UNIVERSAL PAYMENTS℠

MANAGING FRAUD IN AN OMNI-CHANNEL WORLD

THE CHALLENGES AND OPPORTUNITIES FOR OMNI-CHANNEL FRAUD MANAGEMENT IN A RETAIL ENVIRONMENT

Based on a commissioned study conducted for ACI by Forrester Consulting, March 2015

MANAGING FRAUD IN AN OMNI-CHANNEL WORLD

THE CHALLENGES AND OPPORTUNITIES FOR OMNI-CHANNEL FRAUD MANAGEMENT IN A RETAIL ENVIRONMENT

EXECUTIVE SUMMARY

More and more consumers are engaging with retailers through multiple channels, using an ever-expanding choice of payment methods and devices. These varied and fast changing purchasing behaviors — and the growing demand for omni-channel shopping, browsing and fulfilment options — are creating a number of challenges for retailers, including heightened exposure to risk and increased complexity for fraud management.

In March 2015, ACI Worldwide commissioned Forrester Consulting to conduct a research study on omni-channel fraud management capabilities in the retail industry. The study was designed to identify and evaluate current pain points for omni-channel fraud management, and to highlight the tools and strategies needed to combat retail fraud effectively in an omni-channel world.

Key findings include:

- Over 90% of respondents offer multiple service and purchasing channels to their customers
- 65% believe that they do not have adequate fraud management tools to support effective fraud management today
- Only 46% have consolidated fraud management solutions across channels to date, although most others plan to do so in the near future
- Real-time rules and neural models are used for the protection of card-not-present (CNP) channels by under half of respondents. This is a particular concern given the rapid growth of CNP transactions and the upcoming introduction of EMV in the United States, which is widely expected to drive more fraudsters online
- Omni-channel data aggregation, the increasing number of payment options and the demand for faster fulfilment all present significant challenges to retailers' fraud management programs
- Real-time interdiction/decisioning and easy-to-use interfaces are among the tools and functionality required to manage fraud more effectively.

OMNI-CHANNEL PAYMENTS ARE HERE — AND GROWING FAST

Omni-channel commerce — or the ability to provide a consistent buying and payments experience across multiple sales channels — is a phenomenon which has gained significant ground in recent years. It's a development that is here to stay.

Forrester Research has predicted that cross-channel retail sales will reach $1.8 trillion in the U.S. by 2017, from $1.2 trillion in 2012[1]. A survey by IDC Retail Insights[2] also suggests that customers who use multiple channels spend between 15% and 30% more than those who use a single channel.

The reality is that omni-channel consumers benefit from more choice and convenience — able to pay where and when they want, often choosing to use different channels to make purchases or check the status of an order, or even starting a transaction in one channel and completing it in another.

Increasingly, consumers are expecting retailers and other merchants to deliver this enhanced flexibility and convenience.

The survey reveals that many retailers are already well placed to meet the demand for multiple customer touch-points and purchasing channels. In addition to offering in-store point of sale and eCommerce websites, a clear majority of respondents are also embracing mobile (mobile apps and mobile PoS) and other innovations such as unmanned in-store kiosks, while still maintaining traditional service channels such as call centers.

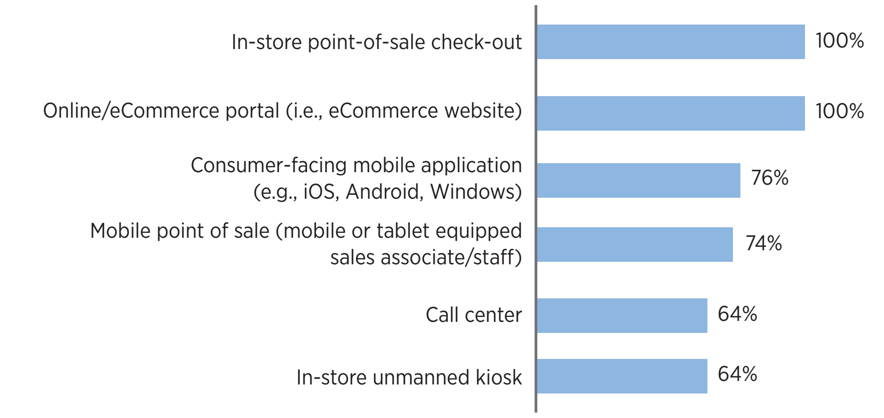
In terms of creating seamless operations across these channels, 57% of respondents already have an omni-channel payments strategy, with a further 36% claiming firm plans to have their strategy in place within two years.

For all charts in this report

Base: 170 U.S. and European retail fraud management decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of ACI, March 2015

"Through which channels does your company currently sell?"



