# TABLE OF CONTENTS

Overview ................................................................................................................................................................... 4  
Executive Summary .................................................................................................................................................... 5  
   Key Findings ...................................................................................................................................................... 5  
   Recommendations ........................................................................................................................................... 6  
The Cambrian Period of Payments .......................................................................................................................... 7  
   E-Commerce and M-Commerce .......................................................................................................................... 7  
      United Kingdom ........................................................................................................................................... 9  
      Australia ..................................................................................................................................................... 10  
      United States .............................................................................................................................................. 10  
   Mobile Wallets .................................................................................................................................................. 11  
   Person-to-Person (P2P) Payments ..................................................................................................................... 12  
   Cryptocurrency ................................................................................................................................................. 12  
The Natural Misalignment of Controls with Payment Adoption ...................................................................................... 14  
   The Phases of Payment Adoption .................................................................................................................... 14  
      The Test Phase ............................................................................................................................................ 14  
      Early Adoption .......................................................................................................................................... 16  
      Mass Adoption ......................................................................................................................................... 17  
      Ubiquity ...................................................................................................................................................... 18  
Exploring the Consequences .......................................................................................................................................... 19  
   The Test Phase/Early Adoption: Mobile Remote Check Deposit (2009–2013) .................................................. 19  
   Early Adoption: Apple Pay Enrollment Fraud (2014) ......................................................................................... 20  
Escaping the Fraud Trap ............................................................................................................................................ 23  
   Partnership ....................................................................................................................................................... 23  
   Control Framework .......................................................................................................................................... 23  
   Monitoring ...................................................................................................................................................... 23  
   Customer Education and Communication ....................................................................................................... 24  
   Technology ..................................................................................................................................................... 24  
Conclusion .............................................................................................................................................................. 25
TABLE OF FIGURES

Figure 1: Forecast of U.S. Internet Sales and Percentage of Total Retail Sales (2011–2021) ..... 8
Figure 2: FPS As a Percentage of Total Non-Cash and Non-Card Payments (2008–2016) ..... 9
Figure 3: Forecast of Mobile Wallet Payments in Dollars and Percentage of POS Payments (2014–2021) .............................................................................................................................................................. 11
Figure 4: Market Capitalization of Cryptocurrencies (as of Jan. 31, 2018)................................................. 12
Figure 5: Availability of Mobile RDC Among Top U.S. Financial Institutions (2009–2015) ...... 19
Figure 6: U.S. P2P Dollar Volume, Overall, Online and Mobile Segments, 2015–2017 .................. 21
Figure 7: POS and CNP Fraud (2002–2013) ............................................................................................................. 22
FOREWORD

This original report, sponsored by ACI, examines how the recent evolution of payments has influenced the choices that institutions make when managing for fraud, the implications of those choices, and opportunities to more effectively get ahead of fraudsters in this new era of digital payments.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

The payment industry is witnessing evolution at a rate that was once inconceivable. And despite the efforts of financial institutions and issuers to prepare for the attempts of fraudsters that inevitably follow the introduction of new forms of payment, there continue to be major, but avoidable, fraud events. At the center of it all is a phenomenon: a general misalignment that often forms on day one between the readiness of FIs and the true fraud risks that accompany payment innovations. In this new world of payment technology, understanding how the alignment between the adoption of payments and fraud controls breaks down from the start is critical. Without it, FIs will continue to fall into the same trap, experiencing avoidable losses and the kind of regulatory scrutiny and reputational damage that undermines consumer confidence and adoption of these new ways to pay and get paid.
EXECUTIVE SUMMARY

Key Findings

New payment technologies are being introduced faster than ever. With the rise of digital technology, the payment industry has exploded with change. Much as life on Earth changed during the Cambrian Period, which ended 485 million years ago, the industry has seen the rapid introduction of a broad range of new payment solutions over the past decade, including cryptocurrency, mobile wallets, and digital person-to-person (P2P) payments.

The future of payment technology is no longer determined by traditional financial services. Today, FIs and issuers can't depend on their ability to dictate how payments work. Instead, they are forced to respond as digital technology has empowered non-bank competitors to introduce new forms of payment that improve upon or even circumvent bank-delivered payment methods, wresting control of the evolution of payments from the hands of the banking industry.

A lack of uniform development has segmented the rollout of new forms of payment. Financial institutions and non-bank providers that are the first to make payment innovations available are relied upon to tread a path, testing various elements until the market indicates that it is ready to accept the payment more widely. At that point, others will follow, adopting standards to ensure acceptance and predictable experiences when that new digital method of payment is used.

Financial institutions consider five major factors that are affected by adoption when deciding on fraud controls. Similarly, how fraud controls are applied at each stage in a payment’s overall adoption follows a predictable pattern, a sort of natural selection influenced by five major factors, including what their peers have done, the amount of time available to map risks to controls, the availability of controls to address risks, how controls could affect adoption, and the availability of predictive data.

