Welcome to the **February** edition of *ACT News – Driving Insights.* This complimentary service is provided by ACT Canada. Please feel free to forward this to your colleagues.

In This Issue

Articles

1. USE OF INTERAC E-TRANSFER SERVICE SURGES IN 2018

Source: Interac Corp. (2/19)

Canadians used the digital money transfer service more than one million times per day last year. The Interac e-Transfer service is showing no signs of slowing down, with Canadian consumers and businesses using the platform at record levels. Interac Corp. released today new record numbers for its Interac e-Transfer service, which reports more than 371 million transactions in 2018, worth a total of more than $132 billion. This represents a 54 per cent increase in volume and a 45 per cent increase in value over 2017.

“The continued adoption and significant year-over-year growth of Interac e-Transfer demonstrates Canadians’ preference for convenient digital money transfer services like Interac e-Transfer as an alternative to cash or cheque,” said Anurag Kar, Director, Digital Push Payments at Interac. “As the payment landscape evolves, we will continue to deliver solutions to suit the changing needs of consumers and businesses across Canada,” he added. Coast to coast, Canadians are embracing the Interac e-Transfer service, using it on average over one million times a day and over 35 million times each month. Whether it is to send, request or receive money, consumers continue to choose the service for everyday needs like splitting dinner tabs, paying rent, sending money to family and friends, and settling up with their babysitter, with the average user sending over three transactions per month, with an average transaction size of $357. And it’s not just consumers. Increasingly, business owners are seeking digital solutions to better manage business administration and cashflow. Interac e-Transfer provides a transformative way to simplify and streamline business payments, with the ability to request and make payments, ultimately saving small businesses time and money. Interac reports 80 per cent of Canadians using online banking are registered to use Interac e-Transfer, with over 15 million unique active users every month.

Stats at a Glance: Interac e-Transfer Usage in 2018

- November 30th was the platform’s single busiest day, with over two million transactions sent.
- Almost 76 per cent of Interac e-Transfer transactions are deposited on a mobile device.
- Over four million users are registered for Autodeposit, a feature which enables funds go directly into a recipient’s bank account without the need to answer a security question.
- Meanwhile, the Request Money feature, which allows Canadians to request money from a recipient, was used nearly one million times.

- Businesses sent over $465MM using our Interac e-Transfer Bulk Disbursement feature – allowing businesses to send bulk payments inastreamlined, secure, and cost-efficient way in a single file upload from online or mobile banking.

About the Interac e-Transfer platform

Interac e-Transfer, a digital money transfer platform, is the fastest and safest way for Canadians to transfer money directly from one bank account to another. Every day, Interac e-Transfer and Interac e-Transfer Bulk Disbursement are relied upon to send and receive money securely, conveniently and efficiently via person-to-person (P2P), person-to-business (P2B), business-to-business (B2B) and business-to-person (B2P) transactions. Users can access the platform through a participating financial institution's online or mobile banking application to send money to anyone with an email address or mobile phone number and a bank account in Canada – without requiring any personal financial information. Transferred funds remain secure with financial institutions, which settle with each other through Payments Canada's settlement systems. More than 255 financial institutions offer access to Interac e-Transfer. The Interac e-Transfer platform offers unique capabilities, such as 24/7/365 availability, real-time payment notifications, analytics, and reporting. All users are protected with multiple layers of security including encryption technology, financial institution authentication and proprietary risk management making it one of the most secure P2P solutions globally.

Interac Corp is a Member of ACT Canada; please visit https://www.interac.ca/en/

2. LAW FIRMS SELECTED TO REPRESENT USERS OWED MILLIONS FROM QUADRIGACX PLATFORM

Source: Global News (2/19)

A Nova Scotia judge has selected two law firms to represent users of the insolvent QuadrigaCX cryptocurrency exchange who are owed about $260 million. Justice Michael Wood of the Nova Scotia Supreme Court issued a decision today saying he had appointed Miller Thomson of Toronto and Halifax-based Cox & Palmer as representative counsel.

Wood says both firms have extensive experience with insolvency cases, and he noted that Miller Thomson has expertise when it comes to cryptocurrency. As well, the judge approved of their communication strategy, which includes the use of social media and online discussion groups to reach 115,000 affected users.

Both law firms have also agreed to cap their fees at this stage of the court proceedings, though the cap was not spelled out in Wood's decision. The Vancouver-based exchange was shut down Jan. 28 following the sudden death in December of its CEO and sole director, 30-year-old Gerald Cotten of Fall River, N.S. Court documents say $190 million in missing cryptocurrency is locked in offline digital wallets – but they are beyond the reach of the company because Cotten was the only person who had the encrypted pass codes.

