Sponsored by

sas

THE ESCALATION OF DIGITAL FRAUD:
GLOBAL IMPACT OF THE CORONAVIRUS

October 2020

Independently produced by:

JAVELIN

PART OF THE ESCALENT FAMILY

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This report, sponsored by SAS, explores how the increasingly digital nature of payments changes how fraud occurs and how mitigation efforts need to adapt. This report is based on 120 independent interviews of payment and security executives in 20 countries and analysis of data available from the various markets. Interviews were conducted in December 2019 through August 2020, capturing details pre-coronavirus, fraud occurring during national closures, and after the reopening of economies. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Digital payments around the world are growing as technology becomes more available across developing countries. In an increasingly digital environment, fraud is shifting drastically from counterfeit card capabilities toward harder-to-identify fraud schemes of social engineering, cyber intrusions, and account takeovers. What has become clear is that although the names of the payment methods may vary, criminals are attacking economies in ways many countries are under -prepared to address.

The coronavirus has not changed how fraud is committed but has shone a bright light on the risks of fraud in a digital age. The move from omnichannels to multichannel, combined with the sophisticated nature of tools that criminals have available to them, provides a road map for financial institutions to build their fraud mitigation strategy over the next several years. Without technological and operational improvements, the global rise of digital fraud will surpass the losses associated with counterfeiting magnetic stripe payment cards.

This report provides readers with a clear picture of how digital fraud has changed the operating environment globally. Financial institutions face significant risks, in reputation and from financial losses, if changes are not implemented. Several recommendations can be deployed quickly to provide immediate relief, while others will be developed over the next several years. The modifications to the business model not only will improve loss metrics but also will deliver confidence to the consumer and build trust in the brand.

EXECUTIVE SUMMARY

KEY FINDINGS

Digital fraud trends have become more sophisticated over the past two years but have accelerated in the past nine months as the coronavirus (SARS-CoV-2) has changed how consumers interact with financial services and commerce. Consistent responses from executives in 20 countries provide details on the increased frequency of fraud attempts and how different countries are addressing the challenges.

The fraud trends have significant points in common even though the geographies are wide—the markets in the Americas, Europe, Middle East, Africa, and Asian Pacific each experience similar attacks across digital payments; however, methods of detection and prevention are still minimal because of the rapid rise of the payment technology. New payment experiences that are launched do not have adequate fraud mitigation measures in process at the time of launch due to a lack of understanding of how the criminals will exploit the technology.

Identified trends expand to multiple digital payment methods, including digital wallets, person-to-person payments, merchant QR code payments, and remittance. Criminals are leveraging the instant and real-time payment networks to rapidly steal and launder the funds, making recovery more difficult and leaving consumers with the responsibility to pay.

The methods used by criminals are varied but are consistent across multiple countries, indicating coordinated and organized use of technology to attack the financial services industry. Social engineering, technology exploitation, and data breach events provide criminals the ability to coordinate and orchestrate attacks that are designed to bypass current fraud mitigation strategies.

The trends in the U.S. market associated with identity fraud attacks are mirrored in other countries that are also implementing digital payments. The current fraud loss rate for point of sale in the U.S. is 1.2% of all purchases, compared with card-not-present fraud rates at 3.1% of all purchases. With legitimate point-of-sale transactions decreasing because of the coronavirus effect on economies and the increase in card-not-present activity, the compression of fraud loss rates will continue.

Merchants have seen an increase in a hybrid fraud method, in which consumers buy online and pick up in-store. The ease of using stolen payment credentials online and having a mule network to pick up the product changes the dynamic of in-person fraud. Online identity verification and transaction monitoring is not effectively capturing this fraud method.

Internationally, criminals are using social engineering to bypass fraud controls by enticing consumers to participate unwittingly in the fraud. Phishing incidents across all channels—email, text message (SMS), voice, and fraudulent applications—are being used to gather data needed for account takeover and scams. The expansion of instant payments makes it the fastest way for criminals to cash out a fraud scheme.

Cross-border fraud takes on a new definition. Beyond currency conversion, financial institutions are having to manage international threats through digital fraud channels. Executives confirmed that international fraud organizations have been identified as perpetrators, which requires more coordination to stop criminals from committing digital fraud.

The greatest technology challenge executives discussed focused on the large amounts of data that are available with digital payments and the complexity of needing multiple solutions to quickly analyze and make decisions. Many financial institutions continue to reply on consumer education, transaction message information for authorization, and post-authorization transaction monitoring.

Operations were hampered due to the restrictions of staff members not being in the office and the communication channels to consumers being limited. Fraud strategies needed rapid modifications due to the high usage of predictive modeling based on past behavior. Neural network models and rules reliant on score were inaccurate due to the activity being abnormal for the full portfolio.

RECOMMENDATIONS

Migrate all fraud monitoring activity to real-time assessment, removing batch processing from transaction analysis. Batch processing of non-monetary transactions or perceived low-risk transactions reduces the likelihood that high-risk activity can be prevented before the loss of funds. Authorization decisions as well as post-authorization decisions should be updating analytics in real time.

Deploy cloud infrastructure for fraud management systems, enabling large data-ingestion capabilities to start using data rivers and move away from data lakes. Ingestion of large amounts of data elements to be used in real time requires multiple data streams to be analyzed simultaneously to make real-time decisions. The pulling of data to a centralized repository can still be maximized for reporting and analysis.

Layer analytic approaches to stop losses before they occur. A layered-model approach—inclusive of consumer, receiver, merchant, device, and other key indicators on the multiple components of the transactions—is required. Focusing solely on the consumer behavior does not identify the complexity of digital fraud, where criminals are able to cast a wider net, and thus limit impact per account. Each of the models should enable adaptive learning to quickly identify fraud trends.

Centralize decision-making through a common rules engine for all payment methods to have a customer-centric view of the transaction. Transaction authorization is generally required in multiple systems; however, the transactions should all be sent to the same rules engine for case management, automated card blocking, and consumer contact. All consumer activity should be available, allowing for decisions that find fraud faster and reduce the negative consequences of false positives.

Use link analysis to identify common traits across fraud cases and determine when organized rings are attacking the payment system. Finding the commonalities provides the ability to determine if a data breach event has occurred and if payment methods should be reissued. Use the common traits to deploy new fraud strategies targeted at the fraud event and minimize negative impacts to consumers.

Create rules to interrogate receiver information for person-to-person (P2P) transactions and identify when a consumer may be falling victim to a scam. Consumers can easily be tricked into providing sensitive information or providing screenshots of payment information to complete a purchase. Preventing screen image capture in payment applications, validating GPS location via QR code, and confirming the receiver of the funds can create profiles of criminal activity and prevent transactions from being processed.

Include cybersecurity, identity management, and access with fraud prevention and detection tools to provide a layered approach to quickly identifying fraud. With multiple payment channels having the same funding source, the identification of fraud requires monitoring and protecting every access point. The multiple analysis tools should be orchestrated into a centralized fraud management system to provide data transparency across the enterprise.