This fraud-control pattern has become a self-reinforcing trap. Following a very typical approach to fighting fraud, FIs institute controls that generally align with volume, both within the institution and across the industry. In essence, what worked with other forms of payment at a similar point in adoption goes on to be used with a new form of payment. Over time, this dynamic creates predictable gaps that are only widened because fraudsters’ tactics are evolving more quickly than ever. Subsequently, otherwise avoidable fraud events can begin to occur as institutions fail to align their controls with risks as they really exist.

Payment adoption can be divided into four phases. Consumers’ adoption of new payment technology can be seen as four phases: the test phase, early adoption, mass adoption, and ubiquity. At each stage, FIs often approach fraud in a similar manner: experiencing the same consequences, for better or worse, and setting them up for potentially even greater fraud losses later on.

History has provided clear examples of when the dynamic breaks down. The vulnerabilities of aligning a common control scheme with adoption inevitably become clear. And in cases when fraud gets out of hand, despite applying the typical sets of controls, FIs find themselves in one of two positions: either resigned to accepting the fraud as a cost of doing business or unexplainably outgunned and in search of solutions. As new payment technologies have come to market and adoption has grown, FIs have experienced this phenomenon time and
time again, such as with Apple Pay’s enrollment issues, e-commerce fraud in the UK, mobile remote-deposit-capture (RDC) misuse by unscrupulous customers, and most recently, Zelle P2P payment scams.

**Motivations are changing, leading some institutions to break the cycle.** Today, a handful of institutions are beginning to approach payment fraud differently than the stage of adoption would normally dictate. Their priorities are evolving as managing for fraud becomes less about loss avoidance and keeping pace with their peers and more about tempering regulatory and reputational risk from avoidable fraud events. In turn, these institutions are developing better partnerships, improving their planning and ability to grow, enhancing the education of and communications with customers, and bringing the latest and most appropriate technology to bear earlier.

**Recommendations**

**Build partnerships before development.** Before a new form of payment technology is ever made available or supported, it is critical to get all of the right stakeholders to collaborate. This partnership and the communication it fosters will ensure the best balance between experience and fraud prevention. It can also give the fraud team insights about any outstanding risks that remain long before fraudsters find them and take advantage.

**Prepare to apply controls based on transaction thresholds and design a framework that will scale in response to regular, frequent reporting.** Instead of planning only for an anticipated number of users, start with a control framework that can adjust based on the value of the transaction and the overall rate of fraud. Diligent reporting is necessary to avoid fraud trends being discovered and responded to far too late.

**Anticipate the need for technology that can be adapted to meet head-on the risks from new payment technology.** With new forms of payment being introduced and occurring faster than ever, institutions should assess the suitability of their fraud technology for the long term. This means that if real-time payments are on the horizon, fraud detection based on machine learning should be as well.

**Institute a smart “kill switch” from the start.** To prevent fraud from getting out of hand before controls can be adjusted, an institution should be able to stop certain types of transaction activity at a moment’s notice with an intelligent kill switch: for example, one that could be used to shut down only mobile channel transactions, or just those with U.S. bank identification numbers (BINs). Although it would inconvenience some users, this switch could prevent losses from spiraling, especially when anticipated volumes greatly exceed expectations.

**Use a platform to coordinate fraud-mitigation efforts.** A centralized fraud platform should be in place to score transactions, monitor for fraud, develop cases, and coordinate alerts. This helps to ensure efficiency, allowing fraud to be detected and remediated faster than it would be otherwise.

**Don’t assume that customers know what not to do with the payment.** Consumers should also be educated about how a payment should and should not be used, their rights when it comes to fraud, and the types of fraud they might encounter, inoculating them from all angles.
THE CAMBRIAN PERIOD OF PAYMENTS

For decades, innovation in the payment industry was slow. Consider that plastic payment cards are more than half a century old and that $261.95 billion in paper checks was used to make U.S. retail purchases in 2016.¹ Until recently, change in the payment industry was often limited to the evolution of existing products and back-office processes, such as the introduction of debit cards, the automation of fraud detection, and the integration of chips that would form the basis of EMV. But since the rise of digital technology, the payment space has exploded with change.

Before about 543 million years ago, life on Earth existed only around the sea floor and encompassed much simpler organisms. This state can be likened to a society with limited possibilities for financial actions and relationships as cash, checks, and credit cards reigned. During the Cambrian period, however, over the span of about 55 million years, life spread and diversified into many multicellular organisms we still recognize today. Similarly, the payment space has seen an unprecedented proliferation of new payment solutions over the past decade.

Illustrating this point are five clear examples of the rapid pace at which payment innovations are being introduced. It is worth noting that although many of these examples were originally designed to meet the needs of consumers, some are expanding into the commercial payment space because of their utility for business-to-business and business-to-consumer payments. And for others, a full understanding of their potential utility — and ultimately the fraud risks they present — remains to be seen.

