ISO&AGENT
May/June 2018
www.isoandagent.com

Why merchants keep failing to protect card data

Fines. Bad publicity. Class actions. Are any of these penalties severe enough to stop data breaches?

SourceMedia™

Smart Retail Solutions

Introducing PAX's new Smart Retail Solutions. Sleek designs that make them look more like a tablet than a payment terminal.

PAXSTORE

PAX has launched an application management platform for resellers and partners to manage applications with the PAX Smart Retail Solutions.

US Headquarters:

4901 Belfort Road, Suite 130
Jacksonville, FL 32256
+1-877-859-0099 | sales@pax.us

Regional Office:

40 West Baseline Road, Suite 210
Tempe, AZ 85283
+1-877-859-0099 | sales@pax.us

Contents

ISO&AGENT

ISOANDAGENT.COM

1 STATE STREET PLAZA, 27TH FLOOR
NEW YORK, NY 10004 • (212) 803-8200

EDITOR
Daniel Wolfe
212-803-8397
daniel.wolfe@sourcemedia.com

CONTRIBUTING EDITOR
David Heun

ART DIRECTOR
Robin Henriquez

GROUP EDITORIAL DIRECTOR, BANKING
Richard Melville
richard.melville@sourcemedia.com

VP, RESEARCH
Dana Jackson

NATIONAL SALES MANAGER, ADVERTISING
Megan Downey
212-803-6092
megan.downey@sourcemedia.com

VP, CONTENT OPERATIONS AND CREATIVE SERVICES
Paul Vogel

DIRECTOR OF CREATIVE OPERATIONS
Michael Chu

DIRECTOR OF CONTENT OPERATIONS
Theresa Hambel

MARKETING MANAGER
Deborah Vanderlinder

FULFILLMENT MANAGER
Christopher Onyekaba

CUSTOMER SERVICE
212-803-8500
help@sourcemedia.com

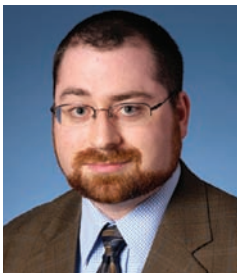
SourceMedia™

CHIEF EXECUTIVE OFFICER ..... Gemma Postlethwaite
CHIEF FINANCIAL OFFICER ..... Robert Dennen
EVP & CHIEF CONTENT OFFICER ..... David Longobardi
CHIEF MARKETING OFFICER ..... Matthew Yorke
CHIEF SUBSCRIPTION OFFICER ..... Allison Adams
SVP, CONFERENCES & EVENTS ..... John DelMauro
SVP, HUMAN RESOURCES ..... Ying Wong

Editor's View

Do retailers strive for security?

Data security is as important to merchants as ever, but a growing number of breaches keep making headlines.



It's fair to question whether merchants care enough about security, or whether they have the right tools in place, or if they are not compliant with the expectations of the payment card industry. But sooner or later, that blame has to get shared with the issuers and processors that put merchants on the front lines of protecting their own card data.

If a merchant is breached, it suffers bad publicity, fines, legal settlements and other consequences. But none of these are enough to put the company out of business. A few executives may lose their jobs, but no one seriously expected the likes of Home Depot, Target and others to go out of business after being breached.

And perhaps that's the right outcome — these companies are victims, after all — but they may not have the right incentives in place. We all have locks on our doors, but do we all need a security alarm as well? Many merchants may not think so until it's too late — they see themselves as low-risk because they have smaller ticket prices or don't sell luxury goods. But the card data they handle is every bit as valuable as the card data handled by the giants of retail.

The merchant acquiring industry can address this problem by educating merchants and providing the appropriate tools and resources to better protect payment card data. If the penalties aren't harsh enough to scare merchants into doing more, there must be other ways to improve their approach to security.

—Daniel Wolfe

Elizabeth Rossiello, founder of Nairobi-based BitPesa

An African startup builds on bitcoin

Bitpesa's founder saw bitcoin as the next big thing, and stuck with her plan as crypto's power crumbled

By Kate Fitzgerald

When jobs in banking dried up after the global economic crash in 2008, Elizabeth Rossiello went to work in Africa at several microfinance operations, where she saw firsthand how Kenya's recently launched M-Pesa mobile money service was transforming payments.

Then, Rossiello heard that cryptocurrencies would be the next big thing. In 2013 she founded BitPesa, a digital foreign exchange and payments platform based in Nairobi.

And while she benefited from the initial craze around bitcoin and blockchain, her company also shares bitcoin's reputational wounds as the cryptocurrency faces more regulatory backlash and pricing volatility.

"It can be frustrating, because this technology is new and the media is riding the waves of excitement and collapsing optimism based on its price, while every day we're over here demonstrating industrial use cases for bitcoin and blockchain," Rossiello said.

Nevertheless, growth has been solid—last month BitPesa expanded operations to Ghana, its ninth country—and it recently bought the Spanish online money service TransferZero.

BitPesa's niche sets it apart from pure bitcoin operations, by offering a range of options for cross-border payments, accepting bank transfers and funds from licensed money transfer operators, in addition to bitcoin. Its platform blends mobile money, blockchain technology and bitcoin acceptance for cross-border business-to-business transactions.

In certain cases, bitcoin offers an elegant solution for businesses in Africa making purchases from foreign suppliers in their own currency with its blockchain approach cutting out several intermediaries, Rossiello explained.

One example she gave is an African company that wants to import Japanese car parts from a vendor that wants to get paid in yen.