Expand fraud investigations to include anti-money-laundering efforts and identify money mules and consumers unwittingly ensnared in money-laundering activities. Use anomaly detection to combine real-time and historical data across the enterprise to identify criminal activity. Money-laundering activities need to move beyond what the customer is doing to the identification of receivers who are part of the money-laundering schemes.

Reduce reliance on staff to monitor fraud activity by using automated actions and predictive case management. Identifying the highest-risk activity will improve the false-positive rate and reduce operational oversight required to rapidly adapt to new fraud schemes. Having an API-based infrastructure that connects to multiple systems to trigger actions (communication, card status changes, reporting, etc.) will increase the efficiency of the fraud management organization.

FRAUD MORPHS THROUGH DIGITAL CHANNELS

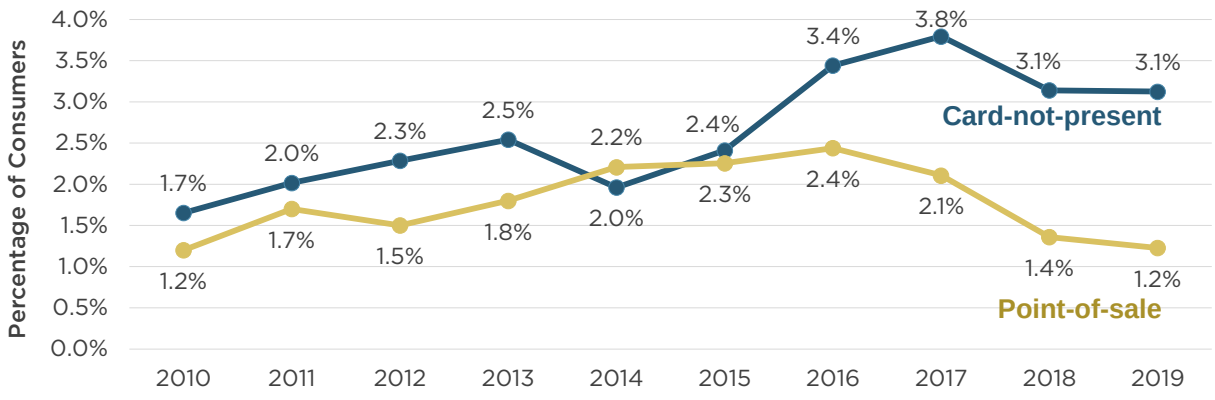
The coronavirus economy demonstrates the differences between in-person and digital fraud transactions in a way that years of data and research have not been able to articulate. Trends over the past decade have indicated the shift to digital payments; however, the coronavirus pandemic acts as an accelerant to change.

Overnight, in-person transactions were not allowed or were severely limited to essential business. Travel spending dried up overnight. To counteract the changes to how consumers could engage with businesses, e-commerce and mobile activities were accelerated, focusing more on accessibility and acceptance than on how criminals would use the technology to steal faster. In normal economies, the percentages of fraudulent transactions are wide. However, newer fraud schemes with digital payments will change how the industry evaluates fraud going forward.

As the second-largest e-commerce market in 2019, the United States provides a glimpse into what is occurring in other digital economies.[1] The curved rate of card-present activity demonstrates the move of cards to EMV technology and the rapid use of counterfeited cards before the conversion was completed. The United States has returned to pre-EMV conversion levels of point-of-sale fraud, with new technology slated to reduce risk even further with tokenization via smart devices. The digitalization of point-of-sale activity provides immediate reductions in point-of-sale fraud, but the longer the technology is relied on, the more likely it is that criminals find ways to bypass the security with account takeover, P2P fraud via social engineering, and click-and-collect fraud. The perceived anonymity of online commerce, paired with the ability to commit fraud regardless of location, will ultimately increase fraud rates.

Compression of Card Channel Fraud Losses Will Occur With Digital POS

Figure 1. U.S. Card Transaction Fraud Rates, 2010 -2019



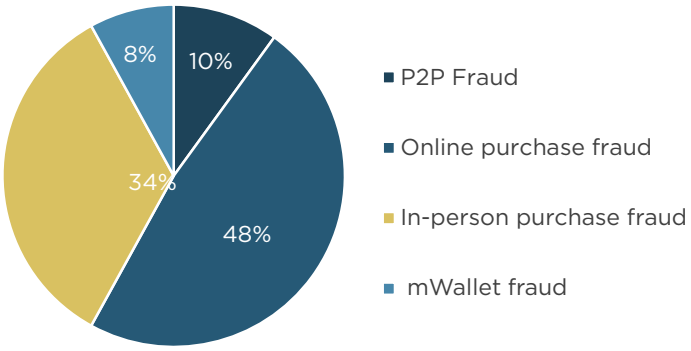
Source: Javelin Strategy & Research 2020

New payment methods in a market will be seen as ripe for manipulation. In the United States, the expansion of person-to-person payments to conduct commerce on social media or for small-business payments has caused an explosion of fraud. From 2016 to 2019, P2P fraud increased 733% as criminals found ways to gain trust and have the consumer transfer funds unwittingly in scams or have accounts taken over. The United States is highlighted as a warning to other markets that are rapidly rolling out different types of faster payments, which instantly transfer funds and are irrevocable.

To transform fraud mitigation strategies, solutions need to be inclusive of how consumers interact with the payment ecosystem to identify where the vulnerabilities are. It is no longer acceptable to monitor transactions in silos. The monitoring needs to happen holistically from point of origination and identity verification, through authentication, account modifications, receivers and transactional—all in real time to keep new fraud trends in check. Instant payment schemes are now normal throughout the world, yet anti-fraud strategies have not moved at the same speed to adapt and reduce risks

Fraud Incidents Now Include Digital Wallet and P2P Activity

Figure 2. Incidents of Card Fraud in the U.S., 2019



Source: Javelin Strategy & Research 2020

Digital Wallets Defined

- Accounts that enable consumers to store value—fiat, crypto, rewards, incentives—or other instruments that enable value to be stored and dispersed.
- Enabled via software on mobile devices, payment credentials are stored online without a physical payment card required.
- Funds can be transferred at a point of sale or through P2P activity, remittance services, or crypto exchanges.

