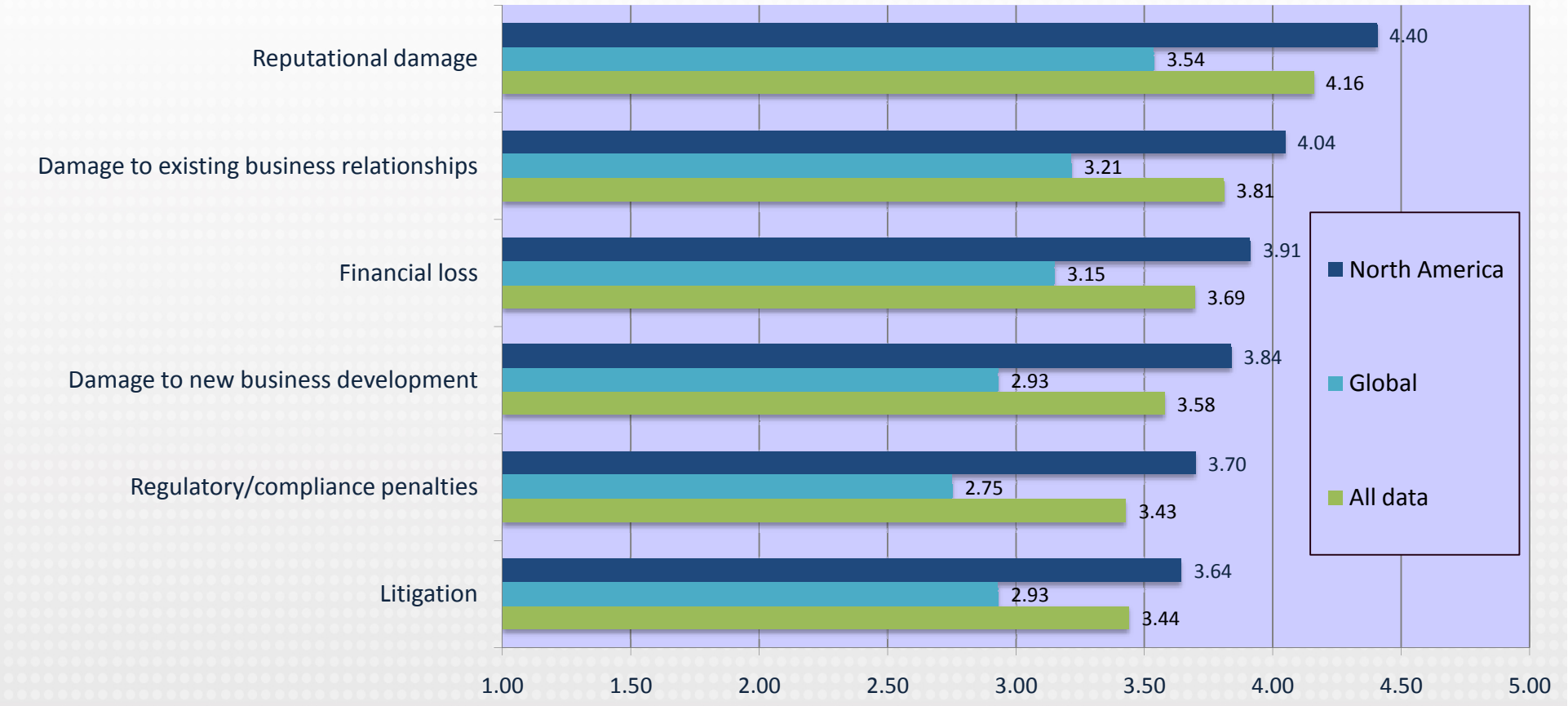




More North American perceive an increase in online account takeover of commercial accounts (63% vs. 50% for global responders).