"Typically you'd need a foreign counterparty to assist in that kind of transaction, but BitPesa lets businesses use bitcoin or another currency to buy those supplies and avoid going through a foreign cash window," Rossiello said. "Customers can now do large transactions during African trading hours, where previously they had to operate on the schedule of brokers in other countries, which also don't recognize African holidays."

BitPesa's cloud-based API enables seamless integration with partners, and with a U.K.- authorized payment institution license since 2015, the company has the flexibility to take funds from licensed money transfer operators in bitcoin or hard currencies and pay out through a network of local companies and banks in African currencies, to either bank accounts or mobile money accounts, Rossiello said.

Typical B-to-B payments for BitPesa's customers include payroll and treasury payments and supplier payments and reimbursements. **ISO**

Do B2B payments need their own Venmo?

Bill.com sees its future in taking the lessons of successful P2P apps and applying them to business payments

By John Adams

Bill.com has implemented a strategy to make B2B payments more like Zelle or Venmo, removing the same pain points that those P2P apps do for consumer payments.

The company is targeting the manual entry of account numbers and other details that often deter organizations from digitizing their payments. The company likens the problem to the early days of P2P transfers, which still required users to know the recipient's bank account number.

"The banks said just type in the account and routing number and we'll take care of the rest," Sanjeev Kriplani, senior vice president of marketing and product management for Bill.com. "People didn't want to type that in. So today the banks ask for an email or a mobile number, something everybody knows, so P2P has taken off."

Since it designed a consumer-bank style experience for business payments, half of Bill.com's business payments are now electronic, up from 44% last year. By most estimates, nearly 80% of businesses overall still rely at least partly on paper checks across the entire market.

Essentially, the company built a cleaner interface for ACH payments, Kriplani said.

"We view ACH in the context of the small business world as not fully developed," Kriplani said. "But it's for reasons that are different than most of the industry believes."

The reasons often given for business' tepid embrace of innovations such as online payments or or digital transfers are businesses want to maintain older cash management models, or simple inertia—the businesses are accustomed to using paper checks and are uncomfortable with change.

Requiring businesses to navigate to different systems, or enter full registrations or logins to digitize payments is also a problem that hinders business payment automation, according to Kriplani.

Bill.com was not immune to these issues. About eight months ago, Bill.com partnered withIntuit to allow users to pay vendors and other suppliers without logging out of their accounting program. Prior to that integration, users had to sign up for Bill.com through its website or through another accounting software program, and then synchronize with Intuit for bill payments.

While integrating with Intuit, Bill.com is also building a network of small businesses that can pay each other by typing in a name or address instead of more "financial" information such as an account or routing number, similar to a P2P app—Bill.com provides a secure wrapper around the payments information that powers the transaction. Bill.com has about 3 million users in its network.

The company's next step is to build in faster processing to enabler payments that are close to real-time. **ISO**

Payments Just Got Easier

Merchants are the heart of your business, making their lives easier helps you grow. Paya's payment solutions work in-store, online, or on-the-go. Our secure, reliable platform delivers the business intelligence your merchants need to thrive in a changing marketplace. Partner with Paya today.

Partner Today

www.paya.com

U.K. fintechs try to offset Brexit disaster

Fintech companies decide whether to flee the U.K. or to 'Brexit-proof' their operations

By Kate Fitzgerald

U.K. fintech companies' fears of Brexit triggering an immediate cutoff from Europe were eased somewhat by the European Union's recent proposal of a 21-month transition period beginning next year, but most operations are crafting survival strategies for worst-case scenarios.

So far, fintech companies' options range from relocating to other countries to finding ways to offset negative effects by attempting to "Brexit-proof" their businesses. The latter option can still be a substantial undertaking.

Cardstream, a provider of white-label payment software and services located 150 miles from London, is trying this.

The company has restructured its payments systems so users outside the U.K. may easily access its platform in other geographies and manage data compliance and tax jurisdiction details remotely if needed, said CEO Adam Sharpe.

"The moment the referendum result was announced in June 2016, we started working on plans to ensure we'd be ready for every eventuality," Sharpe said.

It took Cardstream less than two years to reshape its systems, so that processing for European payments, customer data and taxation now may be managed outside the EU while Cardstream remains in the U.K. town of Taunton, Sharpe said.

Other companies are developing similar strategies to work around the potential effects of a "hard" exit from the EU, which they fear could abruptly alter the current EU regulations and licenses enabling U.K. fintech companies to seamlessly serve European customers.

A potential nightmare for U.K. financial services companies would be the elimination of the traditional passporting rights U.K. companies rely on to do business across Europe, according to David Parker, CEO of U.K.-based Polymath Consulting.

More than 5,000 U.K. financial firms currently use passporting rights in the EU, and more than 8,000 European financial firms in turn rely on passporting to service U.K. customers, according to reports.

"Imagine the paperwork and effect on businesses if all of these firms need to either set up or find new partners to (continue to) work in the other markets," Parker said.

Because government agencies are still negotiating terms on many aspects of the U.K.'s separation from the EU, experts say it's too early to know exactly which processes may change, so many companies are making moves to protect their operations.