E-Commerce and M-Commerce

Creating a virtual avenue for making purchases that eschews not only the physical storefront, but also the phone and mail, e-commerce is devouring brick-and-mortar stores and upending traditional business models. It has given birth to retail behemoths such as Amazon and to industries that exist only because of the channel, represented by businesses such as Google and Uber. The allure of making purchases from anywhere with an Internet connection is undeniable, expanding beyond just desktops and laptops to the hands of nearly every consumer, thanks to the ubiquity of smartphones. In the U.S. alone, these payments are now estimated to be $611 billion, or 12% of all retail payments, and they are expected to grow 6.45% annually through 2021 (Figure 1).

“Don’t shortchange your technology investment. We have seen a couple of peers that did not invest in the types of technology that most of us did, and their losses were enormous. This type of protective technology isn’t easy to put in or implement, so you have to ratchet back the use of the product and consumers will notice, as will the networks. You have to go in with a full-on cost for the necessary technology to protect transactions.”

Operations executive, Large U.S. financial institution
Total Retail Internet Sales Will Have Nearly Tripled in Only 10 Years

Figure 1: Forecast of U.S. Internet Sales and Percentage of Total Retail Sales (2011–2021)

Source: Javelin Strategy & Research, 2018
Faster and Real-Time Payments

Countries around the world have seen the launch of faster payment initiatives to tackle the need of consumers and businesses to send and receive money more quickly than previous methods could facilitate. This capability is finding a home in cases as diverse as payments for municipal transportation that help speed citizens through turnstiles and corporate payments to vendors that help streamline accounting.

Examples of faster payment initiatives around the world include:

**United Kingdom**

The Faster Payment Service (FPS), launched in May 2008, has since expanded to include single immediate payments, forward-dated payments (one-time bill payments), standing orders (recurring bills), and direct corporate access payments. The FPS now accounts for almost 18% of non-card and non-cash transactions. In terms of the value of 2016 transactions, FPS garnered a 1.45% share of the non-card and non-cash payments. Much of its success has been with small-value instant payment transactions (Figure 2).²

“The banks want to have some volume in the system so they are batching up payments and pushing them over real-time rails because they can: They don’t get a fee and they want to work the plumbing. So that UK number is full of transactions that were not requested to be in real time. So you have RTP, but how many commercial entities are going to spend time to determine which trading partners can actually accept a real-time payment? It will take off, but for now the processes will be more manual; they need the volume to learn fraud trends.”

Former product executive, Payment technology provider

---

**The UK’s Faster Payments Service Has Enjoyed Strong Growth**

Figure 2: FPS As a Percentage of Total Non-Cash and Non-Card Payments (2008–2016)

Source: Javelin Strategy & Research, 2018
Australia

The New Payments Platform (NPP) was launched by banks and credit unions in 2018 to facilitate near-real-time consumer, business, and government payments, and is designed to clear transactions within 30 seconds. The consumer person-to-person application known as Osko uses basic contact information such as an e-mail address or mobile phone number, also known as the PayID, as a means of identifying senders and recipients. This service is among the first to support NPP and is available at certain financial institutions.

United States

Same-day ACH, deployed gradually over the past three years, is uniquely positioned as a means of helping accelerate bill payments in the U.S. Today, all banks must accept same-day ACH payments and must make funds from those payments available by 5 p.m. on the day they are credited, although originating those payments is voluntary. The potential volume for same-day ACH is massive: About 99% of ACH volume is eligible for same-day ACH, meaning that more than $42.5 trillion of the ACH network volume in 2016 would have been eligible to be run as same-day ACH payments.
Mobile Wallets

Ever since the introduction of Apple Pay in 2014, mobile wallets have captured the imagination of pundits who foresaw a future without plastic payment cards. Instead of having to pull a card from a leather wallet, consumers were expected to store payment credentials and to pay merchants with this method, not only within stores at the point-of-sale (POS) but also online.

Early banks rushed to sign up with Apple for fear of missing the boat, and other technology-, merchant-, and issuer-branded wallets have since been introduced, but this future has not come to pass as quickly as some might have hoped or feared. Instead, adoption has been gradual, with only $29 billion in volume in 2017. However, adoption is expected to accelerate, reaching $63 billion this year, as acceptance grows across channels and initiatives like the rebranding of Android Pay to Google Pay begin to pay dividends (Figure 3).⁶

“We have recently deployed Android Pay, and as part of that, our team has made it available to a small population and we are monitoring fraud volume. That creates an opportunity to assess fraud risk, but that is misleading as it isn’t heavily promoted and the population is very small. It helps with customer experience and identifying (some) potential risk, especially as it may not have fraud controls. There isn’t a planned approach (to fraud).”