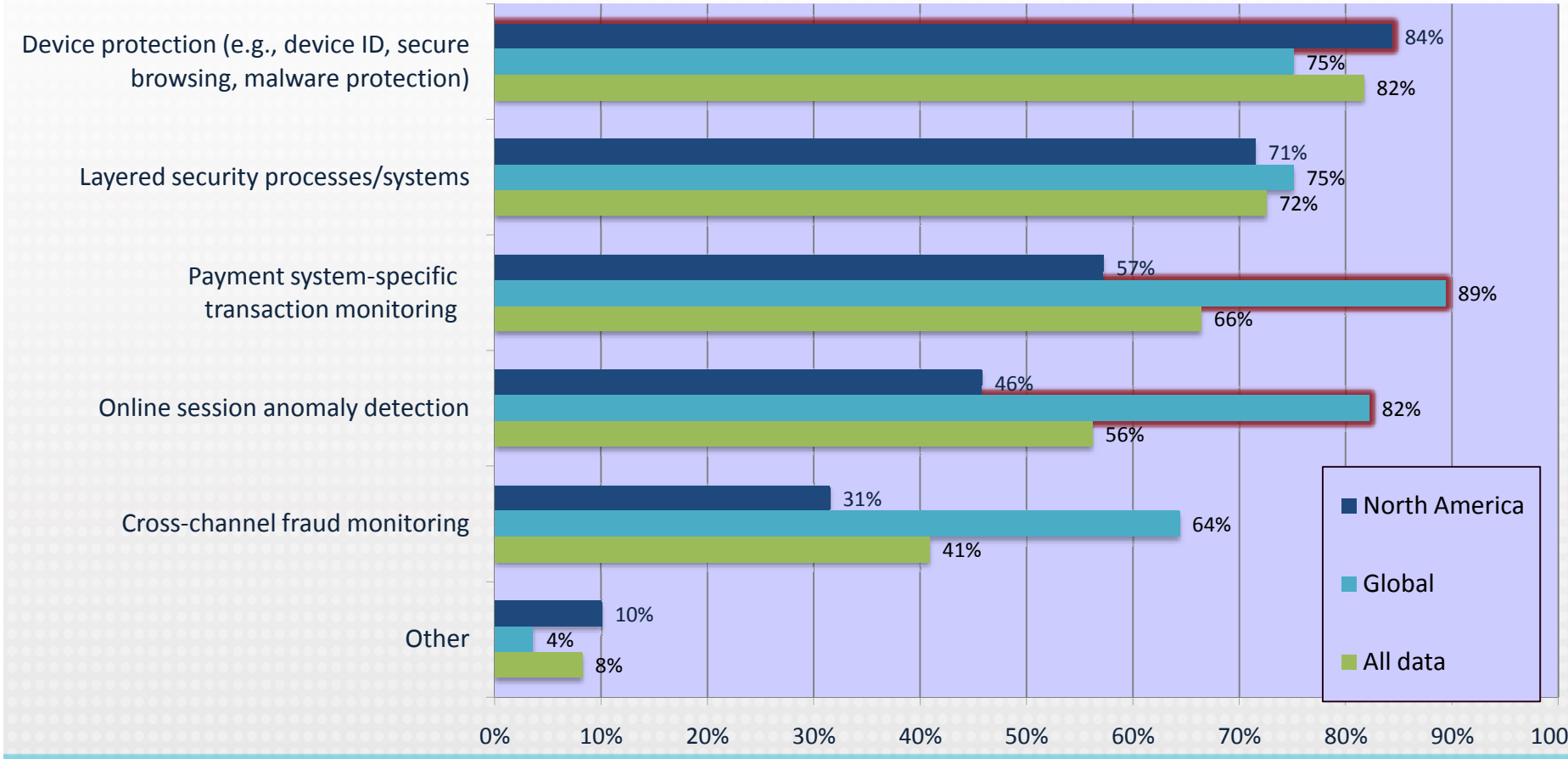
What is your view of the potential negative impacts on your organization from online account takeovers and wire transfer/automated clearinghouse (ACH) fraud?

(Rate 1-5, 1=Little or no impact, 5=Severe impact):



Global responders are generally less concerned than their North American colleagues about the negative impacts from online account takeovers and ACH fraud.