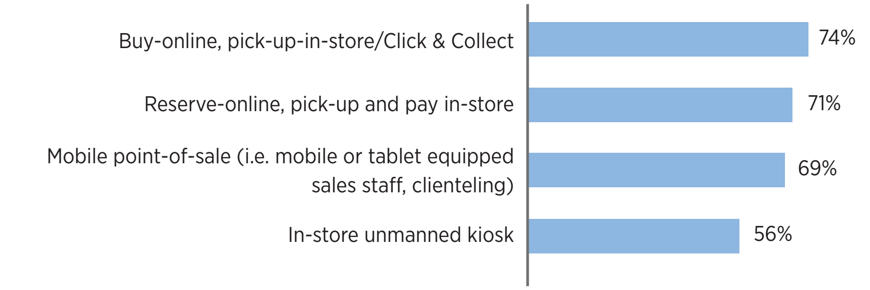
[1] Source: 'U.S. Cross-Channel Retail Forecast, 2012 to 2017', Forrester Research Inc., October 29 2013

[2] Source: 'Satisfying the Omni-Channel Consumers Whenever and Wherever They Shop', IDC Retail Insights, 2009

Furthermore, over 80% of participating retailers claim to have centralized order management and fulfilment, a central data management system governing all systems and to share debit and credit card information between in-store and online channels — all of which underpins the omni-channel customer experience.

The survey also indicates that more than half of retailers are currently supporting some form of omni-channel payment/fulfilment combination, with the most popular option - to buy online and collect in-store - being supported by 74% of participating organizations.

“Which of the following omni-channel payment and fulfilment options does your company currently support?”



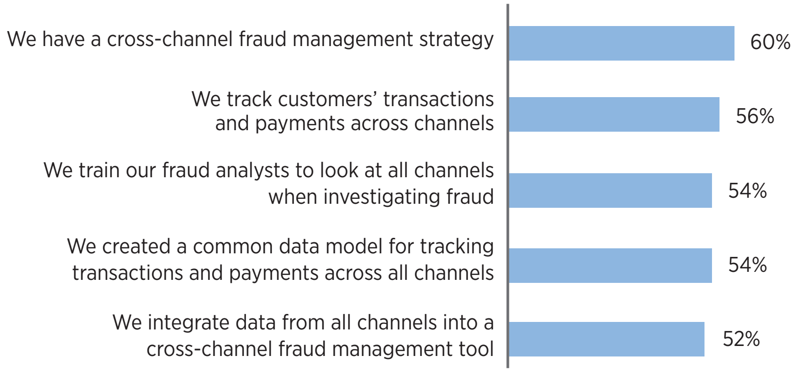
“These (new) fulfilment options do cause additional fraud issues — mostly around promotions and sales available online, that now need to be redeemable in-store. These channels being opened up means we need to open up additional coupons originally designed for eCommerce to the brick and mortar stores as well. Originally, promotions were supposed to be eCommerce transactions that could be tracked — when they are redeemed in-store, we are not able to track the transactions as well.”

Mid-sized retailer

OMNI-CHANNEL FRAUD SOLUTIONS AND STRATEGIES ARE NOT KEEPING PACE

Almost all the retailers in the survey (around 90%) have fraud management programs in place for each of their selling channels, demonstrating a clear recognition of the fraud risk each channel can present. In addition, over half of these retailers are addressing fraud risk through a variety of cross-channel strategies.

“How do you address the risks associated with changes in customer behavior in an omni-channel environment?”



ACI insight

Just like genuine consumers, fraudsters are increasingly operating across channels. In recent months, ACI has seen an increase in cross-channel fraud, with fraudsters taking advantage of the opportunity to get hold of goods faster through buy online/ pick up in-store options. Fraudsters who are successfully challenged in an online environment will also be found attempting to use the same stolen or false credentials through a call center.

With the advent of EMV in the U.S., we should expect to see a significant increase in fraud attempts online. We note, however, that due to the higher maturity of fraud management tools in the U.S. compared to the EU, Forrester believes that CNP fraud will grow at a lower rate in the U.S. than it did in the EU at the time of the liability shift.

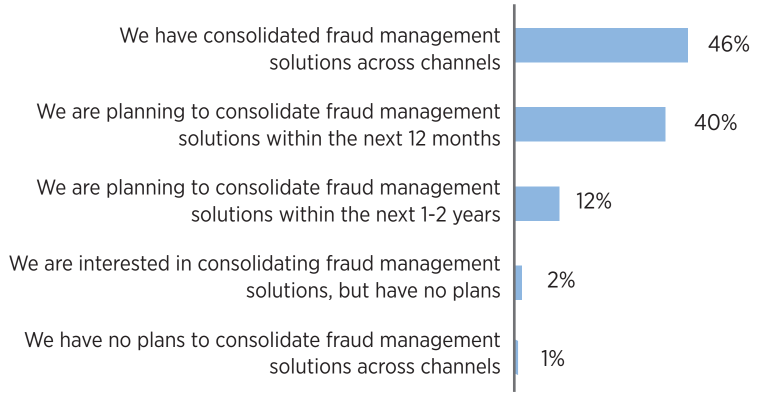
This cross-channel fraud underlines the importance of having a cohesive omni-channel fraud strategy, and negative database, touching all sales channels. In ACI's view, too, it indicates the value of having a single individual with responsibility for managing fraud across CP and CNP channels. Some of ACI's biggest retail customers are now organizing their fraud teams in this way and ACI expects others to follow.

"CNP transactions present more risk to the company, so we need to be sure we are protected. This is one reason why we are not selling internationally yet."