Fraud executive,
Large financial institution (APAC)

Mobile Wallet Payments Are Set to Take Off After a Slow Start

Figure 3: Forecast of Mobile Wallet Payments in Dollars and Percentage of POS Payments (2014–2021)

Source: Javelin Strategy & Research, 2018
Person-to-Person (P2P) Payments

The ability to pay other people digitally, for amounts big and small without using cash or a check, was in many ways revolutionary. Despite the verb-like nature that Venmo has managed to coin among users, it was not a massive head start that allowed this upstart to effectively corner the P2P payment market in only a few years. Rather, it was the effective targeting of an important demographic segment: young consumers. In fact, bank-provided P2P payments were not introduced all that much later: Only two years elapsed between Venmo (2009) and ClearXchange (2011), the predecessor to Zelle.7

Not wanting to cede the market to PayPal, the corporate parent of Venmo, large U.S. banks rebranded ClearXchange into Zelle in 2017. That year, Zelle moved a total of $75 billion — more than twice that of Venmo — and many more banks beyond the original consortium of owner banks are expected to join the platform in the coming months and years.8

Cryptocurrency

Heralded as a truly transformative payment technology and inspiring a legion of followers, cryptocurrency has advanced from the fringe to become a topic covered almost daily by major business publications in only a few years. Based on cryptography and an underlying ledger system known as the blockchain, cryptocurrencies were first introduced as a white paper in 2008.9 The currency found early favor among criminals as a way to pay for illicit goods on sites on the so-called dark web such as the Silk Road. Since then, the value of the progenitor, bitcoin, and a legion of others are now worth billions (Figure 4).
lackluster in 2017. Not all is lost, though, as the potential for merchant acceptance by Square, which has also enabled consumers to buy and store cryptocurrencies through its Square Cash platform, might help reinvigorate the adoption of bitcoin, litecoin, and others as a form of retail payment.

Some of these new channels and solutions have dramatically changed the payment landscape while others are still in the early adoption phase. Nonetheless, financial institutions, merchants, and consumers are being exposed to a new phenomenon: one in which the ways to pay and get paid are becoming increasingly faster and more accessible — but not necessarily safer.
THE NATURAL MISALIGNMENT OF CONTROLS WITH PAYMENT ADOPTION

Today, even the largest FIs might be followers rather than leaders in payment innovation. And when they are leading the charge, a lack of industry coordination — specifically for non-card payments — can mean an uneven distribution of availability. Financial institutions and non-bank providers that are the first to make payment innovations available are relied upon to tread a path, testing various elements until the market indicates that it is ready to accept the payment more widely. At that point, others will follow, adopting standards to ensure acceptance and predictable experiences when that new digital method of payment is used.

“Risk is about mitigating fraud in the future, but investments are often about avoiding pains from the past. There is a chicken-and-egg paradigm. Let’s build the controls before we have to feel the pain. Like Y2K, we spent all that money and didn’t have a problem. Did we need to?”

Fraud executive, Large financial institution (APAC)

Similarly, the way fraud controls are applied at each stage in a payment’s overall adoption follows a predictable pattern, a sort of natural selection influenced by five major factors that are closely tied to the stage of payment adoption:

1. How their peers have approached the problem.
2. The amount of time that fraud teams have to map control risks.
3. Access to controls, often a function of anticipated losses and revenue.
4. A desire to encourage adoption among customers.
5. The availability of predictive data for identifying and mitigating fraud.

Financial institutions have ended up falling into a self-reinforcing trap, following a very typical approach to mitigating fraud and instituting controls that generally align with adoption by consumers, both within the institution and across the industry. In essence, what worked with other forms of payment at a similar point in adoption goes on to be used with a new form of payment. From the very start, this dynamic creates predictable gaps that expand as fraudsters adapt more quickly than the controls. Subsequently, otherwise avoidable fraud events can begin to occur as institutions fail to align their controls with risks as they really exist.

The Phases of Payment Adoption

The adoption of new payment technology by consumers can be divided into four phases: the test phase, early adoption, mass adoption, and ubiquity. At each stage, FIs often approach fraud in a similar manner: experiencing the same consequences, for better or worse, and setting them up for potentially greater fraud losses later on.

Payment Adoption Affects Fraud Control Choices
**The Test Phase**

At this earliest stage, market participants are testing a new way to pay. Very few FIs might be directly involved, pilots are made available to select groups of customers, and the overall number of transactions is low. The overall risk of fraud at this stage will be contained to simple misuse by customers seeking to game the system, meaning that any lessons learned will be of limited use later on.

“Whenever you are doing one of these initiatives, they will always run late and you will be under pressure to get it done. Once you are six months over and $1 million over, the ship is sinking when you don’t have the thing in the market. You want it out the door so you can charge fees. You get squeezed, particularly toward the end of the project, and where that shows up is in fraud.”

Former product executive, Payment technology provider

- **Fraud Controls**

Financial institutions at this stage cannot apply significant controls for fear of risking customer satisfaction because of the potential for a negative customer experience that undermines use and word-of-mouth support, resulting in the following approach to managing fraud risk:

1. **Risk mapping:** Considering that fraud teams are often not engaged until the end of the development cycle for new forms of payment, any traditional risk-mapping exercise will be rushed. This increases the chance that controls will be insufficient because not all risks are sufficiently identified.