United States—
Digital Wallets (Apple Pay, Google Pay, Samsung Pay)

Digital wallet fraud and person-to-person fraud have dramatically risen in the past three years, now accounting for 18% of all card fraud in 2019.[13] Account takeover has risen 70% from 2018 to 2019,[14] which makes it easier for criminals to add stolen credentials to a digital wallet with little friction and identity-proofing. Consumers do not need to enroll their card within the mobile banking app but instead can load accounts directly in the digital wallet. Even if a one-time password is sent, SIM swapping fraud will intercept the password and enable the criminal to validate the card provisioning. **Financial institutions should increase consumer control monitoring and control settings to add a layer of authentication. Updating of fraud detection strategies to identify newly provisioned credentials to validate the transaction is also needed to reduce the fraud through digital wallets.**

GLOBAL RISKS OF DIGITAL PAYMENTS

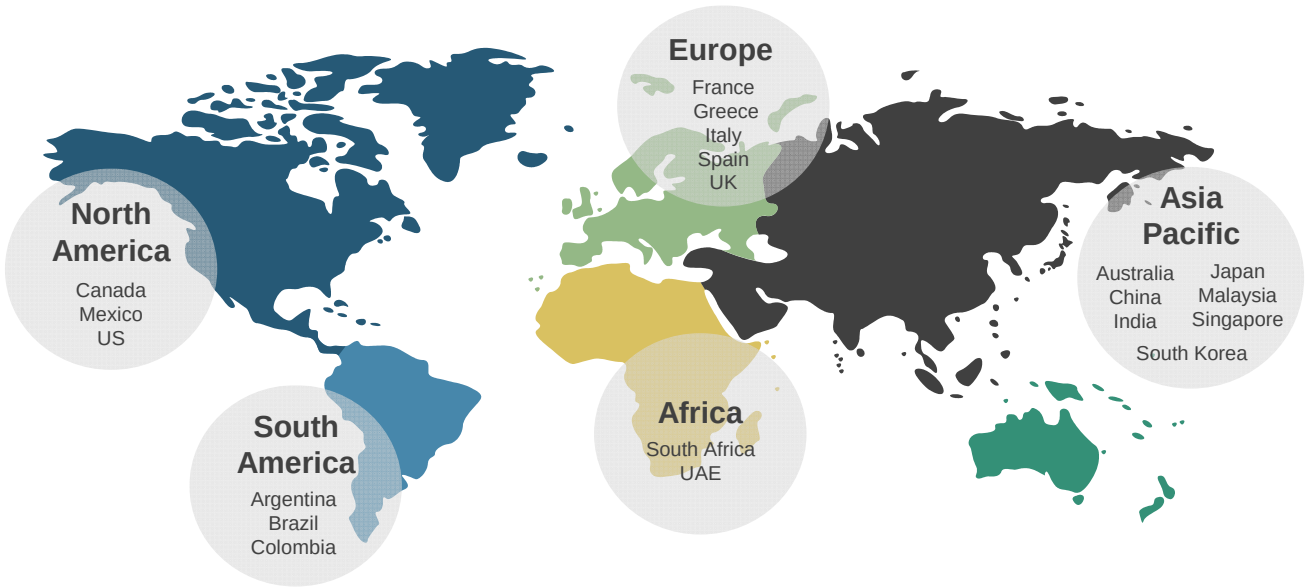
Each country, and each payment method, comes with its own challenges. However, there are more elements in common, indicating criminals are coordinated in their attacks, share information, and work together to steal. Criminals communicate more openly and freely than financial institutions do, placing fraud management professionals at an immediate disadvantage. Understanding how fraud has been occurring across digital channels globally is the first step toward reducing risks.

Standard metrics of basis point loss ratios or percentage of transactions do not necessarily apply to each market due to the loss of legitimate sales. It's critical to understand how digital fraud occurs to reduce risks when new payment methods are deployed. Too often, new payment mechanisms are launched before risk mitigation controls are available.

> We have seen an increase of almost 35% in fraud attempts, which indicates that criminals are more active in breaking through digital channels, taking advantage that fraud strategies leverage normal behavior—nothing is normal from a transaction perspective in 2020.
>
> **Senior Executive, Global Card Processor**

Global Digital Fraud Trends

Figure 3. Countries Researched for 2020 Fraud Trends



Source: Javelin Strategy & Research 2020

AMERICAS

The countries on the two continents are still in the midst of the criminal behavioral changes associated with the United States' migration of cards to EMV, which will now be April 2021, as petrol stations have received a compliance deadline extension due to the coronavirus impacts.[2] The ability to capture magnetic strips and easily counterfeit cards means that card-present fraud is still viable, especially for cross-border activity and ATMs. The increased access to digital commerce in each of the countries also represents a greater risk to financial institutions that need to combat many fraud types simultaneously. Technology and analytic capabilities need to be layered to identify the multiple threats in real time.

POST CORONAVIRUS TRENDS - AMERICAS

"Counterfeit card fraud has decreased, however card not present transactions (browser and mobile) continue to increase. Click and collect fraud is especially a challenge because validating the person in the store to the person who was online is tricky. We are used to porch pirates and non-receipt fraud. What we did not plan for is the amount of grocery fraud from online channels."

Large Merchant, Fraud Operations Analyst, United States

"The biggest challenge we have is with counterfeit cards here in Mexico. We struggle with merchant terminal acceptance of EMV and magnetic stripe counterfeiting is still easy. When the US moved to EMV we started to see an increase of foreign card fraud in Mexico."

Product Manager, Fraud Management for LAC Region, Payment Processor

"In the US we see card fraud reducing because we have more mature fraud detection models. What we do see is that the fraud migrated to P2P and account takeover of the checking account. Criminals are looking for ways to get cash faster. Digital is a low friction, low risk way of stealing. In a way, EMV helped reduce fraud but hurt us because the fraud moved to a way we were not prepared for."

Senior Fraud Director, Financial Institution in the United States

"Authentication continues to be a high priority as we build real-time payments in Canada. The irrevocability of funds and how quickly they disappear is a big red flag. Finding ways to get more data into our fraud systems to monitor senders and receivers is important."

Fraud Management Director, Financial Institution in Canada

"Authentication is becoming a larger problem with mobile payments and SIM swapping. What used to be the known device is now changing and we do not see that information in our fraud management system. This is an area we need to improve on to make sure we know who is making the purchase."

Executive, Payment Platform in Brazil

"The coronavirus has highlighted that our consumer contact capabilities and automated actions do not meet the digital needs. Previous efforts focused on reducing operational expense – we now need to focus on the need to provide services during our worst case scenario – all digital. How we use home assistants, voice bots, and newer communication protocols needs to be on the table."

Fraud Management Executive for South American Operations for a Global Financial Institution

Argentina—
E-Commerce Marketplace

Credit card fraud continues to expand as consumers move online and cross-border payment acceptance rises through marketplaces like Mercado Pago. The online and app-based marketplace makes it easy for criminals to steal, and fraud methods across different banks in the region can vary. As the Argentinian bank launches a digital wallet to compete against Mercado Pago, expect that real-time payment and digital currency fraud will occur.[3] **The managing of directories, the monitoring of sender and receiver, and a reduction of the ability to screen capture QR codes are needed to combat the growing fraud risks of a digital economy.**

Brazil—
PIX

QR message standardization will be occurring in September 2020,[4,5] which will help reduce the risk of fraudulent payments and ensure EMVco's standards.[6] Standardization using the ISO 20022 messaging capabilities provides financial institutions with the ability to interrogate the authorization data in real time and identify potential fraud activities. With the cost of the transaction being fixed by the Central Bank of Brazil, the revenue to financial institutions will not be based on interchange revenue, which can offset fraud losses. **Fraud management strategies need to take this into consideration by monitoring all transactions in real time and having analytic capabilities that can quickly identify fraud schemes.**