Large retailer

Given the different profiles of fraud in each sales channel — and the different fraud prevention techniques that can be applied — it is perhaps unsurprising that less than half of retailers have consolidated their fraud management solutions across channels. Over 80% of retailers in the survey are still operating siloed fraud management teams, monitoring and managing fraud by channel rather than working as holistic cross-channel teams.

"What are your plans to consolidate fraud management strategies or solutions across channels?"



FRAUD MANAGEMENT SHORTFALL IN CARD-NOT-PRESENT CHANNELS

According to Business Insider[3], card-not-present (CNP) transactions (including eCommerce, mobile payment, online bill pay, over-the-phone transactions and others), will grow at an annual rate of 15%, reaching more than 27 billion transactions in 2018. By comparison, card-present (CP) transactions will grow around 4% during the same time period.

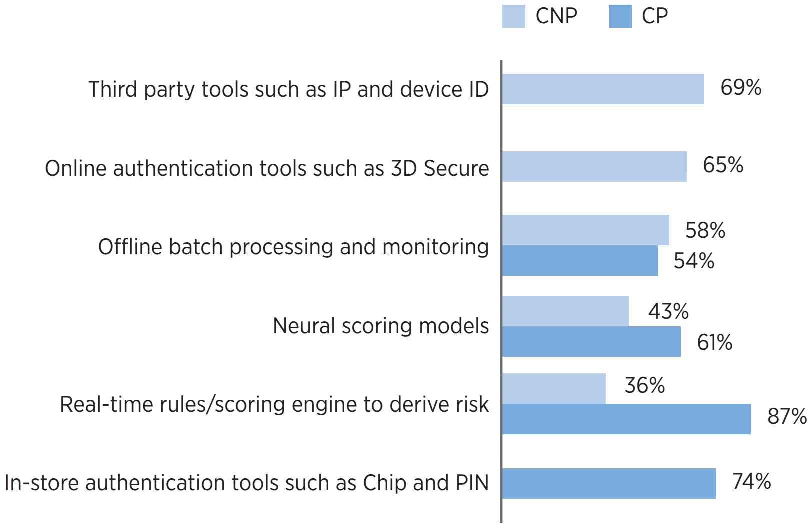
ACI's survey indicates that not only are the volumes of CNP transactions growing, but the revenue split between CP and CNP channels is closing, with CNP transactions now making up an average 42% of the retailers' income.

As one would expect, retailers are using different fraud capabilities for CP and CNP channels, with 74% of respondents indicating that they use in-store authentication methods such as Chip and PIN (or Chip and Signature) to protect their in-store transactions.

In online channels, the most popular fraud detection capabilities being employed are IP and device ID, and 3D Secure. A question remains over 3D Secure implementations in the U.S., which have lagged behind other countries due to customer ease-of-use concerns.

[3] Source: Business Insider, June 2014

“Which of the following fraud management capabilities do you currently have in place for your card-present (CP) and card-not-present (CNP) channels?”



One of the most interesting differences is highlighted when it comes to the use of sophisticated tools which themselves can be used for both CP and CNP channels. For instance, 61% of retailers indicate that they use neural scoring models for in-store point-of-sale transactions, yet fewer than half utilize these same solutions for CNP channels.

Around a third of retailers indicate that they currently use real-time rules to detect fraud in CNP channels (versus 87% for CP channels). This finding seems anomalous with the fact that the majority of retailers are using IP and device ID, as well as 3DS, presumably with rules firing based on the signals received. It is possible that rules may be deployed only in batch processing, and also that some retailers may be using statistical models rather than rules for scoring.

Over half of retailers are using offline batch processing for both CP and CNP transactions.

From ACI’s experience, it is the combination of real-time and post-transaction monitoring that delivers the best protection against fraudsters, enabling fraud rules to be updated as new intelligence is obtained.

CHALLENGES AND SOLUTIONS FOR EFFECTIVE OMNI-CHANNEL FRAUD MANAGEMENT

Central to this study is the exploration of the challenges that retailers face with regard to omni-channel payments and fraud prevention and how these challenges might be addressed with the right tools, resources and processes.

The challenges identified by respondents largely fell into a few key areas: data management, tools, complexity, customer demand and organizational issues.

MANAGING DATA

Many of the top challenges identified by around 70% of participating retailers are centered on the extent to which they are able to manage, monitor and analyze customer payments and fraud data effectively.

“You use the best fraud protection you can, based on the attributes of the channel. In the store, you have a physical view of ID, credit card, etc. Online, you need incremental intelligence. Our vendor solution tracks transactions, uses blacklists/ whitelists, algorithms — they have analysts using all the tools available to prevent fraud on CNP channels.

The primary thing we are having a problem with is high-end items in store. Using our CNP vendor solution in CP channels could potentially mitigate this problem.”

Large retailer

ACI insight

Neural models add speed and sophistication to fraud detection and it is the combination of fraud rules and neural models that provides the best protection. While models may be perceived as complex and costly, ACI’s experience suggests that a neural model tailored to the individual business can deliver a real return to the online retailer, in terms both of frauds detected and revenue and reputation protected.