3. CANADIAN REGULATOR FAILED TO MAKE CHECKS ON RISKY MORTGAGE BROKERS

Source: CBC (2/26)

A sign for the Financial Services Commission of Ontario (FSCO) on September 5, 2017. Documents obtained by Reuters found that the financial services regulator failed to make planned checks on mortgage brokers deemed to have 'elevated risk' of things like fraudulent mortgage applications. The financial services regulator in Canada's biggest province failed to make planned checks on mortgage brokers it had identified as risky because its resources were stretched, according to documents obtained by Reuters under freedom of information laws and information provided by the regulator.

The Financial Services Commission of Ontario (FSCO) planned to complete five on-site examinations of mortgage brokerages identified as risky this fiscal year, which ends March 31. But as of Dec. 31, 2018, nine months into the year, it had not finished any of them, according to data provided to Reuters. During the same period, FSCO staff carried out only four of 50 planned "desk reviews," which are similar to on-site examinations but less detailed. The findings call into question whether mortgage brokers, which originate 30 per cent to 40 per cent of new loans in Canada's $1.5 trillion mortgage market, are being adequately supervised as record household debt and rising interest rates make it harder for borrowers to make repayments.

Banks set to reveal earnings amid wobbly housing market, interest rate uncertainty

Mortgage underwriting standards came under scrutiny in Canada after the country's biggest non-bank lender, Home Capital Group Inc, accepted responsibility for misleading investors about problems with its procedures in 2017. The FSCO plays a particularly important role because it supervises brokerages in Toronto, Canada's biggest housing market. It is due to be replaced by a new regulatory body, the Financial Services Regulatory Authority (FSRA), in the spring of this year but it is currently unclear whether FSRA will have significantly more resources than its predecessor. In a statement, FSCO said it conducts a thorough investigation where individuals or entities are identified as presenting an elevated risk.

"This investigative process, which makes the best use of finite resources to address the most significant risks, may include, but does not require, a site visit," it said. "As a result, planned examinations may not take place, but other regulatory and supervisory activities would occur, based on the resources available."

Former mortgage agent who solicited $9M in syndicated mortgages, fined $300K by regulator

The on-site examinations involve FSCO staff visiting mortgage brokerages that initial reviews have flagged as having "elevated risk levels," warranting further investigation, according to a June 2018 government audit of FSCO's market regulation branch which Reuters obtained through a freedom of information request. They are meant to catch problems early, before they escalate, the report said. The checks can stop problems such as mortgage brokers failing to make proper checks to prevent borrowers' lying about their income in order to obtain a loan. According to credit bureau Equifax, suspected fraudulent mortgage applications have increased by 52 per cent in Canada since 2013, with Ontario seeing the majority. Other types of fraud include brokers charging unlawful fees, FSCO says on its website.

Tight budget

The audit stated FSCO was "operating in a challenging regulatory environment with limited resources to carry out its supervisory activities." Asked if FSCO's successor will have more resources, Ontario's finance ministry said FSRA is consulting with the department over its planned budget and business plan for 2019-20 and is also working on establishing a fee rule enabling it to recover some costs from the sectors it regulates, potentially enhancing its overall budget. According to its 2017-18 annual report, FSCO had 382 staff and an annual budget of C$56.5 million. Its annual budget has declined by 40 per cent since 2015-16, partly reflecting the transfer of its dispute resolution services activities to another Ontario government department.

The data from FSCO shows that the regulator completed fewer reviews in the first three quarters of this fiscal year than it did last year, when it also missed its targets. The June 2018 audit showed that, in the nine months to Dec. 31, 2017, FSCO completed one of 25 planned on-site examinations, while eight of 15 planned desk reviews went ahead. In its statement, FSCO said it eventually completed three on-site examinations and 11 desk reviews in its fiscal year to Mar. 31, 2018.

4. WHY BIG BRANDS CAN’T CREATE LOYALTY WITHOUT A CLEAR VISION OF THEIR CUSTOMERS

Source: PYMNTS (2/19)

The problem with customer retention in an era when consumers are easily distracted and pulled away isn’t that brands aren’t trying, or even that they are using the wrong tools. The problem, Thanx Founder and CEO Zach Goldstein told PYMNTS, is that they are using too many different tools separately without any unified vision in sight.

Businesses are spending a lot of energy trying to build deeper connections with their customers and failing, he said — because they don’t have the right data in hand to offer the right outreach. Using one tool for email marketing, another for loyalty and another for feedback, what they get is three different views of the customer that don’t inform each other. Thanx, he explained, wants to help enable brands by partnering with the card networks and so it can be easy and painless for brands to see their customers, offer them appropriate rewards when they shop and then reach back out to them via email channels to keep the relationship developing moving forward.