Colombia—
Cross-Border Remittance

Colombians are emerging into the digital economy, with 24% of people turning to online commerce in 2018.[7] With the coronavirus pandemic, more Colombians have access to the digital economy as banking becomes more inclusive and digitally provides services to nearly 85% of the population.[8] However, with the digital economy comes the heightened risk of scams, which range from low-dollar to high-dollar losses. In 2019, an international law enforcement effort shut down a $15 million (USD) stock scheme that affected people from Colombia to Switzerland.[9] Moving quickly from cash to digital, consumers may not have situational awareness to know when a scam is being perpetrated. **Fraud management strategies need to recognize large-dollar transfers that are not part of the normal spending behaviors.**

Mexico—
CoDi

CoDi, the Mexican real-time payment system launched in September 2019,[10] also uses the ISO 20022 standard in the Interbank Electronic Payment System (SPEI), which will ultimately make connecting between countries possible in the future.[11] The intent is to leapfrog legacy payment infrastructures by moving from paper currency to mobile in one step. The risk management infrastructure that comes with progression from cash to cards to digital is missing from organizations. Enabling P2P and merchant acceptance via QR code and NFC immediately increases the risks of scams, which are prevalent in Mexico.[12] **Financial institutions will want to monitor receivers of funds to create analytic profiles and spot scams and fraudulent merchants before funds are transferred.**

ASIA PACIFIC (APAC)

The technology modernization efforts in the Asia Pacific region span from very advanced digital commerce capabilities to a wide acceptance of cash. Before the SARS-CoV2 (COVID-19) pandemic, inroads were being made to move away from cash, but the desire to reduce physical contact during outbreaks has driven a wider acceptance.[15] From the India Unified Payments Interface (UPI), interbank ATM cash deposit capabilities,[16] which will enable transfers to Malaysia's expansion of over 45 digital wallet providers,[17] the cash acceptance forecast shows a trend toward digital commerce and wallets.

POST CORONAVIRUS TRENDS - ASIA PACIFIC

"Consumers are under an increasing attack of phishing and scams. Unfortunately with some of the newer ways to pay, QR code and request to pay fraud have all increased with little ability to stop it. Relying on consumers to not fall prey to the sophisticated schemes is not a great strategy."

Risk Management Executive, Financial Institution in India

"Moving India from cash to digital currency has been at a rapid pace which has caused a lot of challenge in how we manage fraud. India has been managing card fraud for years, however new consumers who do not understand how QR codes work, how small merchants can accept payments, has been a challenge. QR codes are very safe, but not when consumers are scammed to giving screenshots to criminals. Finding ways to educate consumers on digital currency has been a major effort in our country."

Senior Executive, Fintech Firm in India

"Batch processing is no longer sufficient when addressing fraud. Previously we had some transactions flow real-time with other transactions batched frequently, but some end of day. We need to move to 100% real-time to minimize the loss rates and protect our bank's reputation."

Senior Risk Executive, Financial Institution in Japan

"Payment card fraud continues to grow, with more problems coming from cross border activity. Having a nation of people who migrate for work, providing payroll services to those abroad and at home has challenges to ensure there is no disruption. When fraud occurs, the full paycheck is lost and cannot be refunded."

CEO Prepaid Card Product, Malaysia

"The greatest breakthrough? Being able to use the data we already had more efficiently. Moving the nation towards API data integrations to facilitate open banking has created many technology breakthroughs in Australia. Enabling faster data access and sharing provides the fraud systems the ability to not wait for overnight batches of information. Cloud storage has also reduced the expense of managing multiple data access points."

Senior Executive, Australia Payment Firm

"We haven't seen a decrease in existing fraud; what we have seen is a continued increase in losses as new payment methods are added. We manage fraud across multiple markets for banks; digital payments, scams, and account takeover have been where our clients have seen the losses increase."

Senior Account Manager, Payment Processor for APAC Region

Australia—
New Payments Platform

Although a lot of time has been spent looking at identity fraud management on the new payments platform due to the PayID data breach in 2019,[18] the fraud from this event was minimal and proved more a lesson on how to secure the ecosystem. The greatest current threat is the number of non-nationals who are unable to work or attend university in Australia because of the pandemic.[19] Increasingly on dark web communication sites, people can be found selling their identity in that country because of an inability to return, in many cases due to finances. Selling true identities that have been validated can lead an increase to bust-out fraud—where credit lines are rapidly used and the consumer cannot be contacted for repayment. **This will bypass authentication capabilities, which are used to capture synthetic identities. The fraud needs to be detected during bust-out scenarios through fraud detection strategies.**

China—
Nets Union Clearing Corporation (NUCC)

The explosive growth of fintechs providing payments outside of the governmental agencies started to cause concern with the rapid rise and liquidity challenges of instant payment networks. The liquidity risks rose significantly to the point that the Chinese government suspended new license issuance for fintech money transfers.[20] In June 2018, China started to regulate the fintech platforms to create a new regulatory body, NETS Union Clearing Corporation, to act as a clearing and settlement apparatus for P2P payments to ensure funding and liquidity.[21] The lack of needing to register name and bank account information to send funds increased money-laundering rates, which led to an increased need to know who the sender and receiver of the funds were. **Financial institutions that leverage the Chinese payment capabilities need to include money laundering and other financial crimes within their risk mitigation strategies to account for the ease of laundering money in a digital wallet.**

India—
WhatsApp

QR code capabilities are made available to multiple payment and merchant mobile apps. WhatsApp has QR code capability added to the platform to be used for merchant and peer-to-peer payments. Unfortunately, consumers who receive phishing text messages requesting confirmation of the codes or validation of PIN numbers can take screenshots of the QR code and banking information and send it to the criminal to use.[22] The social engineering of payment fraud has escalated since the coronavirus pandemic began, with the Reserve Bank of India going public with the notification that the schemes are fraudulent.[23] The QR code that was meant for in-person payment activity has now moved to remote channels. **Consumer education campaigns, disabling screen captures, and real-time transaction monitoring are needed to identify when scams are occurring.**

Japan—
PayPay

In June 2018, PayPay launched in Japan and did not have immediate issues with fraud. However, a major fraud scheme was identified in December 2018, when an incentive program provided a 20% rebate to users.[24] Although the program was expected to last a quarter (end of March 2019), the rebate program ran out of money in 10 days. Criminals were loading stolen card credentials into PayPay, using the payment fraudulently, and getting a 20% cashback rebate. Not only were the card and bank credentials at risk, but the $90 million USD funding of the rebate was lost as well.[25] **Financial institutions will want to set best-practice standards of validating when a card is stored in a digital app and update fraud detection rules to know when a card is recently added. Using additional capabilities, such as 3D Secure, and sending the data into the fraud detection system in real time will also improve monitoring to know when stolen card data is being used in a digital point-of-sale fraud.**

Malaysia—
Bank Transfers

The speed of change—moving from cash to digital wallets—has built a system of anonymity and accessibility for criminals to take advantage of. Add into the equation downward economic shifts and an increase in unemployment, and criminals can recruit money mules more easily. The Internet Banking Taskforce is actively working with financial institutions to monitor and identify mule accounts to minimize laundering from trafficking and counterfeit goods. Financial institutions can help in explaining how money mules are used to launder funds and commit fraud.[26] **Real-time transaction monitoring and link analysis to identify accounts in a mule network will help minimize digital fraud risks in Malaysia.**