ACI insight

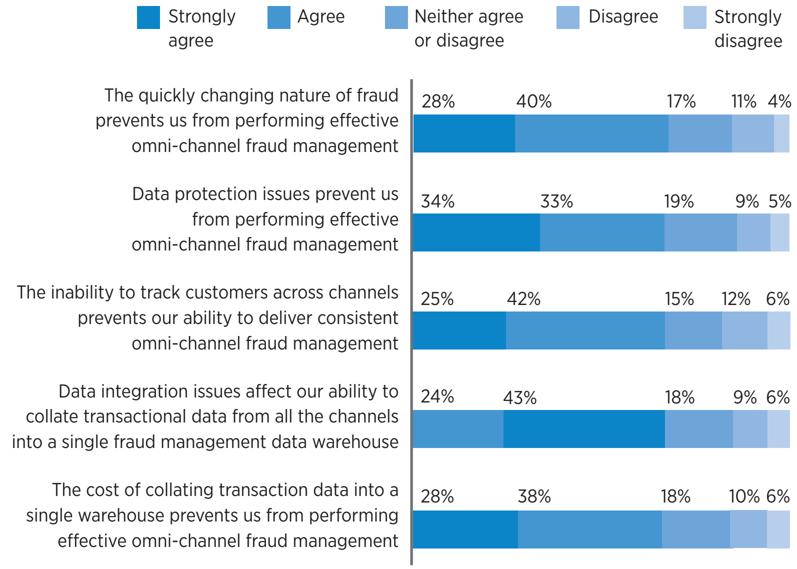
It is easy to understand that the capabilities of in-house repositories built to capture fraud on individual channels will vary — but there is now a fast emerging need for retailers to link these repositories together and use data across channels.

Incorporating a business intelligence capability capable of searching across all channels, covering real-time and batch transactions, will be vital for effective omni-channel fraud management. This will additionally provide valuable intelligence for other parts of the business, and enhance the management and reporting of fraud team performance.

"The most challenging aspect (of fraud management) is defining a new rule set that meets omni-channel requirements. Previously, channels did not interact and each had a well-defined set of rules/best practices. With omni-channel's openness and focus on customer satisfaction, it's an area of learning for us."

Mid-sized retailer

"To what extent do you agree or disagree with the following statements?"



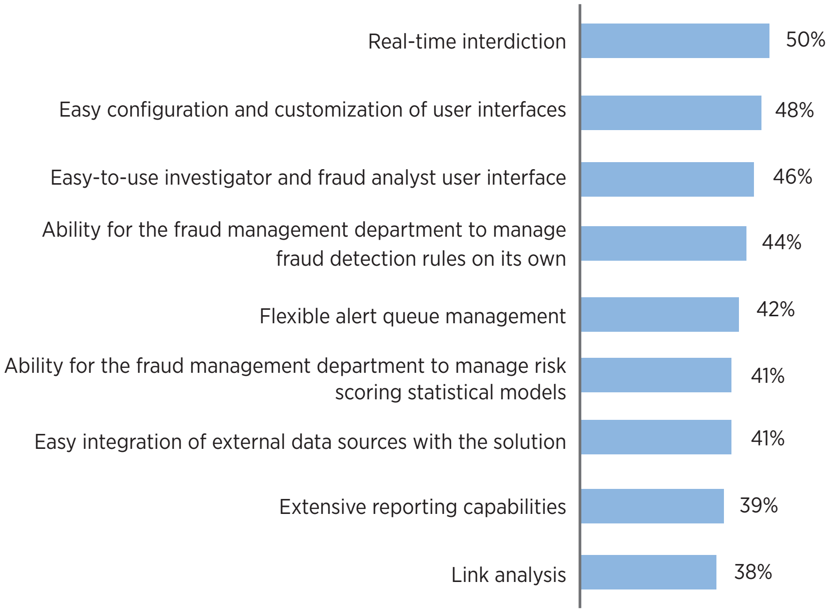
Given the fast-changing nature of fraud, timely access to holistic, high quality data and a comprehensive view of customer behavior across channels are critical to fraud detection and prevention — underpinning well-informed, tailored and adaptive fraud management strategies. The claim that data protection issues are preventing effective omni-channel fraud management is a concern and needs exploring, since the objective — to prevent fraud and financial loss for retailer and customer — is clearly to the benefit of both parties.

INADEQUATE TOOLS

Much of the ability to aggregate, analyze and integrate data across channels comes from having the right payment and fraud management solutions and tools in place. ACI's research identifies a perceived shortfall here, with 65% of retailers saying that they do not have adequate tools to support effective fraud management. More than half say that they need advanced fraud management tools more suited to the new, omni-channel landscape.

When asked which tools and functionality are important for effectively managing fraud, respondents call out real-time interdiction/decisioning and easy-to-use interfaces as the most needed capabilities.

“What technical capabilities do you need to be able to operate an effective omni-channel fraud management strategy?”



It is clear that retailers recognize the importance of flexibility, speed and usability for effective omni-channel fraud management. The fact that real-time capabilities are at the top of the list should come as no surprise and suggests that the absence of real-time rules for CNP transactions identified earlier is a significant concern.