While the EU and U.K. governments appear to be working toward a transition period ending about two years from now—which is better than an immediate implementation—that's still a very tight timeline, according to Parker. **ISO**

WHY MERCHANTS KEEP FAILING TO PROTECT CARD DATA

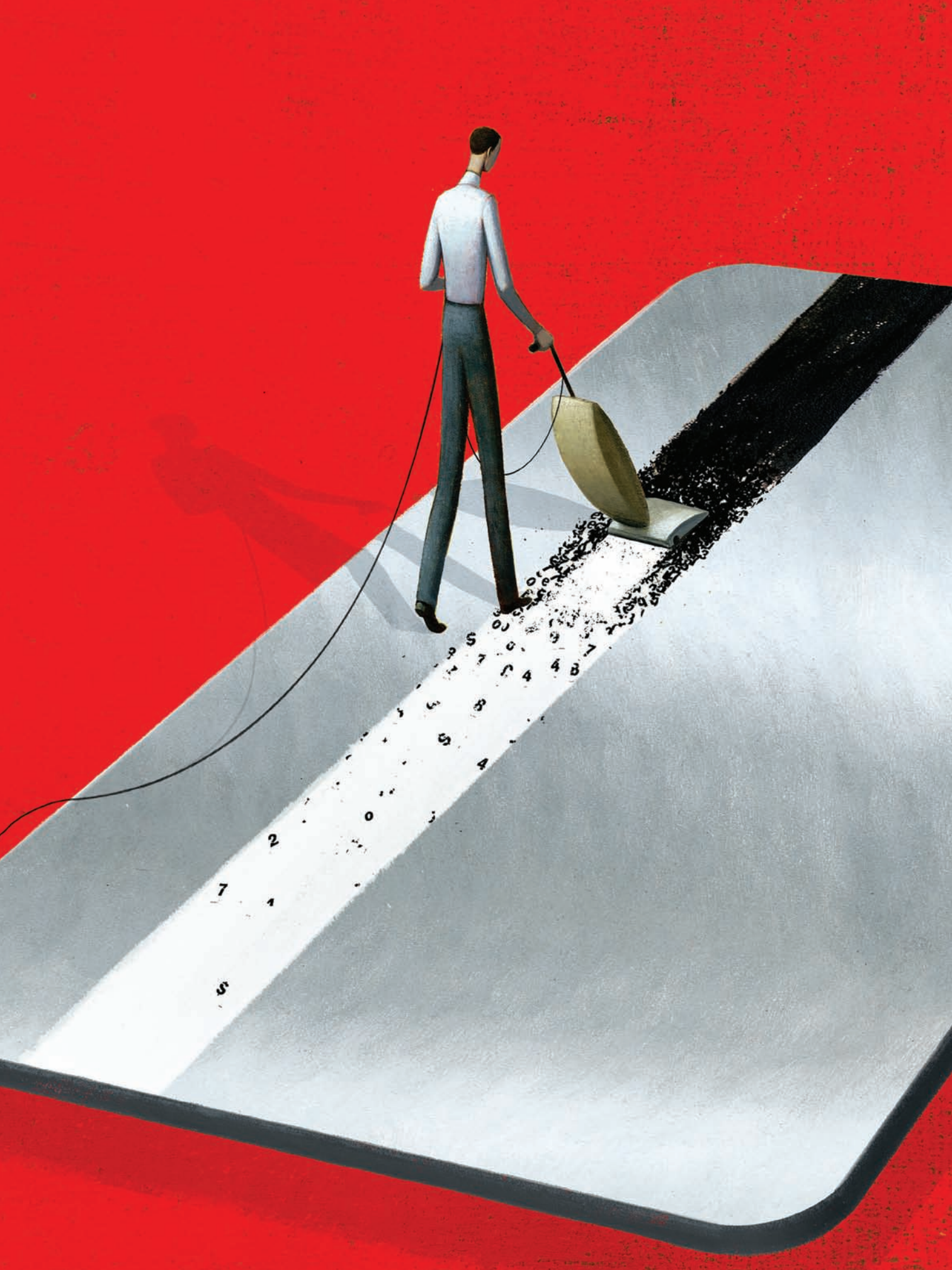
Fines.
Bad publicity.
Class actions.
Are any of these penalties severe enough to stop data breaches?

Merchants would seem to have the most sophisticated tools ever to protect card data — tokenization, biometrics, machine learning, even EMV — but they still leave the door open to fraud at an alarming rate.

Are the incentives for protecting card data so lopsided that merchants feel little need to do more? Or is it wrong to ask merchants to fix the faults in a payment card ecosystem they had little hand in creating?

Every time a major breach happens — including major incidents at Target, Home Depot and TJ Maxx — the immediate reaction is always to declare them as cautionary tales of the kind of negative publicity that no company wants to attract. But these companies never go out of business or get blacklisted from the major card networks (even if a

By Kate Fitzgerald
Illustration by Jon Krause



few executives are sacrificed in the aftermath). Maybe they pay fines, but never enough to threaten their livelihood.

Recently, the big breaches came from Saks, Lord & Taylor and Panera Bread. Details are scant about what caused the exposure of at least 5 million consumers' card information at retailers Saks and Lord & Taylor; their parent company, Hudson's Bay Co., hinted that the breach originated at store cash registers, because online and digital platforms weren't affected.

Separately, Panera Bread exposed millions of customers' records including names, emails, addresses, birthdays and the last four digits of their Social Security numbers, according to security expert Brian Krebs. Panera on Monday told Fox News the issue has been resolved and fewer than 10,000 customers were affected, and Krebs took to Twitter to challenge the sincerity of this statement.

Even as merchants get raked over the coals for every new incident, there is little chance that they can solve the problem any time soon, said Shirley Inscoe, a senior analyst with Aite Group.