Singapore—
Fraudulent Mobile Apps

Straying from approved app stores through the technology providers (Apple, Google, Samsung, etc.) and into app marketplaces can increase the risks of fraudulent apps. Apps that look like the financial institution's mobile app, P2P transfers, and merchant accounts can capture and store valuable personally identifiable and payment credentials that are used for fraudulent activity.[27] Criminals are using the coronavirus and consumers' desire for information to trick them into downloading what appear to be contact-tracing methods but instead are methods used to take over accounts.[28] **Credit and debit card transactions on newly provisioned devices or through new apps should have additional monitoring to ensure that the consumer has not been tricked into providing sensitive information.**

South Korea—
Black Market Sales of Card Credentials

Data breach events continue to have an impact on the South Korean market, with card details being sold on the dark web in various forums.[29] One of the largest caches of card data found in 2019 impacted a significant number of South Koreans, which raised counterfeit fraud activity.[30] With the expansion of P2P apps being used throughout Asia Pacific, stolen card credentials are being used to quickly transfer funds from one account to another, creating a web of transfers that can be challenging to trace.[31] **To minimize counterfeit-card fraud, strategies for P2P activity and e-commerce need to balance the needs of frictionless experiences and additional edit checks on the transaction data and velocity of spending.**

EUROPE, MIDDLE EAST, AND AFRICA (EMEA)

Prior to 2020, EMEA has seen similar impacts to card fraud as more digital methods become available and regulatory action creates harder paths to steal in traditional card channels. The expansion of digital wallets, instant payments, direct debits, and push payments means that consumers and financial institutions are being assaulted by way of multiple digital fraud methods. Card fraud rates increased across the European Union by 13% even as other payment channels were under assault; nearly 80% of card fraud involved digital transactions.[32] With more merchants adding card-not-present options, challenges with cross-border verification, and expansion of faster payments, the EMEA region needs to remain on guard in the post-coronavirus economy more than in years prior.

POST CORONAVIRUS TRENDS- EUROPE, MIDDLE EAST, AFRICA

"We had to adjust our fraud contact center strategies – basically our call centers were closed but consumers needed to be reached. We switched all communication to digital channels, preferring mobile push because it is more secure. However medium risk fraud was sent an email and many cases were closed automatically with no action. To reduce case volumes we turned off rules that had false positive rates above 30:1."

Fraud Strategy Manager at a Financial Institution in the United Kingdom

"Data, data, data. Have I said data? We need to pull all consumer and account data into the debit model. We are missing account takeover activity because we do not see the full picture and are focused on the transaction versus the funds flow."

Senior Executive of Payment Processing in MEA for Mastercard

"We are interested in looking at newer analytics, multi-layer and self-calibrating. We need to have a smarter way to handle rapid change without significant workforce challenges."

Senior Analytics Strategist at a Card Brand Focusing on European Clients

"We made the decision to stop using the fraud score as a factor in the decline of a transaction. The first "hoarder shopping" before the official lockdowns started really made the analytics off balance. And once off balance, our fraud system settings place the account in suspense from monitoring for 30 days if triggered by a fraud score. Basically, because nothing was normal, if we only used the score threshold the wrong decisions would have been made."

Fraud Operations Manager at a Global Payment Processor

"We have seen an increase of almost 35% in fraud attempts which indicates that criminals are more active in breaking through digital channels, taking advantage that fraud strategies leverage normal behavior – nothing is normal from a transaction perspective in 2020."

Senior Fraud Management Executive at Global Payment Processor

"Fraud attempts rose to 5.3% in April 2020 up from 3.7% in April 2019 – this indicates that what we know about card not present transaction is true – there is a higher fraud risk as transactions become more digital."

Merchant Risk Management Executive for International Payment Processor

"Criminals are focusing on specific industries, and the fraud attacks are global in nature. Understanding how different fraud schemes originate can help identify what measures need to be implemented to prevent fraud loss. Telecommunications, e-commerce, and financial services are all top targets."

Senior Fraud Executive at Global Identity Firm

France—
PayPal and Google Pay

As a member of the European Union, France is in the implementation phase of the Payment Service Directive 2 (PSD2)[33] for the deployment of stronger authentication for e-commerce activity. Criminals are actively working phishing attacks to obtain card and direct debit information from consumers under the guise of receiving subscription purchases or goods associated with remote purchasing because of the pandemic.[34] By obtaining PayPal credentials through remote channels, the criminals are able to load the PayPal account into Google Pay and perform fraudulent transactions.[35] **Financial institutions should be prepared to rapidly update rules to balance analytics accommodating payments processed on bank accounts and cards associated with PayPal and for Google Pay transactions. Transactions could be e-commerce, in person via QR Code, or P2P activity.**

Greece—
Synthetic Fraud

Fraud in Greece can often be found in forged documents[36] and synthetic identities, with travel to other countries easily completed as a gateway to other parts of the continent.[37] Risk management executives in the region are concerned that a large increase in card-not-present fraud has not occurred compared with some of their peers in other countries. The stabilization of fraud rates raises the question of what is being missed, with an estimation being an increase in synthetic fraud booked as legitimate accounts. **Financial institutions should consider adding digital identity data—including analytics of documents, device sessions, and other digital footprint components—into their fraud rules engine for transaction monitoring.**

Italy—
Malvertisements

Direct-debit fraud has been on the rise throughout Italy as consumers are caught in false advertisements for goods or services that ultimately are never delivered. Using wire and instant-payment mechanisms, the victim sends the funds, which can immediately be moved, thus making the fraud difficult to find.[38] Malicious advertisements do not necessarily need to be maintained in Italy, The digital nature of fraud means that data can be stolen and used anywhere, similar to the recent fraud ring identified in Singapore.[39] **Fraud detection strategies should include providing consumer controls on cross-border and online commerce, with the data being leveraged within the fraud detection rules engine to balance false positives while still detecting instances of fraud.**

Spain—
SIM Swapping

Phone number theft can be a gateway to account takeover by gaining access to digital wallets and other accounts stored within the phone profile with the carrier.[40] Recent arrests in Spain indicate how prevalent this fraud is and the amount of money that can quickly be stolen.[41] Taking over the SIM is the

first step, and the second comes with taking over the bank accounts, calling into customer service, or making account modifications online. If the email account is also taken over, the criminal then has full access to have the multi-factor authentication via email or SMS, making account takeover inevitable. **Financial institutions need to provide in real time the account changes—password resets, email changes, PIN changes, and any other non-monetary transaction—to minimize losses.**