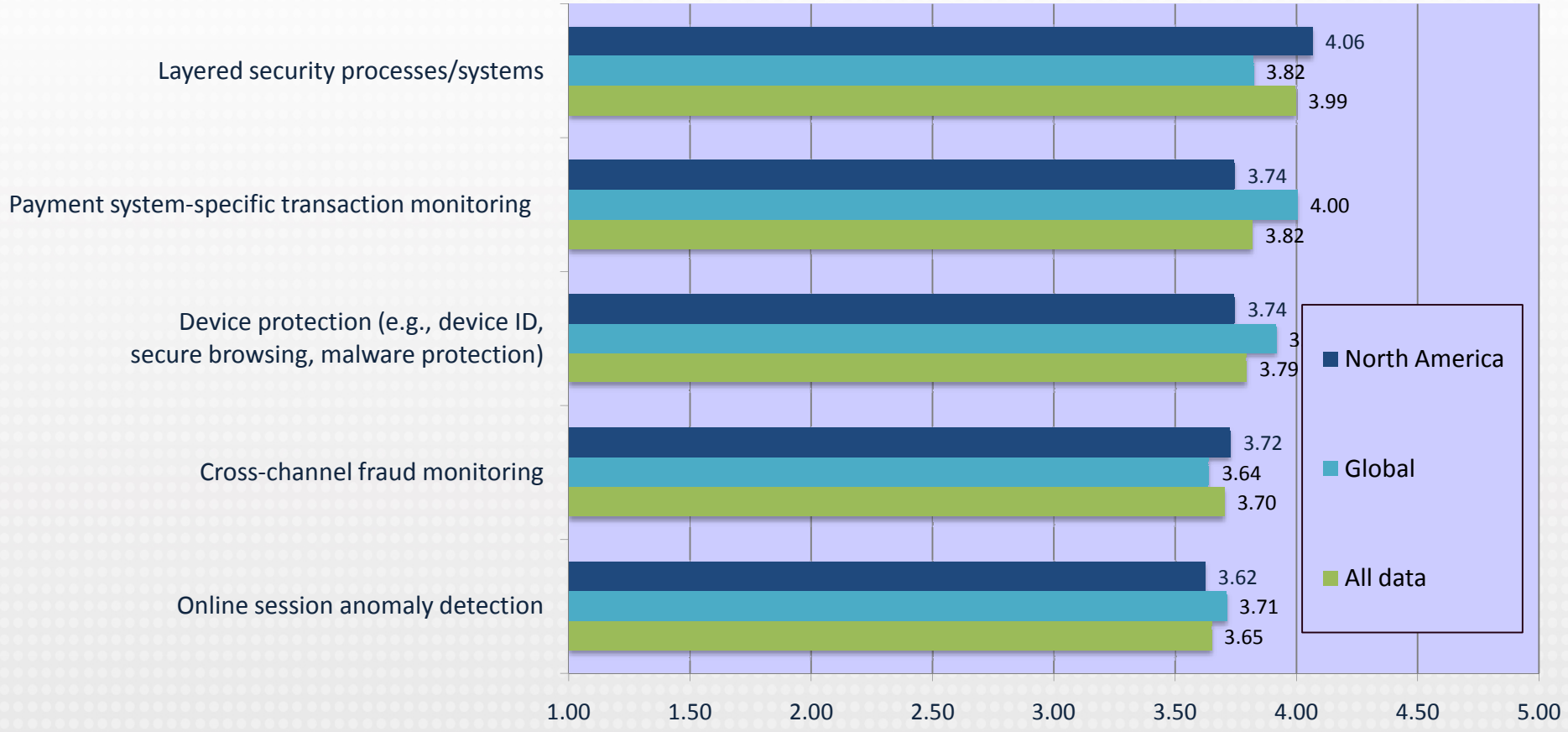
Do you currently utilize any of the following fraud monitoring solutions to help protect against online account takeover and/or ACH and wire fraud?



North American responders concentrate most on device protection; global responders concentrate most on payment specific transaction monitoring and online session anomaly detection.

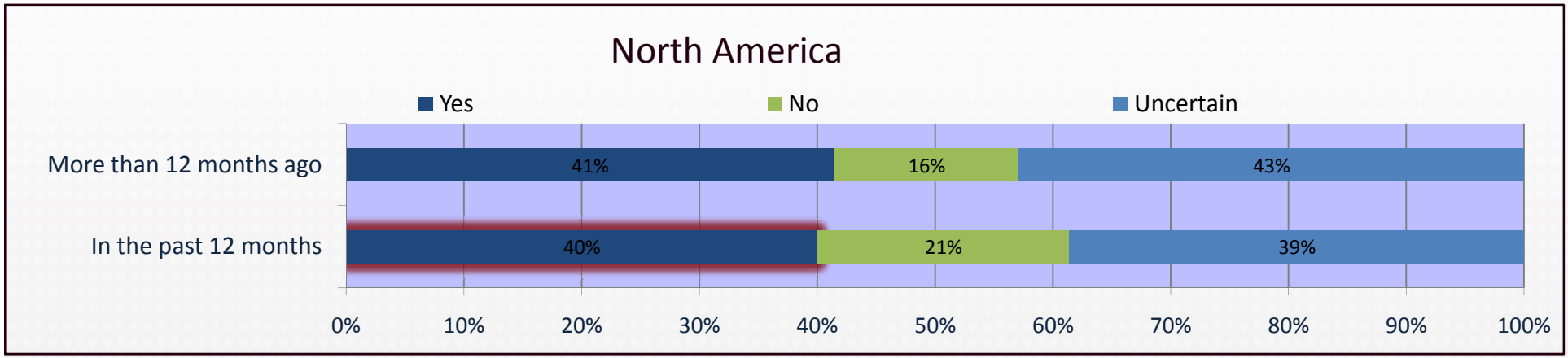
How would you assess the effectiveness of the following to defend against online account takeover and/or ACH and wire fraud?