“That has been our focus,” Goldstein said. “We want to help brands move away from spray-and-pray generic email offerings to truly personalized campaigns.” It is a challenge that Thanx embraces on behalf of a variety of retail and restaurant industry clients, as the interest in identifying and then targeting a brand’s best and most loyal customers has a certain broad appeal. This can be seen most recently in its expanded partnership with Tommy Bahama restaurants — a brand that suffers from being both too well known and too unknown at the same time. Most people, of course, are familiar with Tommy Bahama clothing and fashion accessories, so familiar in fact that the news that there is also a dining component to the brand often comes as a surprise.

“A lot of business like Tommy Bahama with a massive retail presence have spent a lot of time and money investing on the retail side of the business, particularly in building data-driven relationships with their customers,” Goldstein said.

But for the restaurant side of the business that simply wasn’t the case. Tommy Bahama wasn’t able to build the same kinds of repeat customer engagement with its restaurant customer base for the good reason that it just didn’t know who those customers are. And while a brand may know it needs such knowledge, and may be aware of the power of personalization, the challenge is technological. Like most big and diverse brands, Tommy Bahama restaurants are operating with a few different IT systems in place, which can make aggregating and understanding the data a challenge. And data one can’t see or can’t decode is essentially wasted material, Goldstein pointed out. Customers who walk in and out of a restaurant with no way of making themselves known are essentially at the mercy of the store manager. That’s not a bad thing, and restaurant managers can do amazing things with their memories and remembering frequent customers, but the reality is busy nights happen (hopefully often) and finding and highlighting regulars is lot to hang on a single point of human interaction.

Technology provides a systematic approach to keeping customers interacting. The way to do that, Goldstein said, is to encourage the customer to enroll in an account with the Tommy Bahama restaurant brand. From that account, he said, the customer gets a channels to rewards and offerings, and the brand gains a tool with which it can actually get a view of the consumer, their preferences and their use habits. And all of that happens, Goldstein said, through paying with whatever chosen card is linked to the account.

“There are no extra steps, there is no added friction. And that makes it really easy for consumers who sign up once to participate. It doesn’t have to be top of mind.” Beyond the rewards, he notes, it creates a feedback channel so that if the consumer has an issue with their service they have a path to reach the company — and receive direct outreach back. That’s part of the standard toolbox on offer, he said, because the needs of the establishment can vary with time or by context. A customer who has been a regular diner and has suddenly stopped coming, he said, can be targeted for a “win back” campaign, or loyalty offerings can be geared around a certain time of day where the brand wants to see more business. The point, he said, is that brands need to be able to reach out to customers, and make offerings to them, and find a way to tap into that effortlessly. On the consumer side, it means making a simple card swipe (or dip or tap) the entry point, and for brands it means making the integration simple, and the data accessible and actionable.

“Brands don’t have time to take on another burdensome technology,” Goldstein said. “They need to be able to drive value in the business with literally one or two clicks — and then measure what campaigns are working and which aren’t.”

5. EXPERTS SAY EQUIFAX DATA BREACH WAS A SPY JOB

Source: PYMNTS (2/14)

Remember all that stolen Equifax data?

Remember how all those names, addresses, dates of birth, Social Security and drivers’ license numbers and other information were stolen in September of 2017 – the information of some 143 million people – in what still stands as the one of the biggest data breaches of all time?

Well, investigators reportedly cannot find it. What that means – and what is setting off alarm bells – is that the absence of that stolen data on digital black markets is a sign that criminals are trying to fence those stolen goods. And that is leading to suspicions that spies, not fraudsters, were ultimately behind the Equifax breach. If so, that would serve as a harsh reminder that the dangers out there in the digital wilds come not only from criminals bent on creating fake accounts and other vehicles, but also intelligence operations that keep developing their hacking and cyberwar expertise.

Breach Confusion

The news comes down to this: Eight experts on hacking the dark web, cybersecurity and associated areas who were contacted by CNBC reportedly don’t know “where the data is now. It’s never appeared on any [of the] hundreds of underground websites selling stolen information. Security experts haven’t seen the data used in any of the ways they'd expect in a theft like this — not for impersonating victims, not for accessing other websites, nothing." That lack of clarity is, according to CNBC, crafting a "consensus" that the Equifax data "thieves were working for a foreign government and are using the information not for financial gain, but to try to identify and recruit spies."