United Kingdom— Push Payments

Push payments are another way scams are proliferating globally and criminals are able to get away with a significant sum of money. In 2018, UK citizens lost £354 million,[42] and the total was £456 million[43] in 2019, demonstrating the ease with which criminals are able to bypass security measures and use social engineering tactics directed toward consumers. The losses triggered a new system—Confirmation of Payee[44]—to be developed to minimize the risks and provide consumers with the ability know who they are sending funds to. The process is relatively intuitive, with each financial institution managing the workflow within its digital banking channels. When a new payee is added, a confirmation is completed, and consumers can be warned if a scam is being perpetrated.[45] **Payment schemes and financial institutions will greatly benefit from having identity verification and fraud modeling on receivers to minimize push-payment fraud as instant and real-time payments expand globally.**

South Africa— Credit Card Fraud Schemes

Credit card fraud increased 32% between 2018 and 2019, to a total of R652 million, a majority being card-not-present transactions (R404m).[46] Adding to the complexity of the fraud is that two-thirds of the credit card fraud happens through cross-border activity, making it more challenging to investigate and link to broader criminal networks. International activity often occurs in travel and entertainment merchant category codes, which most likely will not be the primary focus through 2020 as travel transactions are reduced during the pandemic. International activity is starting to mimic more of the domestic fraud, which includes tolls, supermarkets, ATMs, and other goods and services. **Fraud strategies on credit cards need to be evaluated frequently to ensure that the changing nature of fraud—what is available for criminals to steal—can be adapted to in those strategies.**

United Arab Emirates— Instant Payment Instruction System (IPI)

The implementation of the Instant Payment Instruction System (IPI) in 2019 has made stealing from debit accounts in real time very attractive. The Central Bank of the UAE released a consumer alert associated with scams occurring because criminals were taking advantage of the coronavirus pandemic and the traditional Ramadan donations to charity.[47,48] Phishing via email, text, and calling encouraged the sharing of personal information. In many instances, the consumer provides enough information to enable account takeovers and immediate access to funds. **Account takeover strategies need to be managed in real time due to the speed of instant payments and how rapidly accounts can be emptied.**

TRANSFORMING TO MITIGATE THE NEW DIGITAL NORMAL

To add layers of security to digital payments, different markets are using multiple tactics to reduce the risk of digital fraud. Measures to validate users with identity-proofing technologies, QR code delivery to embed EMV payment acceptance, tokenization, and encryption are being used globally. Yet the delivery of the payment mechanism does not discount the risks involved with digital transactions, and in some respects the false sense of security makes the payments more vulnerable to fraud. Creating secure delivery is not enough. To fully protect the financial services ecosystem from digital fraud, the full life cycle of fraud management needs to be modernized to accommodate not only the speed of funds movement but also the multiple access points that are vulnerable to fraud.
During each of the interviews Javelin conducted, executives were quick to point out areas where they have had success or have identified as places to begin their transformation to mitigate the risks of the digital age. It was apparent that changes in fraud were expected over time. The speed of change required initially blunt instruments to stop fraud from occurring, and there are plans to improve technological capabilities and organizational structures to be agile in response to the changes in criminal tactics. The initial skepticism that came with early national coronavirus lockdowns has now solidified into agreement that the changes are here to stay.

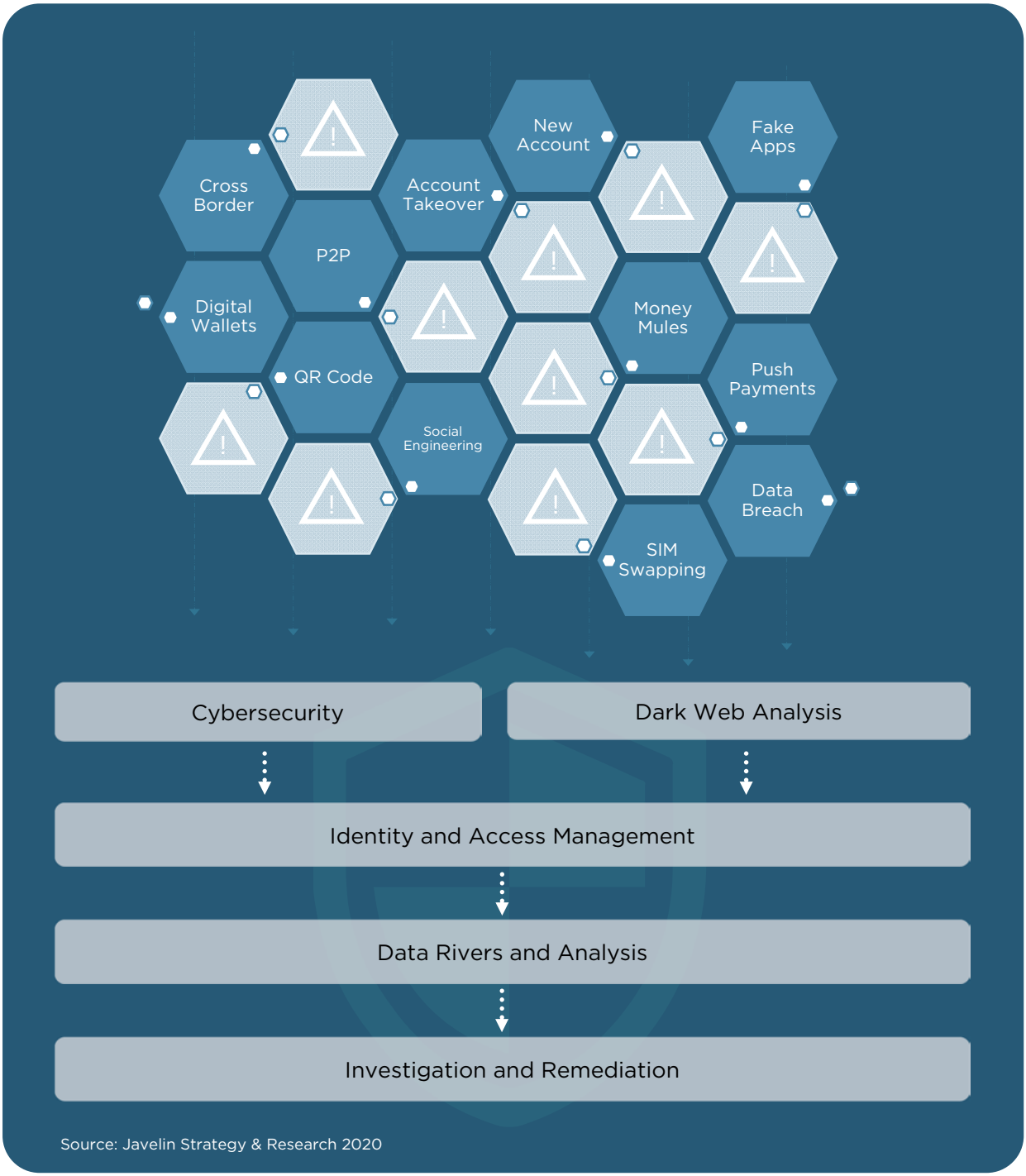
The complexity of the multiple attack vectors criminals are taking means that financial institutions must have a layered approach to preventing and detecting fraud, while also having a way to orchestrate strategies and investigation activities. Teams that might never have worked together before within the organization will need to come together as part of a fusion center to share resources, knowledge, and tactics to stop the fraud from happening. The skill sets required to do each aspect of digital fraud mitigation are different, requiring investigative skills, software development, and strategy.