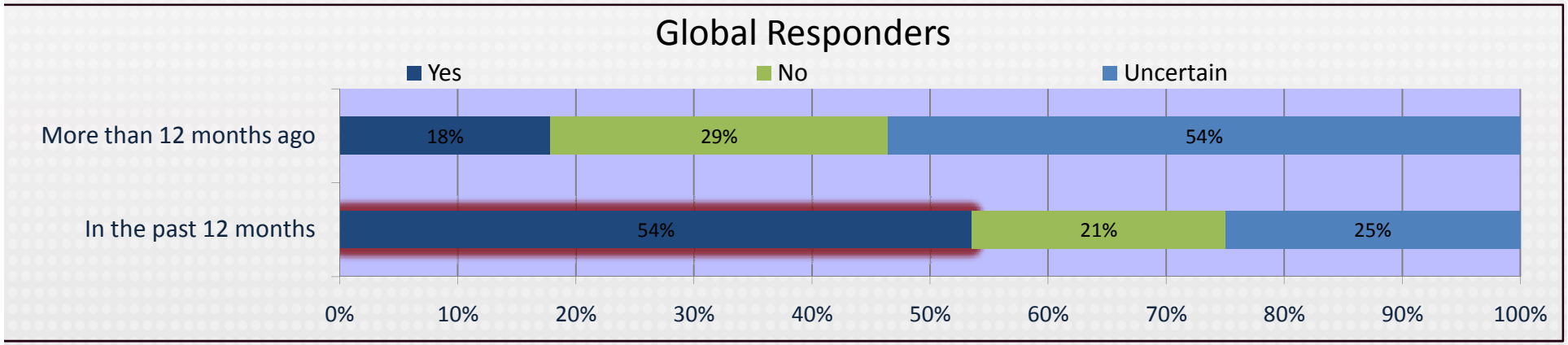
(Rate 1=5, 1=Not effective, 5=Very effective)



Both global and North American responders report confidence in fraud fighting tools: there is most room for improvement in cross-channel fraud monitoring and online session anomaly detection.

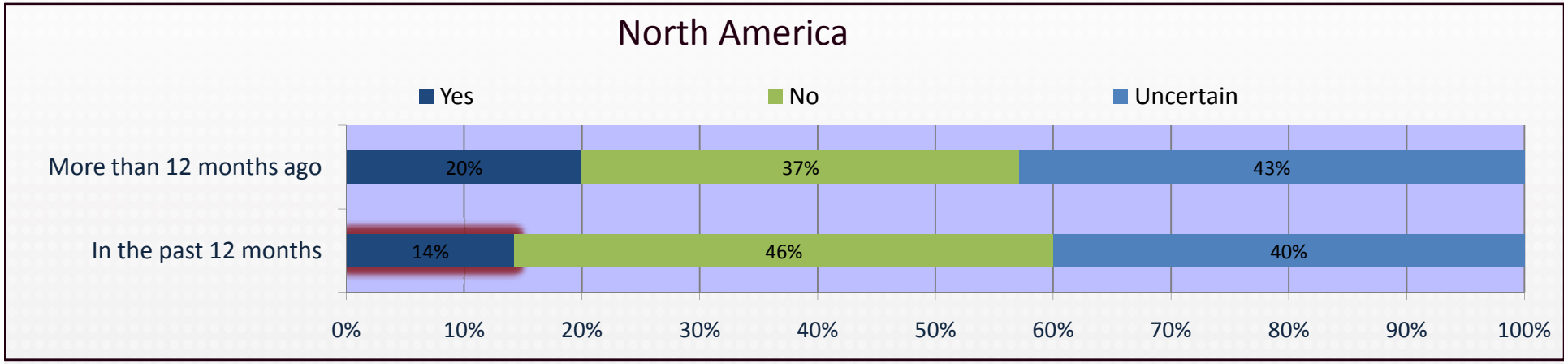
Has your organization experienced attempted commercial account fraud in wire transfer or automated clearinghouse (ACH) operations?