"The data criminals obtain is so valuable and criminal rings can sell it on the dark web for many kinds of fraud—payment fraud, account takeover fraud, application fraud, the list goes on and on. All a hacker needs is one gap in security that he can exploit, and as hard as companies try, it is difficult to shore up every potential gap," Inscoe said.

Merchants are also frustrated by the piling on of requirements from the payment card industry, as well as the industry's habit of blaming the victim any time a merchant suffers a breach despite having been told they were doing everything right. This is a problem that stretches back nearly a decade; when the Princeton, N.J., pro-

A look at data breach penalties: Are they too lax?

As the names pile up — Equifax, Target, Home Depot, TJ Maxx, etc. — there's one thing all of these brands have in common. They all disclosed a major data security breach, and they all remain in business despite what happened.

In theory, rules such as the Payment Card Industry data security standard as well as national regulations should have a more adverse effect on these companies. At most, they pay a fine they can more than afford, and remove a few executives to appease bloodthirsty shareholders, but they are not even temporarily barred from accepting the very payment card data they failed to protect.

Consumers, despite their ire, are still willing to work with all of these brands — including Equifax, a company they arguably had no choice to work with in the first place. According toAuriemma Consulting Group, although there is increased consumer skepticism of credit bureaus in the wake of the Equifax breach, 82% of cardholders believe their financial accounts are secure and about 80% reporting confidence in their bank's and/or credit card issuer's ability to protect their financial information.

The short-lived outrage over the Equifax breach may be a symptom of rapid-fire news cycles.

While Equifax sucked all the air out of the room last year, it is worth noting that according to the Identity Theft Research Center, there were 1,578 other data breaches in 2017, exposing a total of 178.9 million data records. This builds on the 1,079 data breaches in 2016 and 780 in 2015. It is therefore of little surprise that consumers are no longer shocked by their data being made public given that there were an average of 4.3 data breaches per day last year. (Equifax did not respond to a request for comment for this story.)

The high level of consumer apathy may be something of a disincentive for organizations to properly invest in cybersecurity, but another aspect is that the cost of a breach really isn't that much for large companies.

Much of this comes down to cost-benefit analysis. For example, the net expenses related to the Home Depot data breach of 2014 were $28 million, which ultimately represents less than 0.01% of Home Depot's sales for that year. Similarly, Target incurred $105 million in cyber breach-related expenses, but this amount was only 0.1% of their 2014 sales. While the final tab for the Equifax breach is still being tallied, it's estimated to cost insurers $125 million. According to Property Claim Services (PCS). That is not to say that these events were not financially punitive, but certainly the losses incurred from these breaches were a drop in the ocean of total revenue.

Some have had more reputational breaches, such as Ashley Madison and Sony; the former exposed would-be adulterers and the latter exposed sensitive internal emails that got considerable media exposure due to the celebrity gossip content. The cost for Ashley Madison was a $11.2 million class action settlement, while direct costs from the Sony Pictures breach totaled $35 million.

To find data breaches that were actually devastating to the company that suffered the exposure, one needs to go back over a decade.

The CardSystems data breach of June 2005 was — by today's standards — a fairly vanilla example of a data breach, with 40 million cards exposed. But the penalty was much bigger: In the wake of this incident, both Visa and American Express dropped CardSystems as a credit card processing company and a federal investigation launched. In a tailspin, CardSystems was acquired by the biometric payments company PayByTouch later that year. PayByTouch, in turn, went out of business in 2008.

cessor Heartland Payment Systems disclosed a breach in 2009, it did so after repeatedly passing audits for the Payment Card Industry Data Security Standard.

"The audits that are used to determine compliance are very much overvalued, and we overvalued our audits," Robert O. Carr, Heartland's chairman and chief executive at the time, said in an interview shortly after disclosing the breach.

It's much the same with the EMV chip card migration. Despite a shift in fraud liability that took effect in late 2015, just over 50% of U.S. merchants have adopted the technology, according to Mastercard. This figure was part of the justification for eliminating the requirement for signature authentication this month.

It also indicates that nearly half of merchants see EMV as unnecessary to have right now. Perhaps it's because they feel their own anti-fraud systems are sufficient, or because they are willing to accept a less secure environment. Or the merchant wanted to comply but the payments industry wasn't able to move fast enough.

A sense is growing among data-security firms that the threat to merchant card data is too broad and ubiquitous to pin all the blame on merchants.

"Credit card breaches involved a more complex equation than just lazy merchants or sneaky criminals … even well-prepared merchants can become victims," said Tim Erlin, vice president of product management and strategy at Tripwire, a Portland, Ore.-based cybersecurity firm.

While there's no doubt some merchants fail to implement appropriate controls or do the bare minimum to be compliant with payment card industry security standards and recommendations, that's not the whole story, according to Erlin.

> @briankrebs **Hey Panera, despite your statements to the contrary, you still haven't fixed this customer info leak. Would you like to revisit the 10k number you just gave to Fox news?**

"Over the years we've seen myriad attacks that were simply opportunistic or were well-planned, sophisticated assaults," he said, underscoring the limitations of most merchants' capabilities to protect card data in the face of ongoing, aggressive criminals who continue to find a market for stolen card credentials.

Threats to data are intensifying faster than merchants can adapt to them, especially as retail environments morph to omnichannel delivery approaches, which can increase risks, said Terry Ray, chief technology officer at Imperva, a cybersecurity firm based in Redwood Shores, Calif.