Depending on the maturity of the organizations, the advancement of capabilities will vary. However, organizations at all stages of maturity have a common need for as much real-time data as possible to make decisions. The best practices that will lead the transformation required to solve the complex challenges of identity, security, fraud management, and money laundering that have been identified. Implementation of these best practices, however, depends first on an organization's data management practices.

As organizations mature and can readily access data, the next step is to transform data lakes into data rivers. Using data for real-time analytics and automated actions will be crucial to thriving in this new digital normal. The blessing of digital transactions is that more data than ever is available to drive informed decisions. The curse of more data is that it renders the age-old solution of devoting human capital to review and understand the data obsolete. Gone are the days of adding staff members to review cases. Effectively implemented data rivers will be too deep and move too swiftly for humans to navigate alone. Just as money moves in real time, so do decisions.

Multiple Challenges Require Multi-Dimensional Fraud Mitigation

Figure 4. Global Digital Fraud Types

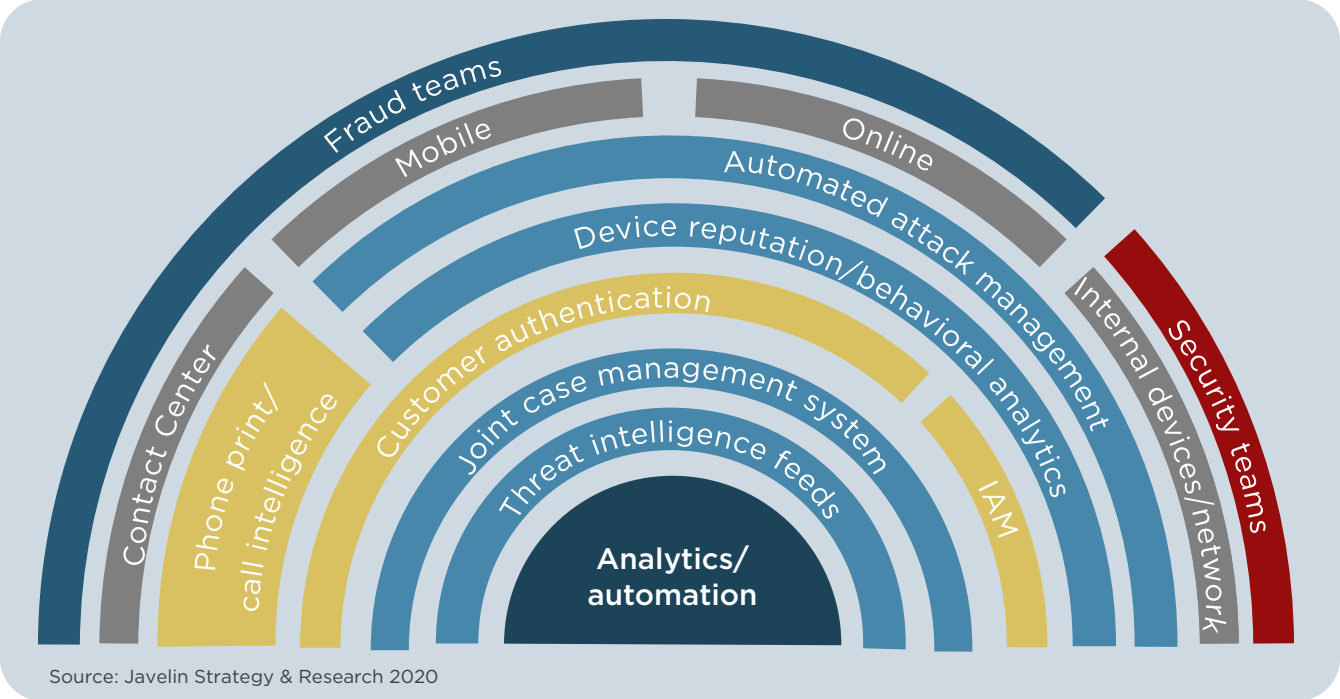


Source: Javelin Strategy & Research 2020

The diversity of attack vectors criminals are using is an aspect of the new digital normal. This diversity of fraud types—coupled with the rising speed of funds movement—demands a rethinking of the fraud management life cycle. Financial institutions must have a layered approach to preventing and detecting fraud while also being able to orchestrate strategies and investigation activities. This also means teams that may never have worked together before within the organization will need to come together as part of a fusion center to share the resources, knowledge, and tactics necessary to prevent many different forms of fraud. Investigative skills, software development, and strategy development are all skill sets required for different aspects of digital fraud management. Organizations already have these skill sets at their disposal; fraud centers facilitate the effective application of these capabilities wherever they are needed.

Digital Fraud Requires Layers of Technology to Orchestrate

Figure 5. Fraud and Security Capabilities, 2020



Source: Javelin Strategy & Research 2020

METHODOLOGY

The research for this report was compiled from 120 interviews with executives within financial services or technology between December 2019 and August 2020. The interviews were conducted at the beginning of the coronavirus outbreak through August to gain perspective through the stages of the coronavirus shutdowns. Interviewees were provided anonymity to provide them the opportunity to speak openly. Third-party confirmation of events discussed is identified and provided in the endnotes.

Number of interviews: 120

Range of titles: Chief executive officer, chief risk officer, chief innovation officer, senior vice president/financial crimes, vice president, operations manager, fraud investigator, fraud operations manager, merchant processing executive, and cybersecurity analyst.

Types of companies where the respondents work: Financial institutions (global and regional), prepaid program manager, network/scheme, payment processor (acquiring and issuing), technology.

Markets: Argentina, Australia, Brazil, Canada, China, Colombia, France, Greece, India, Japan, Malaysia, Mexico, Singapore, South Africa, South Korea Spain, United Arab Emirates, United Kingdom, United States

Time when study was conducted: December 2019 through August 2020

For market statistics in the United States, the 2019 ID Fraud survey was conducted online among 5,000 U.S. adults over age 18; this sample is representative of the U.S. Census demographics distribution. Data collection took place from October 22 through November 4, 2019. Data is weighted using 18+ U.S. Population Benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets.