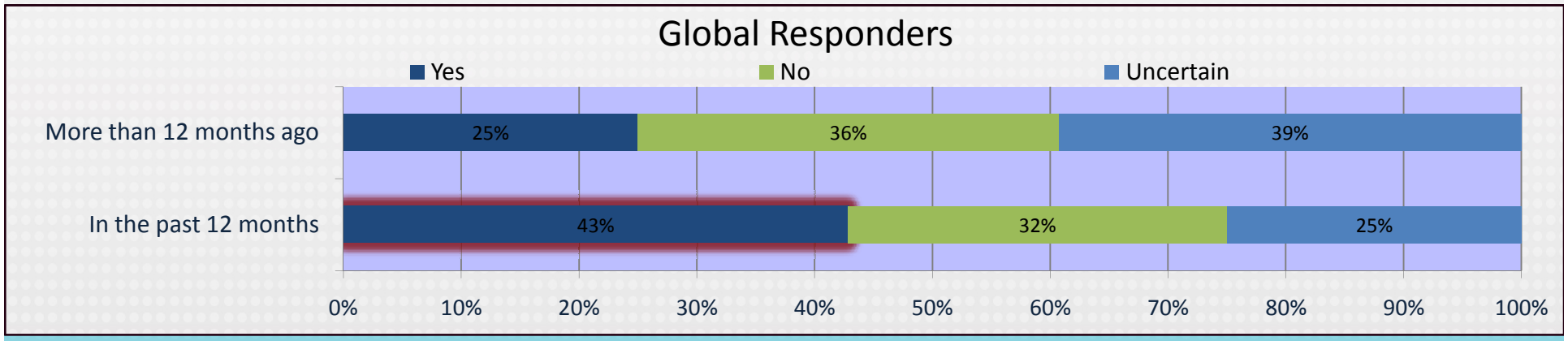




Attempted commercial account fraud is higher in the global market – 54% have experienced it in the last 12 months, versus 40% in North America.

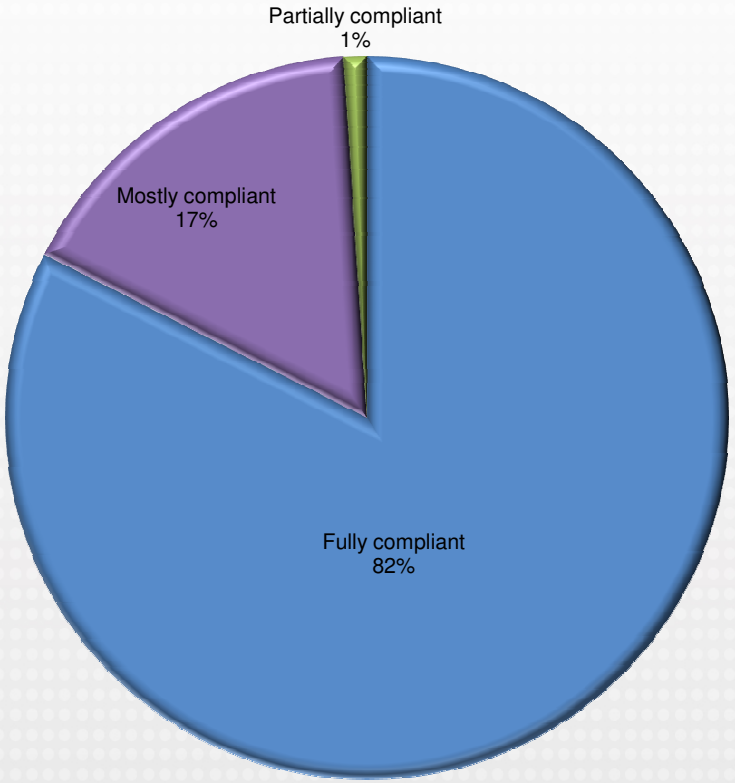
Has your organization experienced actual commercial account fraud losses in wire transfer or automated clearinghouse (ACH) operations?