2. **Customer enrollment:** There might be few or no barriers for existing customers to enroll in new forms of payment at this early stage, although availability might be limited to preselected customers. In cases where identity verification exists, it is remedial: no more than a simple PIN or challenge questions.

3. **User authentication:** Whether online or at the POS, authenticating the payee is a basic exercise, involving static credentials such as a password or PIN, because there is no learning curve for consumers and they represent negligible technology costs.

4. **Communication and education:** Messaging to consumers about fraud and security risks is one of the most sensitive areas for most payment providers because it can be viewed as an adoption inhibitor. Because the goal at this stage is to hone the product and create initial awareness, specific notification capabilities around activity, especially suspicious activity, are likely to be nonexistent.

5. **Transaction analysis and reporting:** Fraud prevention usually takes the form of simple, near-real-time rules focused on transaction limits and velocity, and any reporting on unauthorized transactions and associated losses is on an as-needed basis.
Implications
For pilots and the first rollouts open to the public, initial cases of fraud will come from existing customers or family members who have access to their accounts or devices and are trying to game the system. Unfortunately, this does little to prepare the institution for the true breadth of attacks they will face later, when adoption begins to swell. And financial institutions can rest assured that serious fraudsters are beginning to take notes.

Early Adoption
No longer limited to a small set of customers, this new form of payment is broadly available because multiple FIs — typically the largest, digitally inclined institutions — have signed on. Appealing most to customers that are first-adopters of technology, or where the payment provides an especially attractive benefit, overall use is beginning to rise. At this stage, FIs are most concerned with limiting the potential for high-dollar losses and establishing more accurate baselines for normal transaction activity.

Fraud Controls
During the early adoption stage, institutions do their best to reduce risk with fraud detection and transaction monitoring solutions, using generally understood early lessons within the industry to model risk. More substantial controls might be in place, but the approach for managing fraud risk remains biased toward a positive experience:

1. Risk mapping: Fraud teams might not yet be able to exert much influence on what customer-facing controls are implemented — if any — but will have more time to consider the breadth and depth of risks that exist and can better align the appropriate controls with risks.

2. Customer enrollment: Enrollees might now be challenged to provide one-time passwords sent through secondary channels. Data that has just become available from the network or underlying technology provider adds a layer of intelligence for determining whether or not the enrollee is legitimate.

3. User authentication: Passwords and PINs will still be the primary gatekeepers, but stronger forms of authentication, such as one-time passwords, will now be used to ensure that the enrolled customer is the one conducting a high-risk transaction as institutions mine their toolboxes for reliable, more secure, but still inexpensive authenticators.

4. Communication and education: Security might be a selling point with some customers at this stage, so education about the security benefits of a new form of payment start to be touted. Customers may be able to opt in to alerts when these transactions occur, but suspicious-activity alerts are not yet practical because institutions don’t have the necessary analytics to make that determination effectively without relaying excessive alerts to the customer.

5. Transaction analysis and reporting: Near-real-time rules based on basic regression models are now in use, along with a so-called kill switch to stop all transactions should a large, unexplained, or otherwise uncontrolled series of fraud events occurs. Device- and location-based data may also be used because digital intelligence is
better brought to bear. Reports are now standardized and run regularly, although the optimal metrics for managing fraud risk have yet to be established.

**Implications**

Initial attacks tend to focus on one or two significant vulnerabilities because criminal groups share intelligence and pile in. These can target any stage of the process, from enrollment through transactions, using compromised accounts. There is the potential for significant fraud events, but they are unlikely. Instead, these events are more likely to undermine the reputation of the institution as the media or regulators become apprised.

**Mass Adoption**

At this stage, the market has now become much more aware of the benefits of a new form of payment. An FI’s customers are generally familiar with the payment technology, and it has users from across the spectrum, from technology-first Gen Z consumers to more traditional Baby Boomers. On the verge of ubiquity, FIs are now instituting and refining more mature controls that greatly diminish the potential for significant fraud losses.

**Fraud Controls**

Controls are now time-tested, coordinated through a central platform and based on intelligence from both within the institution and across the industry as known risks and so-called best practices begin to solidify. Financial institutions don’t break the mold with new technologies but instead rely on solutions that have become generally accepted standards in their approach to managing fraud risk:

1. **Risk mapping**: With years in the market, fraud teams can use a significant breadth of knowledge about common schemes and known vulnerabilities, along with expected levels of fraud loss, making the effort of risk mapping an exercise in keeping pace with peers.

2. **Customer enrollment**: Having learned from earlier enrollment abuses, FIs now achieve a higher level of identity assurance as a combination of deep background intelligence, better data capturing, and authentication capabilities are brought to bear, along with tighter limits on new users.

3. **User authentication**: Customers begin to be presented with an option for more modern authentication, such as biometrics — whether to log in or to authorize a transaction — instead of the use of a password or PIN. This might be designed to bolster the perception of security as much as the actual security of an account or transaction.

4. **Communication and education**: FIs now talk about the security benefits of this form of payment and emphasize the controls that are in place more openly and are now in a position to alert customers when suspicious transactions occur without overwhelming them with false positives.