ENDNOTES

1. https://www.emarketer.com/content/global-ecommerce-2019. Published June 27, 2019; accessed July 9, 2020.
2. https://www.businesswire.com/news/home/20200723005177/en/New-Deadline-EMV-Liability-Shift-Opportunity-Upgrade. Published July 23, 2020; accessed August 6, 2020.
3. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/4-argentine-banks-to-launch-e-payment-platform-to-take-on-mercado-pago-56957930. Published February 5, 2020; accessed August 6, 2020.
4. https://www.bcb.gov.br/en/pressdetail/2334/nota. Published May 28, 2020; accessed September 25, 2020.
5. https://www.bcb.gov.br/en/financialstability/instantpayments. Accessed July 9, 2020.
6. https://www.emvco.com/wp-content/uploads/2018/05/EMVCo-QR-codes-QA_-FINAL.pdf. Accessed July 9, 2020.
7. https://www.pewresearch.org/internet/2019/08/22/in-emerging-economies-smartphone-and-social-media-users-have-broader-social-networks/pi-pg_2019-08-22_social-networks-emerging-economies_0-03/. Published August 12, 2019;accessed August 5, 2020.
8. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/covid-catalyzes-financial-inclusion-in-colombia-59068822. Published June 23, 2020; accessed August 5, 2020.
9. https://qz.com/1675811/how-an-undercover-fbi-sting-busted-a-multimillion-dollar-stock-fraud/. Published July 26, 2019; accessed August 5, 2020.
10. https://www.eluniversal.com.mx/english/codi-mexico-launches-its-qr-based-payments-system. Published September 30, 2019; accessed July 9, 2020.
11. http://www.latinamerica.tech/2019/09/30/codi-the-platform-for-digital-payments-in-mexico/. Published September 30, 2019; accessed July 9, 2020.
12. https://www.eluniversal.com.mx/english/6-most-common-types-fraud-mexico-city. Published January 6, 2019; accessed July 9, 2020.
13. Javelin Strategy and Research Securing P2P Payments, July 2020 https://www.javelinstrategy.com/coverage-area/securing-p2p-payments
14. **2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis,** Javelin Strategy and Research, April 2020.
15. https://www.policyforum.net/managing-a-second-spike/. Published June 25, 2020; accessed August 6, 2020.
16. https://economictimes.indiatimes.com/industry/banking/finance/banking/you-can-soon-deposit-cash-at-any-atm/articleshow/73178997.cms?from=mdr. Published January 10, 2020; accessed August 6, 2020.
17. https://www.bnm.gov.my/index.php?ch=ps&pg=ps_regulatees. Accessed August 6, 2020.
18. https://www.finextra.com/newsarticle/34291/aussie-banks-warn-of-payid-data-breach?utm_medium=rssfinextra&utm_source=finextrafeed. Published August 21, 2019; accessed August 6, 2020.
19. https://www.policyforum.net/what-does-australia-look-like-without-international-students/. Published June 30, 2020; accessed August 6, 2020.
20. http://www.chinabankingnews.com/2018/04/16/chinas-third-party-payments-providers-severe-direct-ties-bank/. Published April 16, 2018; accessed August 6, 2020.
21. Research on the influence of China Nets Union Clearing Corporation on third-party non-interest payment business by Yuguo Yang in the Advances in Economics, Business, and Management Research volume 76, 2019.
22. https://economictimes.indiatimes.com/wealth/save/5-digital-payment-frauds-and-how-to-avoid-them/new-forms-of-payments-offer-scope-for-confusion/slideshow/72168663.cms. Published November 21, 2019; accessed July 9, 2020.
23. https://www.indiatvnews.com/business/news-rbi-warns-phishing-chinese-cyber-attacks-fraud-transaction-digital-payments-reserve-bank-of-india-sbi-bank-628789. Published June 24, 2020; accessed July 9, 2020.

24. https://www.japantimes.co.jp/news/2018/12/17/business/corporate-business/japans-paypay-update-app-wrongful-charge-complaints/. Published December 17, 2018; accessed September 25, 2020.
25. https://www.bankinfosecurity.com/japans-december-credit-card-fraud-debacle-a-12021. Published February 13, 2019; accessed September 25, 2020.
26. https://www.cimb.com.my/en/personal/help-support/security-and-fraud/money-muling.html. Accessed August 6, 2020.
27. https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data. Published June 10, 2020; accessed August 6, 2020.
28. https://www.csa.gov.sg/singcert/advisories/ad-2020-004. Published June 12, 2020; accessed August 6, 2020.
29. https://www.group-ib.com/media/south-korean-and-us-banks-cards/. Published April 24, 2020; accessed August 6, 2020.
30. https://krebsonsecurity.com/2019/10/takeaways-from-the-566m-briansclub-breach/. Published October 29, 2019; accessed August 6, 2020.
31. https://pulsenews.co.kr/view.php?year=2020&no=589848. Published June 9, 2020; accessed August 6, 2020.
32. https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html#toc3. Published August 14, 2020; accessed September 15, 2020.
33. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en. Accessed August 6, 2020.
34. https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/lamf-et-lacpr-mettent-en-garde-le-public-contre-les-risques-darnaques-dans-le-contexte-de-lepidemie. Published March 26, 2020; accessed August 6, 2020.
35. https://www.zdnet.com/article/paypal-accounts-are-getting-abused-en-masse-for-unauthorized-payments/. Published February 25, 2020; accessed August 6, 2020.
36. https://counterfeitnote.co/shop/fake-drivers-license/purchase-fake-greece-drivers-license/. Accessed August 6, 2020.
37. https://exit.al/en/2020/02/21/greek-fake-passport-ring-busted/. Published February 21, 2020;accessed August 6, 2020 and https://bestcounterfeits.com/product/buy-fake-greece-drivers-license-online/ August 6, 2020.
38. https://www.europol.europa.eu/newsroom/news/italy-and-romania-take-down-cyber-fraud-ring-generating-%E2%82%AC20-million-year-in-criminal-profits. Published July 7, 2020; accessed August 6, 2020.
39. https://www.straitstimes.com/singapore/courts-crime/at-least-21-people-in-singapore-fall-prey-to-transnational-online-credit-card. Published July 28, 2020; accessed August 6, 2020.
40. https://www.issms2fasecure.com/dataset. Accessed August 6, 2020.
41. https://www.euroweeklynews.com/2020/07/10/spanish-mobile-phone-scam-94-arrested-in-e500000-cloning-fraud/. Published July 10, 2020; accessed August 6, 2020.
42. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf. Accessed August 7, 2020.
43. https://www.finextra.com/newsarticle/35480/app-fraud-losses-hit-456-million-in-2019. Published March 19, 2020; accessed August 7, 2020.
44. https://www.lendingstandardsboard.org.uk/contingent-reimbursement-model-code/. Accessed August 7, 2020.
45. https://www.wearepay.uk/10-common-confirmation-of-payee-questions-answered/. Accessed August 7, 2020.
46. Sabric Annual Crime Stats 2019.
47. Consumer Beware – Fraudulent Actions During Covid-19 Pandemic, Central Bank of U.A.E 5.17.2020. Accessed August 7, 2020.
48. https://www.centralbank.ae/en/node/2186. Published May 17, 2020; accessed September 25, 2020.

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research helps its clients make informed decisions in a digital financial world. It provides strategic insights for financial institutions, government, payments companies, merchants, fintechs and technology providers. Javelin's independent insights result from a rigorous research process that assesses consumers, businesses, providers, and the transactions ecosystem. It conducts in-depth primary research studies to pinpoint dynamic risks and opportunities in digital banking, payments, fraud & security, and lending. For more information, visit javelinstrategy.com. Follow us on Twitter and LinkedIn.

Author: Krista Tedder, Director of Payments

Contributors: Jacob Jegher, President
Crystal Mendoza, Production Manager

Publication Date: October 2020

ABOUT SAS

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 70,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW®.