Experience of commercial account fraud losses is much higher globally than in North America – 43% versus 14% in the last 12 months.

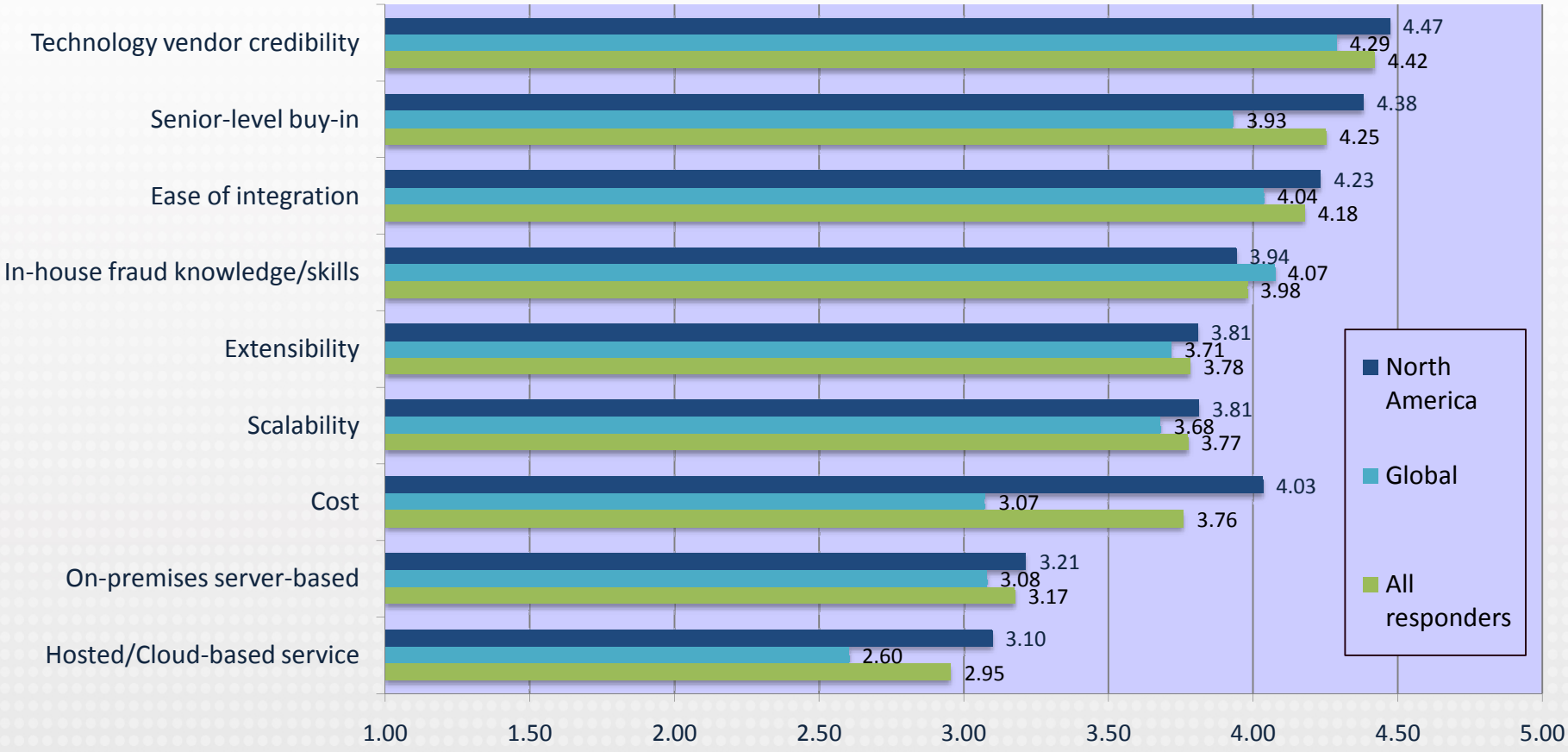
How compliant are you with regulations (e.g. FFIEC) regarding security of commercial accounts from takeover and online fraud?



18% of responders admit to being only mostly or partly compliant with current security regulations.