Another problem is the lack of critical expertise in battling data security, he said. Ray's research suggests there's a dearth of experts globally in "data security" compared with "network security," highlighting the fact that many organizations lack resources to adequately battle the growing problem of card data security.

"If organizations know little about data security, then data will likely receive very little attention in any corporation's grand security strategy and the result is that we'll continue to see breach after breach, day after day," Ray said. "Frankly, most organizations can't tell you where all of their sensitive data is, who touches it, when they touch it, or whether they should be touching it. This is a problem." **ISO**

Cryptocurrency

A crypto card looks past its limitations

The idea of a cryptocurrency debit card has been tried before, but MoxyOne has a fresh take

By John Adams

Tanshul Kumar insists the problem of merchants not accepting cryptocurrency for payments carries its own solution: Customers convert their cryptocurrencies right before the money hits the merchant's account.

In yet another twist on the idea of a cryptocurrency debit card, MoxyOne has developed its own network as a way to address the setbacks some have faced in relying on Visa and Mastercard. Merchants would still have to sign up with MoxyOne, but they would never see or touch anything but their local fiat currency.

Issuing its own debit card and using liquidity providers could give MoxyOne more control over its network, and possibly avoid pressure from card networks and other problems cryptocurrencies have had when trying to use debit cards to convert bitcoin to fiat currency at the point of sale by circumventing traditional financial companies.

The card networks have taken a cool posture toward using debit cards for cryptocurrency payments at the point of sale.

The list of crypto debit cards is relatively small, and even the cards that do exist are not universally accepted.

Visa recently banned some Wavecrest cards from using Visa debit cards in this manner, though Visa said the ban was due to noncompliance with card network rules, rather than being related to cryptocurrency debit as a payments model.

Three of Wavecrest's prepaid cryptocurrency payment providers — BitPay, Cryptopay and Bitwala — were suspended, meaning they could not be used for payments, putting a damper on an already slow cryptocurrency payment market.

In some cases, banks in the U.S. and U.K. have banned the use of credit cards to buy cryptocurrency, which isn't the same issue as barring the conversion of cryptocurrencies onto debit cards, but still has the effect of depressing the amount of cryptocurrency in the open market that's usable for retail payments.

MoxyOne's model relies on "just in time funding," or a method of automatically transferring funds at the time of a payment, thus avoiding a preloaded individual accounts and acting as an alternative to the traditional financial services market, which has at times taken a hard stance against cryptocurrencies which has delayed the development of a payments market.

"All the merchant sees is a successful or unsuccessful transaction," said Kumar, co-founder and lead front-end developer for MoxyOne, an Australian company that has developed a middleware between cryptocurrencies and the fiat currencies that merchants are more accustomed to using. "The merchant doesn't have to deal with any cryptocurrency or anything like that whatsoever." **ISO**

Gig innovator Grab pulls ahead of Uber

Uber has a well-deserved reputation for payments innovation, but Grab has been far more ambitious

By John Adams

Companies that aspire to be the Uber of their industry should take a second look at the ride-sharing market, where Grab has become a lightning rod of payments investment and innovation.

The Singapore-based ride-sharing company is attracting some of the world's most well-heeled fintech technology investors, including a reportedly hefty investment from Alibaba. Grab was valued at $6 billion as of late 2017, double its $3 billion valuation from 2016.

Though this is far behind Uber's valuation of $72 billion, Grab is ahead of rival Uber in building out horizontal payments and financial services off of its core ride-sharing business. In the past year, Grab has become a portal into the broader economy for contractors, part-time workers, freelancers and other members of the gig economy.

"I don't think that a processor needs necessarily to have a 'ride share' offering to be viable, but I do think that a 'gig economy' or marketplace capability is getting really close to a core requirement for online payment processing," said Thad Peterson, a senior analyst with Aite Group.

Late in 2017, Grab launched a mobile wallet app, turning its ride-sharing base into a potential merchant acquiring powerhouse.

GrabPay has already made inroads among Singapore's restaurants, shops and marketplaces as it plots expansion to other markets.

In January, Grab acquired iKaaz, an Indian mobile payments platform that supports NFC, QR codes and other forms of contactless and online payments.

iKaaz allows Grab to pair ride-sharing with P2P, bill payment, in-app mobile and retail payments.

The iKaaz team will join Grab's research and development center in Bangalore; financial terms of the deal were not disclosed.

Another noteworthy deal was Grab's 2017 acquisition of Kudo, giving it a cash payment option in Indonesia. The deal gives Grab a way to serve the underbanked as part of its overall $700 million "Grab for Indonesia" 2020 master plan. The company seeks to bring financial inclusion to the forefront through its various mobile payment offerings.

Uber is, of course, no slouch — it recently launched a debit rewards card for drivers, a fleet card for Uber Freight clients, and a consumer credit card that can be obtained and managed within the Uber app.

Uber also applied for an e-money license in the Netherlands in recent weeks.

These efforts still fall short of Grab's ambitions with projects like Grab Financial, which supplies lending and insurance via partnerships with Credit Saison, a Japanese consumer finance company; and Chubb, a property and casualty insurance company. Grab is also attempting to get regulators to

approve its acquisition of Uber's Southeast Asian business.

Grab's app is used 5 million times daily in Southeast Asia and has been downloaded 90 million times.