5. **Transaction analysis and reporting**: Enough data exists that real-time rules are now in place, powered by neural network models. A kill switch still exists as a backstop. The most appropriate metrics for controlling for fraud have been identified, they are actively tracked, and in turn, authorization strategies are adjusted immediately.

> “I have all this knowledge and a fraud engine that supposedly works in real time. This should all work, right? Bad guys are very creative. The banks need to be right all the time and the bad guys just need to be right once.”

Former product executive, Payment technology provider
**Implications**

With broadening awareness in the market, legitimate customers are targeted through social engineering and are actively encouraged to make payments to fraudsters under false pretenses. New functions might introduce vulnerabilities that have yet to be accounted for, but while institutions suffer a higher volume of fraud attempts and wayward customers might continue to test the limits, losses are mostly manageable with established controls in place.

**Ubiquity**

A close to second to cash, this method of payment is accepted practically everywhere and by everyone. This now constitutes a major product or channel for the institution, with dedicated fraud resources and performance that is regularly discussed among the most senior executives in the risk function of the institution.

**Fraud Controls**

Moving the needle on fraud at this point could result in significant savings, but a misstep has the potential to affect a large number of customers, so any changes are closely scrutinized, resulting in the following approach to managing fraud risk:

1. **Risk mapping:** Fraud teams dig for new vulnerabilities and threats, but armed with a wealth of potential controls to bring to bear, the prominent challenge is in aligning the most effective control with the risk rather than just securing against it.
2. **Customer enrollment:** A standard component of an FI's overall payment suite, no additional enrollment is required because the consumer is provided access from the moment he or she becomes a customer.
3. **User authentication:** Multifactor authentication protects the entirety of the FI's app, protecting access to this payment as well. Users might still be confronted with a form of step-up authentication, depending on the risk of the transaction.
4. **Communication and education:** The security risks and liability coverages of this form of payment are among the first things disclosed to the customer, prodded by regulators or by lessons reinforced by media coverage of old fraud events. Alerts and notifications might now have an interactive element, in which customers can confirm or deny the legitimacy of a transaction immediately after being alerted of suspicious activity.
5. **Transaction analysis and reporting:** Beyond neural networks, machine-learning models are used to finely tune authorizations. Reporting metrics are standardized so that institutions can effectively gauge their performance over long time horizons and against their peers, and little room is left for the effects of a significant fraud event to manifest without notice.

**Implications**

With not only the payment, but also the associated controls, long since established, the greatest risks come from predictable controls and a lack of communication. More specifically, criminals learn over time how institutions generally control for fraud and will begin to exhibit thoughtfulness in their approach. This can lead to a significant, but small, number of fraud cases affecting high-value targets or a significant number of small fraud cases that fly under the radar. And in the event that stakeholders fail to keep open lines of communication, for which ubiquity of acceptance is no guarantee, effectively remediating fraud might take far longer than it would have otherwise.
EXPLORING THE CONSEQUENCES

The vulnerabilities of aligning a common control scheme with adoption inevitably become clear. And in cases when fraud gets out of hand, despite applying the typical sets of controls, FIs find themselves in one of two positions: either resigned to accepting the fraud as a cost of doing business or unexplainably outgunned and in search of solutions. As new payment technologies have come to market, FIs have experienced this phenomenon time and time again.

The Test Phase/Early Adoption: Mobile Remote Check Deposit (2009–2013)

Once largely the purview of businesses, remote check deposit (RDC) made its way to consumers because of mobile banking. Despite promises as early as 2008 to make mobile remote check deposits broadly available, the availability of the technology to retail banking customers was slow, hampered by a small population of vendors that were unable to meet industry demand (Figure 5). And when they did make mobile RDC available, FIs applied the same rules to it as they had in business banking and as outlined in regulatory guidance from the Federal Financial Institutions Examination Council (FFIEC).13,14

Mobile Remote Deposit Capture Got Off to a Slow Start

Figure 5: Availability of Mobile RDC Among Top U.S. Financial Institutions (2009–2015)

Percentage of Top U.S. Financial Institutions

Source: Javelin Strategy & Research, 2018
Nonetheless, unscrupulous retail banking customers began to look for ways to manipulate the digital nature of mobile RDC early on. And as a result, duplicate deposits quickly became a problem, with customers who conducted mobile deposits subsequently depositing or cashing the same checks elsewhere. Ultimately, thousands of dollars were lost in some cases, and the phenomenon was not easily controlled until data sharing on check deposit activity was more uniformly established among institutions and check-cashing businesses.¹⁵,¹⁶

**Early Adoption: Apple Pay Enrollment Fraud (2014)**

Unlike some other forms of digital payment technology, Apple Pay enjoyed a relatively broad rollout as the use of fingerprint biometrics and tokenized payment credentials instilled confidence in the largest U.S. banks, which went on to make Apple Pay available to their customers on day one.¹⁷ But rather than attacking the data or trying to circumvent Touch ID, fraudsters instead focused on the identity and verification process that was used to confirm that the card being enrolled belonged to the owner of the Apple device.