COMPLEXITY AND CUSTOMER DEMAND

The drive towards omni-channel retailing is not simple — and it is further complicated by the continuing introduction of new payment options and by consumer demands for ever-increasing speed in fulfilment and delivery. It is clear that these factors are top of mind for fraud managers as they assess the challenges they face.

ACI insight

ACI was surprised to see the relatively low scoring of link analysis here. ACI’s experience indicates that link analysis can deliver a significant uplift in fraud detection — and that it doesn’t need to be as costly as sometime appears. Within ACI ReD Shield®, we are conducting link analysis to link IDs and common data points across channels, and sharing fraud intelligence between merchants enables us to link new fraud cases to old ones for faster fraud prevention. This capability is within reach of many more merchants than use it today.

“In October 2015, the liability for Chip and PIN will be with the merchant. We need to scramble to get infrastructure in place for Chip and PIN. This will be a very expensive tool refresh, with both POS modifications and in-store training changes. It will be a behavior change for the company.”

Large retailer

“My guess is, less than 50% of retailers will be ready (for Chip and PIN).”

Large retailer

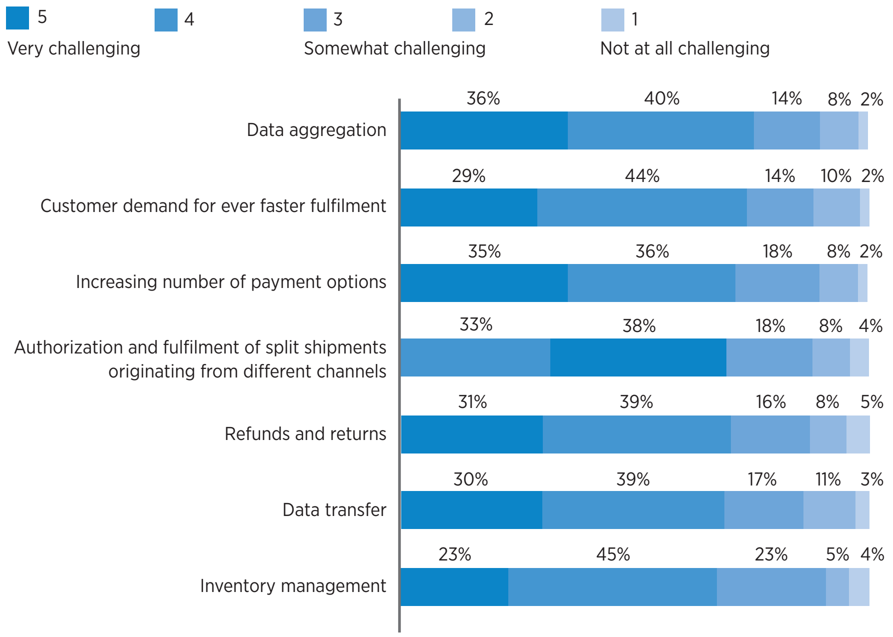
ACI insight

The problems caused by split shipments can be a major headache for retailers. Where payment networks are insufficiently flexible to support such shipments, retailers are shoe-horning transactions into legacy authorization and settlement systems, with resulting confusion that is further exacerbated by returns. Some retailers are seeking help from their acquirers but there is increasing evidence that fraudsters are testing split shipments and exploiting the disconnects to their advantage.

ACI insight

As consumers seek faster access to their purchases, it becomes critical that retailer fraud teams are able quickly to identify and respond to the fulfilment options chosen by these consumers. Moving transactions requiring in-store pick up to the top of the review queue, or into a separate queue, will help retailers to prevent fraudsters from exploiting this growing demand for speed.

"On a scale of 1 to 5, which of the following aspects of omni-channel retailing present the greatest challenges to fraud management?"

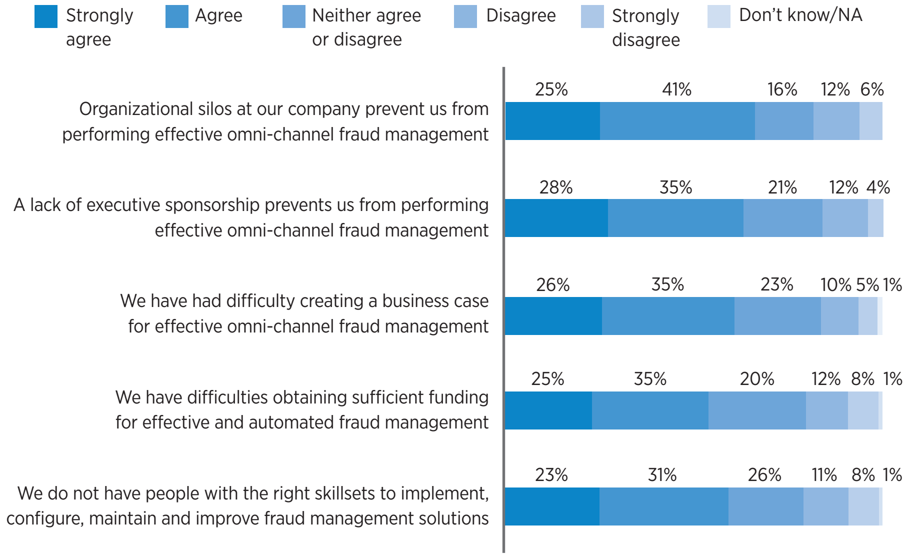


Many of these problems are likely related to the issues already outlined with regards to tracking customers across channels, and the retailers' ability to access and review holistic customer and fraud data. Undoubtedly, the drive for ever faster fulfilment reduces the window of time within which fraud must be identified — in some instances, 'click and collect' transactions require that the product is available for in-store collection within five minutes of the transaction being completed. In these circumstances, real-time or near-real-time screening is essential and retailers need fast access to the richest possible information to ensure that customer service is maintained while holding down chargebacks.