Alibaba and Grab did not return requests for comment, but TechCrunch reports Alibaba is in the early stages of an investment following initial talks last summer. Alibaba would joinSoftbank as major Asian companies to invest in Grab.

Alibaba also made a major investment in Ele.me, a Chinese food-ordering company that has also doubled in value in the past year. By investing in Grab, Alibaba would gain exposure and potential partnership and integration with a company that's expanding in all of the areas financial institutions and e-commerce companies want to see expansion.

With these investments, Alibaba is moving deeper into the sharing economy as it keeps pace with rival Tencent, which works with China's other large food delivery apps and in 2017 made an investment in Go-Jek, one of Grab's rivals in Asia.

Many of Ele.me's clients are smaller restaurants, or even private kitchens that take advantage of China's soft restaurant regulations to use the Ele.me app to become their own restaurants. Like its rival Uber, Grab is a gig economy powerhouse since it almost entirely relies on contractors and provides and on-demand service for consumers that can be easily paired with other revenue-generating activities.

"The big [Asian] payment players have been tying in or partnering with practically everyone to establish horizontal leverage, which means that merchants and on-demand services such as ride-hailing are prime candidates to be part of the major apps' ecosystem," said Raymond Pucci, associate director of research and consulting services for Mercator Advisory Group. "Most Asian nations find consumers doing anything and everything with their phones, especially financial and commerce-based transactions."

While China's e-commerce companies have jumped ahead of U.S. companies in providing emerging mobile technology for merchants, many companies outside of China are adding technology that accommodates payments and other services for gig workers.

Intuit earlier this year improved its payments technology for gig workers. First Data is using its acquisition of Acculynk's PaySecure to support real-time gig economy payments, and Wirecard earlier this year collaborated with Moonrise to power faster payments to part-time and other freelance workers. And PayPal sees contractor payments as a way to offset losses from eBay's decision to shift its processing business to Adyen.

"Providing support for a more broadly defined gig economy is a possible path, with ride sharing being one example of that. Alibaba and Tencent have an insatiable need for broader functionality as their core value to consumers is in the value that they provide through their Alipay and WeChat Pay apps," Peterson said. "They are also throwing off a great deal of cash through their properties, so it makes sense that they would be moving more broadly into new categories and markets." **ISO**

A London processor targets the U.S.

Checkout.com wants to expand by keeping its offerings narrowly targeted

By John Admas

Checkout.com has used alternative fees and a high-touch approach to build a market for its online payments toolkit in Europe. Now it's come to the U.S., where the likes of Stripe and Braintree already own a sizable chunk of the market.

The London-based company says the retail industry relies too much on APIs for a one-size-fits-all approach to technology and pricing. Checkout.com is attempting to outflank that by relying on its private ownership model, which he said precludes heavy pressure to build a huge base of consumers. By focusing on expanding midtier businesses, Checkout.com hopes to build relationships that encourage customized cross-selling as an alternative to themultibillion-dollar firms such as Stripe and Braintree.

"It's not a numbers game; we want to understand the businesses," said Peter Caparso, Checkout.com's president of North American operations. "We don't have a bank or a PE firm telling us, 'This is what you need to do. You need to hit a certain goal.' If a merchant wants to have a certain function created, we pick up the phone."

Checkout.com has about 300 employees and 100 developers. Its 700 clients include Samsung, TransferWise, Hopper, Virgin and Adidas. The company recently opened offices in Boston and San Francisco, where it will tackle an e-commerce enablement market that includes huge established brands.

Checkout.com's niche includes small businesses that have gained some traction, creating a sudden burden of merchant service and payment needs to accommodate the merchant's more aggressive growth plan.

"We get to the business right as they take off, at a crucial inflection point for the merchant, when it wants to expand into a new territory or offer new payment methods," Caparso said.

Its online payments tools cover most international credit cards, pass-through wallets such as Apple Pay, stored value wallets such as PayPal and Alipay; and alternative payment options such as Klarna, Nets, Boleto and iDeal.

Checkout.com is also using a fee structure that's different from most APIs for payments, which usually charge 2.9% plus 30 cents per transaction, or something close to that. Checkout.com is charging "interchange++ (a formula of processing and card payment costs designed to spot the "best" rate), which standardizes commissions that card issuers collect, Caparso said. The amount varies by card type, bank, merchant location and other issues, making it more customized to the specific merchant.

Alternatives to the standard 2.9% plus 30 cents have been tried before, including by mobile payment and marketing company LevelUp, which has changed its fee policies several times over the years. Caparso said combining Checkout.com's lack of a long-term contract and no setup or maintenance fees creates a sense of cost transparency that's attractive to merchants. **ISO**

Why Verifone needs to be taken private

Verifone has worked hard to turn itself around, but the market it serves has also come a long way

By John Adams

The $3.4 billion deal to take Verifone private is more than just an effort to strengthen the company by placing it alongside the many other payments-related technology holdings owned by Francisco Partners. It's also a signal of how much the market has changed from the days when Verifone found itself scrambling to combat a newcomer called Square.

Verifone's attractiveness to Francisco is partly a testament to CEO Paul Galant's turnaround.Galant became CEO of Verifone in 2013, taking over a company that was struggling financially and technologically, suffering from what Galant called "self-inflicted wounds" such as missed deadlines, poor customer service and even prohibited business dealings in Iran.

The mobile point of sale market grew by preying on these weaknesses. Square's pitch was less about technology and more about ease of access — small merchants that didn't want to contend with Verifone's customer service issues could instead pick up a card reader at any convenience store for just $10. Verifone tried to match this with products like PayWare Mobile and Sail, but neither device reclaimed much ground against Square.