Bolstered with limited intelligence from Apple, enrolling in Apple Pay proved little challenge to fraudsters armed with card credentials and answers to remedial authentication challenges used by institutions to verify identity, such as requesting the last four digits of Social Security numbers or answers to account security questions. The prominence of the institutions that made Apple Pay available to early adopters meant that these fraud cases became fodder for headlines in major media publications.

---

“We used to be motivated solely by loss avoidance, but that won’t work now. It is still about loss avoidance, but there isn’t a two-year payback period. The cost recovery is more perception than actual math. We have more compliance, reputation, customer awareness, etc”

Former product executive, Payment technology provider

---

**Mass Adoption: Zelle Scams (2017–2018)**

Enjoying the benefits of a significant rebranding and marketing effort, Zelle has also been confronted with some of the negative consequences of fame. Criminals have manipulated early Zelle users, abusing their lack of understanding of how Zelle was designed to be used to solicit payments. Whether for goods bought online that are never delivered, or as part of a social engineering scam, Zelle users could be left holding the bag because the payment does not provide for the same types of fraud protection as cards or even PayPal.¹⁸

“Banks get excited about a new product, but the customer doesn’t understand it and they use it in ways that are not intended. They may not know the limit of their protections and how it is meant to be used. And now it is up to the bank to decide how to handle those cases: happy customer or end up with that on Twitter as a way to teach everyone else.”

Former product executive, Payment technology provider

---

“We used to be motivated solely by loss avoidance, but that won’t work now. It is still about loss avoidance, but there isn’t a two-year payback period. The cost recovery is more perception than actual math. We have more compliance, reputation, customer awareness, etc”

Former product executive, Payment technology provider
The scams place Zelle banks between a rock and a hard place. They are forced to decide between compensating the victims despite being under no legal obligation to do so and inciting the wrath of consumer advocates and media members who would label the practice of denying victims reimbursement as patently unfair. With P2P payment volumes on the rise — and set to grow further as the use cases broaden and availability at banks grows — denying a fraud claim could diminish trust in the nascent payment method (Figure 6).

Mobile P2P Payment Volume Fuels Overall Growth

Figure 6: U.S. P2P Dollar Volume, Overall, Online and Mobile Segments, 2015–2017

Source: Javelin Strategy & Research, 2018

Issuers in the UK market were early adopters of EMV chip card technology. Although this development helped reduce point-of-sale (POS) card fraud dramatically, it did little to discourage card-not-present (CNP) fraud. Over the course of only a few years, CNP fraud grew dramatically as e-commerce in the UK took off. Despite the efforts of issuers and merchants, it wasn’t until the broad availability of risk-based 3D Secure that CNP fraud finally began to wane in 2009 (Figure 7). This dynamic was subsequently misunderstood, as EMV was labeled the primary cause of CNP fraud, instead of the confluence of rising volume and an absence of communication technology that bridged the knowledge gap between issuers and merchants.

In UK, Internet Card Fraud Has Grown Dramatically Since EMV Introduction

Figure 7: POS and CNP Fraud (2002–2013)

Source: Javelin Strategy & Research, 2018
ESCAPING THE FRAUD TRAP

Today, a handful of institutions are beginning to approach payment fraud differently than the stage of adoption would normally dictate. Their priorities are evolving as managing for fraud becomes less about loss avoidance and keeping pace with their peers and more about tempering regulatory and reputational risk from avoidable fraud events. In turn, these institutions are developing better partnerships, improving their planning and ability to grow, enhancing the education of and communications with customers, and bringing the latest and most appropriate technology to bear earlier.

Partnership

Before a new form of payment technology is ever made available or supported, it is critical to get all of the right stakeholders to collaborate. This partnership and the communication it fosters will ensure the best balance between experience and fraud prevention. It can also give the fraud team insights about any outstanding risks that remain long before fraudsters find them. This means not only partnering internally but also with vendors and even across industries.

Control Framework

Instead of planning only for an anticipated number of users, start with a control framework that is designed to adjust for the value of the transaction and the overall rate of fraud. This can work to an institution’s advantage by dramatically enhancing the experience of the customer and helping an institution better align with regulatory mandates like Payment Services Directive 2 (PSD2). Note that if controls are insufficient to manage fraud at an anticipated number of users, or at certain transaction thresholds, then the overall approach should be scrutinized and adjusted appropriately.

Monitoring

That is not to say that every risk can be anticipated; far from it. Diligent reporting is necessary to avoid fraud trends being discovered and responded to far too late. And to prevent fraud from getting out of hand before controls can be thoughtfully adjusted, an institution should be able to stop certain types of transactions at a moment’s notice with an intelligent kill switch: for example, one that could be used to shut down only mobile transactions, or just those using U.S. bank identification numbers (BINs). While inconveniencing some users, it could prevent losses from spiraling, especially when anticipated volumes greatly exceed expectations.