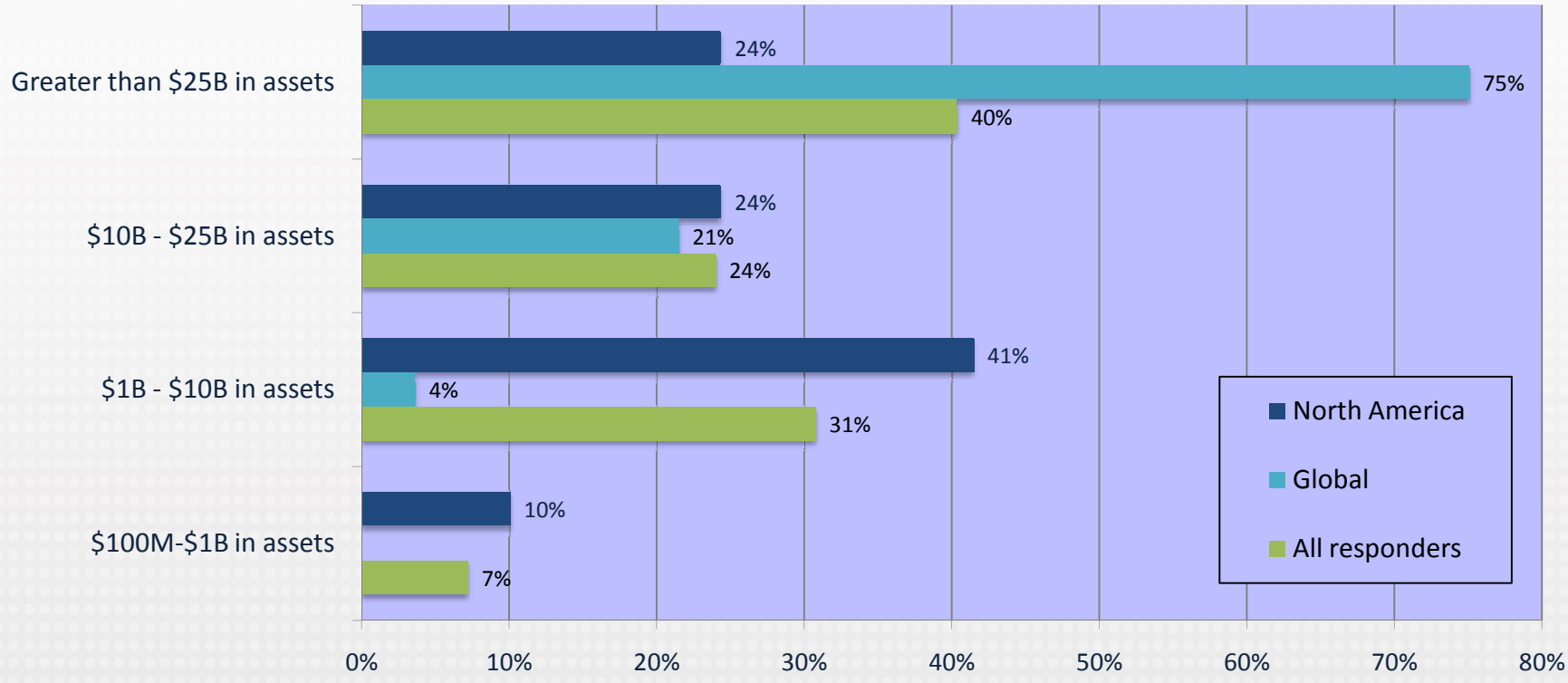
What factors are important when considering a potential technology solution to help mitigate online account takeover and ACH/wire fraud?

(Rate 1-5, 1=Least important, 5=Most important):