Verifone's turnaround was gradual, but in the past two years it has sharpened its move from payment terminal-based company to a software provider. The strategy is showing some effect, despite headwinds from the EMV migration, as CEO Paul Galant noted in the company's most recent earnings report on March 8. In addition to reporting solid earnings, Galant noted progress in expanding Verifone's multichannel and digital capabilities.

The deal with Francisco Partners will make Verifone a privately held company, and will also allow it to accelerate its strategy in a dynamic merchant acquiring industry that looks much different than it did as recently as five years ago, with billions of dollars in acquisitions and investments birthing a tech revolution. The deal includes Verifone's debt, and is expected to close in the third quarter. Verifone's board has approved the deal, which includes a "go shop" period through May 24, meaning it's possible another company could come in with a better offer.

Verifone's traditional rival, Ingenico, has also bulked up through the M&A market, acquiring the Swedish digital payment company Bambora in 2017 in a $1.7 billion deal to accelerate Ingenico's diversification beyond terminals. Ingenico later bought Paymark to add clients in New Zealand and Airlink to expand in Asia.

But Ingenico and Square are only two examples of the substantial pressure Verifone faces.Stripe's API has swept the market for digital payments, giving merchants a low-touch alternative to both Verifone and Ingenico. Stripe's valuation of more than $9 billion looms over traditional acquiring like a hammer.

And Stripe's not alone. PayPal's Braintree has expanded rapidly over the past three years by tying PayPal's digital transfers to Braintree's open development tools.

Verifone and Francisco did not return requests for comment on Monday night.

For Verifone's part, it's kept up by pushing the adoption of Verifone Connect, its new cloud-based omnichannel digital services platform, connecting its 30-million-device footprint through Verifone's gateway and expanding use of its Carbon digital payments system.

By coming under Francisco's investment umbrella, Verifone will have plenty of potential partners, some of which Verifone is already working with.

These companies cover multi-channel support for EMV, mobile payments, omnichannel shopping, quick service payments systems, gateway, ISO sales and authentication/security. Verifone has been building out its business in all of these areas, so gaining a roster of easy-to-integrate collaborators will place Verifone and Francisco's other holdings in front of merchants in dozens of countries, in nearly every category and almost all sizes.

The San Francisco-based Francisco Partners formed in 1999, has raised more than $14 billion in capital and has invested in more than 200 technology companies. Other investors in the Verifone deal include British Columbia Investment Management Corp., a Canadian institutional investor.

Francisco has invested in many health care companies, and it has several fintech companies in its portfolio of current investments. These companies include 2Checkout, a global online and mobile payment technology company that's now a unit of Avangate, providing access to cross-border e-commerce, an increasingly popular option for online merchants that sell in multiple countries with a single location.

Francisco's holdings also include Paysafe, a Houston-based company that provides connections for mobile wallet, online payments and other digitally focused merchant services. Paysafe is already collaborating with Verifone to sell Verifone's Carbon and Engage terminals through Verifone Connect, powering business, marketing and loyalty programs.

Another Francisco holding, NMI, develops technology that supports ISOs, independent software vendors and payment facilitators to offer branded payment gateway services on a white label basis. NMI just purchased Creditcall to add single-platform support for retail, e-commerce, mobile and unattended payments.

Other collaborations with Francisco portfolio companies could come from Dynamo, a CRM and reporting company; and OneIdentity,an authentication company. Prosper, a P2P lending company founded by Chris Larsen, who later went on to head Ripple, is also in Francisco's current stable.

Each of these companies touch on some or all of Verifone's diversification needs.

Verifone is still grappling with the U.S. EMV migration, which also influences merchant and ISO adoption of contactless payments. The company is partnering with banks to extend mobile payment acceptance in Europe, and is expanding its embrace of open development. **ISO**

Payment cards

Why merchants won't care about the sig rule

Is the death of signature authentication upon us? Merchants may not be moving so fast to eliminate it

By Kate Fitzgerald

The card networks recently admitted what consumers have long suspected—card signatures have become worthless for authentication at the point of sale. But that's not the end of this story.

Even though the card networks will stopped requiring signatures on purchases, merchants are unlikely to make immediate changes in their routines.

For some, no change will be necessary — the majority of lower-value store transactions already get automatic card network authorization without a signature, as the networks had gradually relaxed the signature requirement over the years. For others, it's easier to keep collecting signatures than to overhaul the technology that prompts for them.

Why merchants drag their heels

Merchants can't simply instruct cashiers to stop asking for signatures. They must also reconfigure the software and card-prompting commands for payment terminals, a process that takes time and money — two things many merchants lack, particularly when it comes to card acceptance.

"It may be several months or quarters before we see any tangible changes at the point of sale from the elimination of merchants' requirement to collect a signature at the checkout," said Jason Bohrer, senior vice president and general manager of secure card solutions at CPI Card Group.

Bohrer points to the fact that 30% to 40% of U.S. merchant payment terminals are still using the older, less secure magnetic stripe technology to process cards at the point of sale, despite an October 2015 liability shift putting the burden of counterfeit card fraud on the party that hasn't upgraded to EMV-chip card technology.

"You can expect to see a similar pace of change with the no-signature shift," Bohrer said.

But other merchants are still exhausted by the last few years of upgrade investments, alongside the shocks of a steady stream of card data breaches. By comparison, they have little interest in the elimination of signature for a dwindling number of their sales.