ORGANIZATIONAL ISSUES

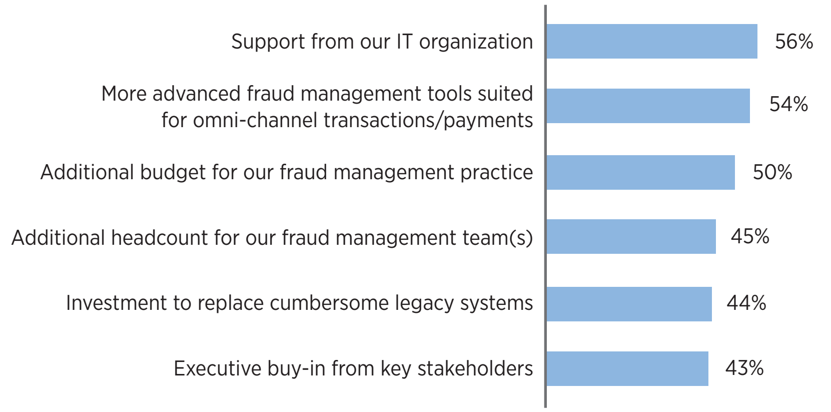
In addition to the challenges raised by the complexities of omni-channel retailing, the fraud managers in the survey clearly struggle with limitations caused by their own organizational structures. Chief among these are the problems involved in managing fraud across silos - this might be relieved to some extent by the appointment of a single person with responsibility for fraud management across CP and CNP channels, as outlined earlier.

"To what extent do you agree or disagree with the following statements?"



The strong support for additional funding and improved skills for fraud management is clearly to be expected and is repeated – with a call for greater executive level endorsement - when respondents are asked what additional support they need.

"What additional resources do you need to be able to operate an effective omni-channel fraud management strategy?"



ACI insight

Many of the issues flagged here by our respondents are common concerns across the industry – and can be addressed through development of a cost/benefit model that presents the business case for fraud management.

These issues are also among the reasons given by our customers for accessing a managed fraud prevention service. In particular, the difficulties of staffing up and down, to meet the peaks and troughs of retail demand, and the continuing need for investment in new tools and systems as fraud evolves, are mitigated by the use of a managed service. Such a service can additionally give you access to a much broader pool of fraud intelligence, to inform and improve fraud decisioning.

WHO OWNS FRAUD MANAGEMENT?

All respondents to this survey have responsibility for fraud management strategy and implementation. Yet, in the United States, 82% of respondents are from the IT department, versus just 21% for France, Germany and Italy.

Where fraud management sits in an organization will influence perspectives on how fraud is managed and on the perceived challenges and solutions. Across all respondents, those from IT are more sensitive to the challenges presented by organizational silos, inadequate fraud management tools, data integration issues, insufficient funding, lack of executive sponsorship and data protection issues.

They are also more sensitive to the need for real-time capabilities than their counterparts in other departments (60% vs. 41%). Where IT decision makers are responsible for fraud management, the retailers are also more likely to have deployed or be piloting technologies such as EMV/chip and PIN acceptance, estate management, P2PE, tokenization and network segmentation.

"First, there needs to be an individual or team with a high level of understanding of how all channels work and the different types of fraud per channel, to manage the whole thing. Siloed fraud management and lack of communications can lead to critical misses."

Mid-sized retailer

"In my mind the financial department owns fraud management, but it is a collaborative effort between many different channels and people."

Large retailer

ACI insight

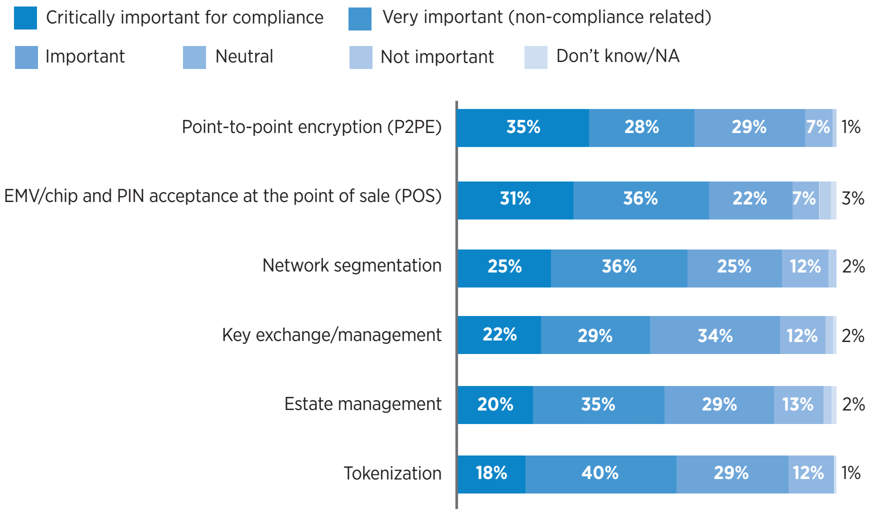
Where fraud management responsibility sits within an organization is far less important than is the extent to which departments are connected, enabling information to be exchanged, challenges understood and goals shared.