“In the past, we develop something, we roll it out, then we have a problem and bring them in... That has all changed. The product development life cycle is different. The model now is that digital is the hub with everyone in the room: risk, fraud, audit, second line, compliance, etc. That never happened long ago. The fraud team owns the impact so we partner together. That level of conversation has evolved and is critical.”

Risk and security executive, Regional financial institution (U.S.)
Customer Education and Communication

Not to be left out of the equation, consumer education and communication can be critical to both in managing fraud risk and in shaping perception. That means educating consumers about how a payment should and should not be used, their rights when it comes to fraud, and the types of fraud they may encounter, inoculating them from all angles. And even remedial, high-value transaction or threshold-based alerts set by customers can provide a wealth of feedback about potential fraud risks without being held hostage to the efficacy of models.

Technology

Sometimes it is simply a matter of bringing the right existing technology to bear in advance. With new forms of payment being introduced and occurring faster than ever, institutions should assess the effectiveness of their fraud technology relative to the inherent qualities of that payment method. In practical terms, if real-time payments are on the horizon, real-time solutions should be, too. That means stronger authentication, along with fraud detection based on machine learning and behavioral analytics.

“You need a fraud evaluation mechanism in place before you deploy. But you may not be able to monitor fraud as it isn’t distinguishable. So there should be a kill switch if things get out of hand. But as far as having that thinking out front, we will pilot and make an informed decision if something needs to be employed before something is deployed. And if we know what our exposure is, we need a plan to act if that is exceeded.”

Fraud executive,
Large financial institution (APAC)
CONCLUSION

The misalignment of fraud controls with the relative rate of new payments adoption has created control gaps, leaving FIs exposed. The resulting fraud is not unpreventable, but unless institutions are willing to break out of their usual approach to managing the risk of payment fraud then they very well may seem unavoidable.

Understanding the implications of this misalignment can allow institutions to identify whether they have fallen into the fraud-control gap, and where exactly they might be at risk of becoming victim to preventable losses, reputational damage, and regulatory scrutiny. In turn, they can adjust their approach to fraud, instituting a more modern and effective plan to fight fraud as new ways to pay and be paid are introduced to the market, adopted by their customers, and ultimately become commonplace.

<table>
<thead>
<tr>
<th>Typical Drivers for Choosing Controls</th>
<th>Consequences</th>
<th>Steps to be Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How their peers have approached the problem.</td>
<td><strong>Test phase</strong>&lt;br&gt;first party fraud</td>
<td>1. Partner early</td>
</tr>
<tr>
<td>2. The amount of time that fraud teams have to map control risks.</td>
<td><strong>Early adoption</strong>&lt;br&gt;enrollment fraud</td>
<td>2. Use a scalable control framework</td>
</tr>
<tr>
<td>3. Access to controls, often a function of anticipated losses and revenue.</td>
<td><strong>Mass adoption</strong>&lt;br&gt;customer victimization</td>
<td>3. Monitor regularly</td>
</tr>
<tr>
<td>4. A desire to encourage adoption among customers.</td>
<td><strong>Ubiquity</strong>&lt;br&gt;low and slow fraud</td>
<td>4. Setup a kill switch</td>
</tr>
<tr>
<td>5. The availability of predictive data for identifying and mitigating fraud.</td>
<td></td>
<td>5. Provide transparent communication and education</td>
</tr>
</tbody>
</table>

Source: Javelin Strategy & Research, 2018
METHODOLOGY

Consumer data

Consumer data in this report is based on information gathered in several Javelin surveys administered in 2015, 2016 and 2017. Data was gathered and weighted to reflect a representative sample of the adult U.S. population:

- A random-sample survey of 3,000 respondents conducted online in October-November 2017. The overall margin of error is ±1.74 at the 95% confidence level. The margin of error is larger for subsets.
- A random-sample survey of 3,200 respondents conducted online in October 2016. The overall margin of error is ±1.74 at the 95% confidence level. The margin of error is larger for subsets.
- A random-sample survey of 3,200 respondents conducted online in October 2015. The margin of sampling error is ±1.74% at the 95% confidence level. The margin of error is larger for subsets.

Mobile scorecards

Scorecard data in this report is based on Javelin evaluated mobile banking features of the nation’s largest retail FIs total by deposits, excluding banks focused on investment banking. Surveys were administered from 2009 to 2015.

In support of this research Javelin interviewed financial industry executives in payment risk and fraud across different markets, including the U.S. and APAC.
ENDNOTES

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based consulting firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants, and other technology providers.

Authors: Al Pascual, SVP Research and Head of Fraud & Security
Contributors: James Wilson, Analyst, Digital Lending
Kyle Marchini, Senior Analyst, Fraud Management
Editor: Chuck Ervin
Publication Date: May 2018

ABOUT ACI WORLDWIDE

ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI’s private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience. To learn more about ACI, please visit www.aciworldwide.com. You can also find us on Twitter @ACI_Worldwide.