"The no-signature rule for smaller transactions has been in place for a long time, but plenty of merchants still ask for a signature for a $5 purchase, which shows you how unlikely merchants are to react just because the rules are changing April 15, and consumers aren't likely to care either way," said Rodman Reef, an analyst with Reef Karson Consulting.

Of course, larger merchants have the resources to implement the change — even if they don't have an immediate timeline.

Walmart said a majority of its sales already flow through the checkout with no signature required, but higher-value transactions still require a signature. The retailer plans to reconfigure its systems to bypass signatures altogeth-

Advertising Index

er but no date has been set yet, said spokesman Randy Hargrove.

Shoppers never know what to expect at the checkout, anyway. "Consumers don't understand why one merchant requires a signature for a $10 purchase while another does not, and I predict this change will be viewed as more of the same," said Shirley Inscoe, an analyst at Aite Group.

Didn't merchants want this?

The irony is that merchants for years have been asking the card networks to clarify their stance on signatures and the role they played in assigning liability in case of lost or stolen cards.

"Merchants have been pressing the brands to remove signature capture from rules or else provide more transparency about how issuers were using signature as a fraud tool," said Randy Vanderhoof, executive director of the Secure Technology Allliance, a cross-industry organization.

Not only do signatures take up time and resources at the POS and give issuers another reason to shift fraud to merchants, but they also give consumers a false sense of security, said Mark Horwedel, CEO of the Merchant Advisory Group.

Horwedel's group unsuccessfully advocated for the U.S. to adopt the more-secure chip-and-PIN approach used in most major markets outside the U.S. when EMV was introduced.

But the networks decided not to mandate chip-and-PIN, claiming modern online authorization methods made PINs superfluous for blocking counterfeit card fraud—the biggest category—even in Europe.

Meanwhile, PIN use has dramatically declined worldwide in recent years as contactless and mobile payments took hold. In the U.K. and Australia, the majority of transactions under $100 are contactless—requiring no PIN—and card security experts agree PINs aren't necessary except for larger transactions.

"Chip and signature is effectively as good as chip alone," said Al Pascual, senior vice president of research and head of fraud and security at Javelin Strategy & Research, noting that EMV chip technology makes counterfeiting plastic cards nearly impossible.

The Merchant Advisory Group and individual U.S. merchants continue to insist on the value of PINs for in-store transactions—a method that effectively blocks losses from stolen or counterfeit cards—but support for PINs is collapsing globally, according to Pascual.

"We're unlikely to see a proliferation of chip-and-PIN here and in fact we're likely to see a loosening of the limits for PIN transactions as has occurred in other markets like Australia," Pascual said.

What's replacing PINs is a combination of mobile location methods, plus biometrics and real-time behavioral analysis from the card networks and banks, according to Pascual.

Are contactless cards inbound?

While eliminating the signature requirement carries little risk for the card networks or banks, there's a significant upside in further streamlining the checkout process, card industry experts say.

"Getting rid of the signature requirement takes card payments a step closer to the contactless experience, which U.S. issuers are very interested in," CPI Card Group's Bohrer said, noting that the rapid growth of contactless card volume in the U.K. and Australia makes a compelling case for banks evaluating whether to stick with contact-only or add contactless cards to the mix.

Though only about a third of U.S. merchants' terminals are NFC-enabled, several midsize U.S. card issuers have asked CPI Card Group about the cost of shifting all or part of their portfolios to contactless cards within the next couple of years, Bohrer said.

"We're getting lots of questions and we expect to see more active pilots for contactless cards taking place starting next year," he said. **ISO**

Accelerate
your career with Harbortouch

The most successful **POS** program in the payments industry

- ☑ Best-in-class Elite POS & Tablet-Killer Echo POS
- ☑ Solutions for Bar & Restaurant, Retail, Salon & Spa, Delivery
- ☑ POS delivers a more stable and profitable portfolio

$25,000
Signing Bonus

12x/$400
Terminal Bonuses
up to $5000

Free Leads
Receive warm leads every month from our digital marketing and telesales initiatives

Free VX 520 Terminals

Reward Point Program
Earn points for every deal that can be redeemed for exciting prizes

VIP Program
Obtain higher quality merchants with special incentives and VIP support

$100+ billion processed annually | 1+ billion transactions annually

Now offering PCI-validated P2PE, tokenization, EMV and offline EMV processing

For more information, contact:
Brian Fitzgerald, National Sales Manager Central - 800-201-0461 x 1257 or bfitzgerald@harbortouch.com
Rich Lopez, National Sales Manager East - 800-201-0461 x 1205 or rlopez@harbortouch.com
Max Sinovoi, National Sales Manager West - 800-201-0461 x 1219 or msinovoi@harbortouch.com
or visit www.isoprogram.com

HARBORTOUCH®
A SHIFT4 COMPANY

HT3173_01252018

WE'RE THE BEST!

JUST LIKE EVERYONE ELSE!

Tired of seeing the same ad over and over? So are we.

We could tell you how amazing our team is (we are!), how much our partners absolutely love us (they do!), and that we'll help your business grow (we will!), but then our ad would be like all the others... and we're definitley ***not*** like the others.

If you're tired of false promises, terrible customer service, and lack of portfolio growth then it might be time for a new approach.

Contact us and learn *how* we're different and *why* your business will benefit.

Because, you know, we're the best!

iPayment®
Different By Design

ipaymentinc.com