Perhaps one of the greatest challenges for fraud management teams is communication of the value they deliver to their organizations. In some sense, fraud teams are the victims of their own success — where fraud is managed effectively, it is only the costs that are apparent, not the losses prevented. Fraud managers need to work together, and with third-party providers, to communicate more effectively the value they deliver, in terms of losses prevented but also revenues enabled and customers satisfied.

INVESTING IN PAYMENTS SECURITY

When asked about the importance of different technologies for payments security, respondents identify point-to-point encryption (P2PE) and EMV/chip and PIN acceptance at the POS as being most important.

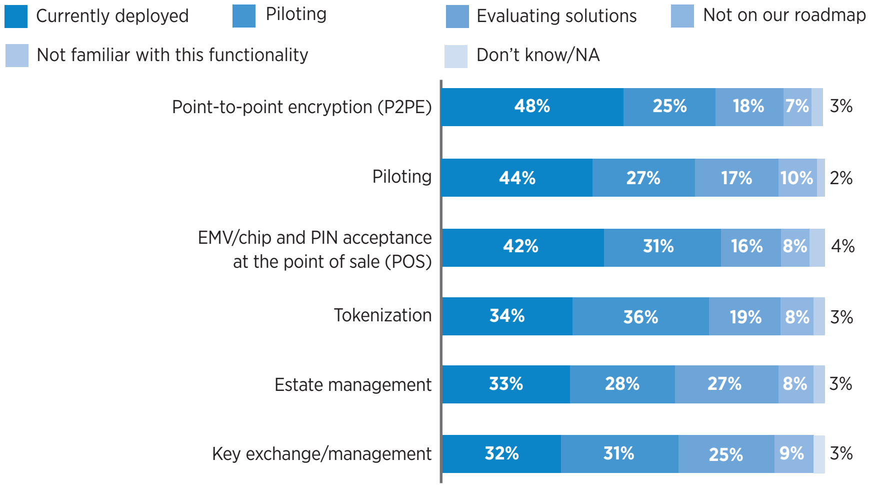
"How important are the following technologies as they relate to your payment security initiatives?"



P2PE — which helps to diminish the ROI for fraudsters — is the most widely adopted technology, in use by 48% of the participating organizations, with a further 25% piloting these capabilities.

Tokenization also features relatively strongly, with 34% of retailers having deployed the technology and a further 36% in the process of piloting tokenization solutions.

"Please identify the status of the following payment security technologies deployed in your organization today"



As part of this survey, respondents were asked about their payment security challenges and initiatives. Large scale data breaches at major retailers have not only had an impact on customer loyalty to the affected organizations, but also on wider consumer confidence in payment security.

ACI insight

Another recent survey conducted for ACI by Ovum[4] found that 54% of retailers were holding back their payments investment due to security concerns. In many instances, retailers appeared to be maintaining the status quo and relying on older, often less secure platforms with which they felt comfortable. However, these concerns over security are precisely the reasons why retailers should be investing in their infrastructure.

ACI insight

P2PE is fundamentally a single-channel, CP solution (hardware encryption by the card reader, and decryption in a secure data center), whereas tokenization is inherently multi-channel. In an omni-channel world, retailers will need to redress this balance and a recognition of this fact may explain the higher percentage of retailers now piloting tokenization.

[4] Source: 2015 Ovum Global Payments Insight Survey

CONCLUSION

This research study indicates that retailers have a clear understanding of the challenges and issues affecting omni-channel fraud management and, to an extent, the resolutions, tools and support available to help address those challenges.

However, there are shifts in organization and strategy that need to be made, to enable an integrated approach to the creation of a true omni-channel environment for payments and fraud management — in a way that enables effective risk management and fully supports the customer experience. There is much work to be done here as retailers embrace an omni-channel world.