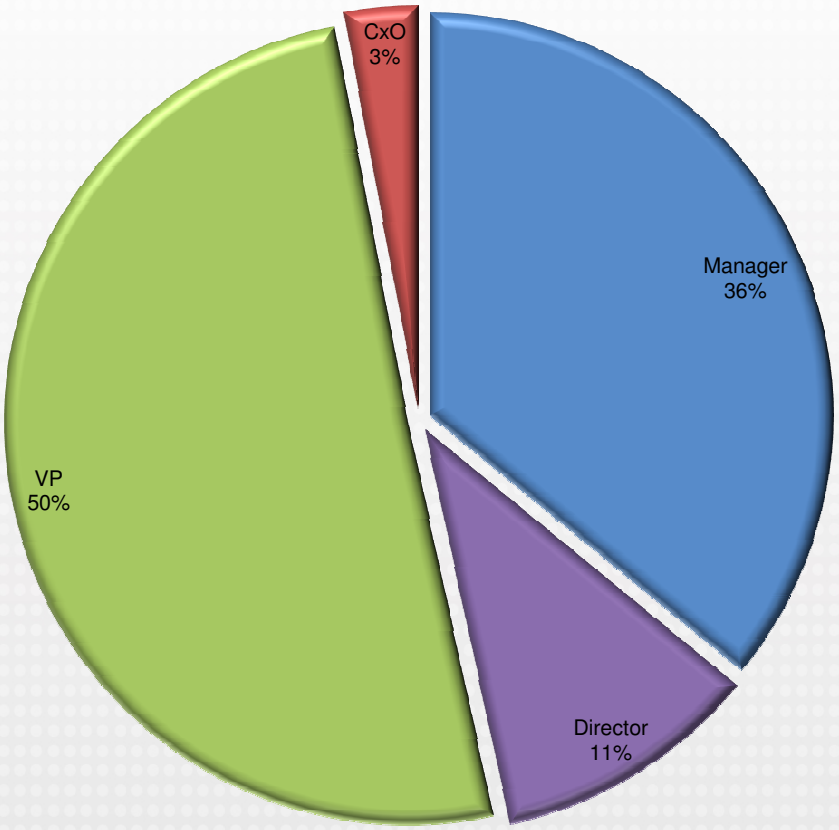
When buying a new fraud mitigations solution, North American responders worry most about cost, integration, and vendor credibility. Globally, vendor credibility also tops the list.

Describe your organizational reach and asset size.



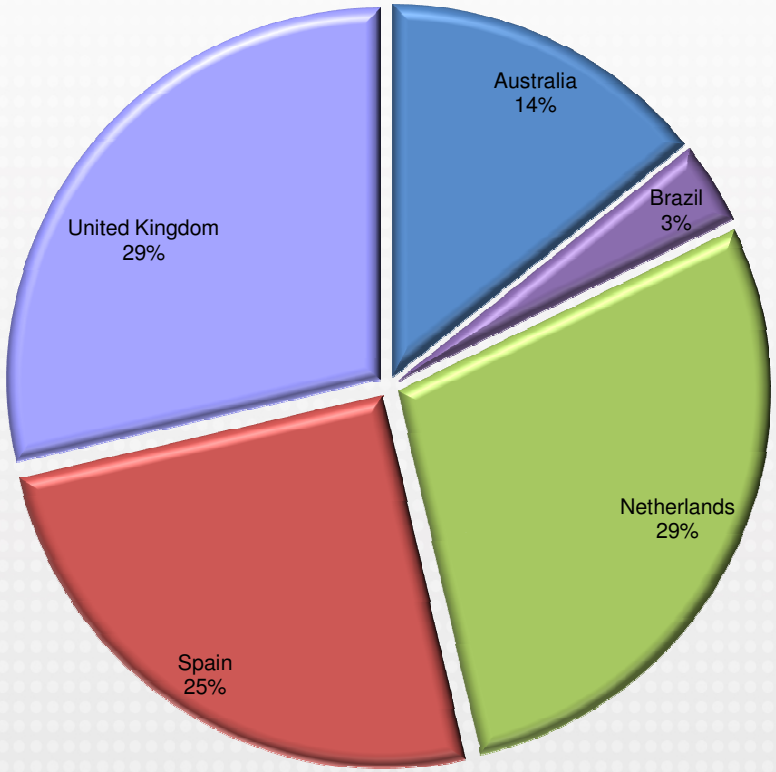
Survey participants from global organizations command large assets: 75% have more than $25b in assets; 90% of North American responders have assets of more than $1b.

Profile of Responders: Job Level



Survey responders are senior financial decision makers.

Profile of Global Responders by Country



Global responders come from the UK, Spain, the Netherlands, Australia, and Brazil.

ACI Worldwide powers electronic payments and banking for more than 5,000 financial institutions, retailers, billers and processors around the world. ACI software enables $13 trillion in payments each day, processing transactions for more than 250 of the leading global retailers, and 21 of the world's 25 largest banks. Through our comprehensive suite of software products and hosted services, we deliver a broad range of solutions for payments processing; card and merchant management; online banking; mobile, branch and voice banking; fraud detection; trade finance; and electronic bill presentment and payment.

To learn more about ACI, please visit www.aciworldwide.com.

You can also find us on Twitter @ACI_Worldwide