The challenges and pain points outlined by participating retailers lead us to make the following recommendations:

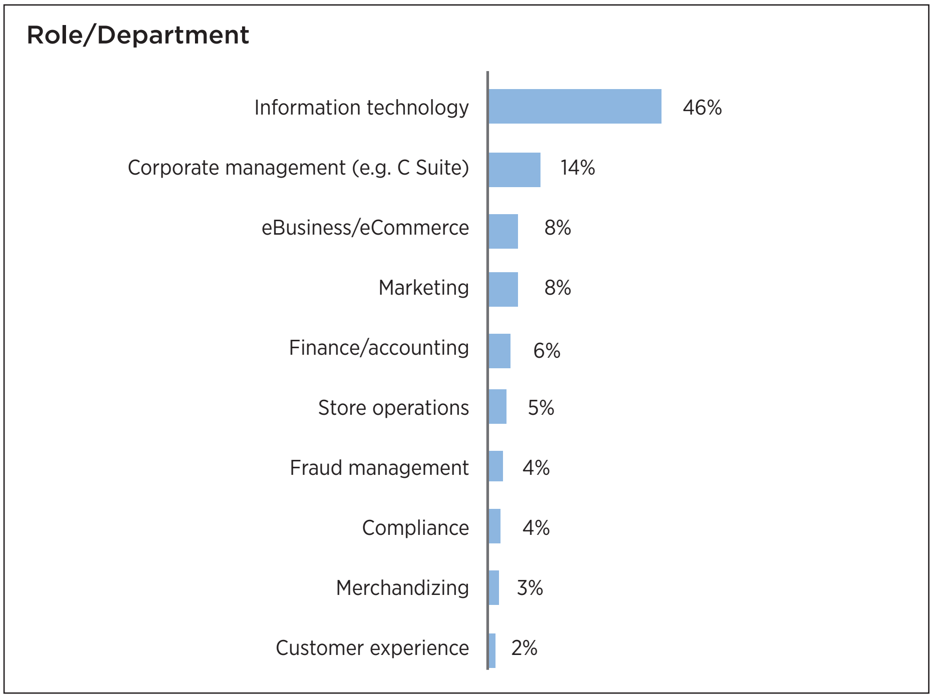
- Eliminate line of business silos and establish a lead fraud management individual or department to ensure that data can be shared, and fraud tracked and prevented, across all sales channels
- Clearly articulate the value of effective fraud prevention across the business, to secure the funding necessary to maintain effective protection as the business grows and expands across borders and channels
- Ensure that tokenization and P2P encryption technologies are adopted to increase payment security and simplify compliance
- Gain access to tools and services that will enable:
  - Fast, effective data integration across channels
  - Real-time and post-transaction fraud screening, across channels
  - Flexible rule strategies and queue definitions
  - Easy-to-configure user interfaces for agents and analysts
  - The ability to turn fraud and payments data into actionable intelligence

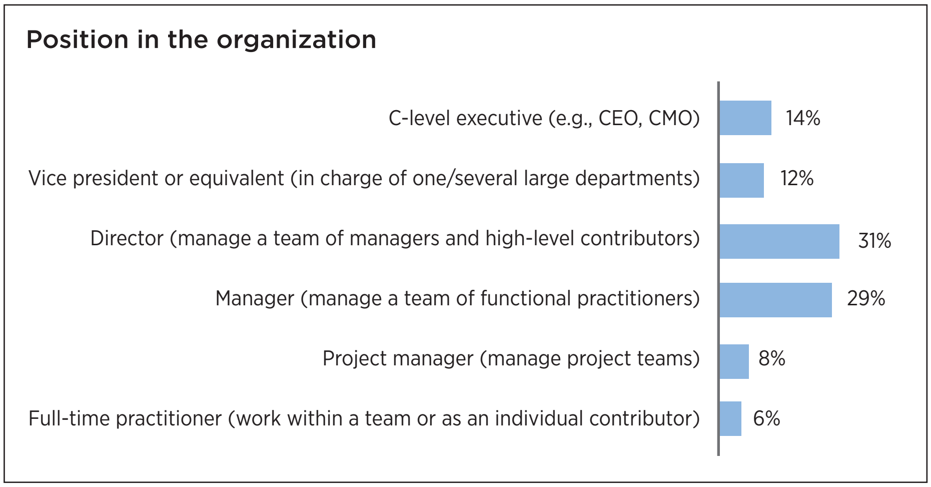
METHODOLOGY

Forrester Consulting conducted this research on behalf of ACI Worldwide in March 2015, surveying 170 participants from across the U.S., U.K., France, Germany and Italy. Participating organizations are retailers selling through both online and offline channels, with a minimum turnover of $2B in the U.S. and $1B in Europe.

Over 80% of the retailers surveyed are conducting business both domestically and internationally.

All individual respondents are decision makers with responsibility for fraud management strategy and execution.





ABOUT ACI WORLDWIDE

ACI Worldwide is the leading provider of secure, omni-channel payment systems to retailers globally. Our Universal Payment — UP — Retailer Payments solution supports a variety of in-store, eCommerce and digital channels providing the framework for retailers to create and manage a customer-centric experience that spans from earning new sales through dynamic rewards programs to ensuring optimum customer service with refunds management. ACI's advanced fraud prevention and payment data security tools reduce merchant risk while protecting the bottom line and protecting brand. ACI powers electronic payments and banking for more than 5,600 financial institutions, retailers and processors globally. Through our comprehensive suite of software products and hosted services, we deliver a broad range of solutions for payment 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.

www.aciworldwide.com

Americas +1 402 390 7600

Asia Pacific +65 6334 4843

Europe, Middle East, Africa +44 (0) 1923 816393

Managing fraud in an omni-channel world — ATL5791 06-15