Spies continue to be recruited via a variety of methods, including those that involve ideology, blackmail and extortion, and simple financial gain. And thieves often have to delay selling their ill-gotten goods until attention on a particular theft dies down — that is a common situation when it comes to thefts of famous artwork, for instance. Even though some experts, quoted by CNBC or speaking elsewhere, had said such a principle might apply to the Equifax breach, its size and scope continues to attract a huge spotlight, including in the U.S. Congress. Seventeen months, according to those experts, is a long time to wait to sell such valuable data. According to the experts quoted by CNBC, the Equifax heist could have happened like this: "The breach probably started with a low-level criminal who exploited a vulnerability in Equifax's defenses but was not experienced or capable enough to do more damage by moving further throughout the company. This criminal then sought help via the criminal underground, and shared or sold information about the vulnerability. The buyer was probably a proxy for the Russian or Chinese government."

Marriott Similarity?

That is certainly imaginable. Another recent major data breach involved Marriott and the theft of data on about 500 million guests, information that included names, passport numbers, email addresses and Starwood account information. That breach is also among the biggest in history. The latest information puts the blame for the theft on China, as well as an intelligence-gathering campaign that hacked health insurance companies and security clearance files of millions of people living in the U.S. That revelation came as the U.S. government was gearing up to launch actions against China's trade, which include indicting Chinese hackers who work for the government. Russia, too, has been accused of multiple data breaches, and the country keeps developing a form of "asymmetrical" warfare that depends heavily on hacking and other online activities. North Korea is also regularly charged with conducting its own major hacking activity — including activity related to cryptocurrency.

Even if the Equifax data ended up in the hands of state-backed intelligence operators instead of the dark web, that doesn't relieve any pressure when it comes to online fraud, of course. In late 2018, for example, Juniper Research predicted there will be a 175 percent boost in cybercrime by 2023. That's on top of the 12 billion records expected to be compromised this year alone, and a cumulative tally of 146 billion records accessed by 2023. That comes amid a relatively tepid projection for cybersecurity spend, slated to grow 9 percent annually. The U.S. will remain a disproportionately large target by 2023, tied to half of the breaches.

Fraudsters and intelligence operators will continue to keep payments and commerce operators on their toes as they search for the latest technology to keep hackers at bay and reduce the scope of any future breaches.

6. NEW TECHNOLOGIES DRIVING NEW CONVERSATIONS ON PAYMENTS AND DEMANDS FOR ACCESS

Source: MasterCard (2/25)

Want to grab that purchase and go? You're not alone. Today more than ever, people are living an increasingly digital – and mobile – life and they expect their ability to pay for their needs and wants to match that same "always on" mindset, according to social media conversations identified in the 2019 edition of the MasterCard Digital Payments Study. Mobile payments represented more the 27 percent of the total social media conversation around payments, with total mentions increasing 20 percent over the prior year. Mentions of mobile wallets specifically more than doubled since 2017. Now in its sixth year, the study, developed in partnership with PRIME Research, analyzed more than 3.3 million conversations from the past year across several social media channels, including Twitter, Facebook, Instagram and Weibo.

"On-demand isn't just an expectation for cable and content provider; it's a reality for how people say they want to shop and pay every day," said Rose Beaumont, senior vice president of European communications and sales enablement at MasterCard. "In this year's study, we see just how much these fast, convenient and secure ways to pay are being embraced across all markets. And, it points to the continued interest and demand for years to come."

Interest in New Technologies

People are looking to newer technologies to have an impact on their lives. In the past year alone, such mentions on social media increased 30 percent since the last study. Today, nearly 20 percent of all mobile commerce payments are focused on contactless payments and mobile wallets. Beyond these primary focus areas, consumers are interested in how artificial intelligence, QR payments and wearable payments will impact their lives. Overall, people are increasingly positive toward these newer technologies. Virtually all (95 percent) mobile wallet conversations were favorable, with 30 percent of posts praising the speed, efficiency and simplicity of the current products. The adoption of mobile payments is seen in markets across Asia and Africa. India was the most dominant market – 30 percent – in discussing the use and potential of mobile wallets, particularly around public transit and the use of QR-based payments, led by specific references to MasterpassQR and PaytmQR in India. The U.S. was a distant second in consumer's discussions on mobile wallets (10 percent).

Primed for Action with Peace of Mind

Among the conversations analyzed, consumers clearly continued to be focused on the security of their money and their data as a foundational requirement. In their posts, people recognize the value of new technologies on delivering this peace of mind across mobile payments.

Looking at the newer technologies:

- Biometrics reached a potential 111 million, driven primarily by an interest in voice payments and fingerprint scanners
- Tokenization – and its critical role in supporting and protecting payments of all type – was featured in conversations reaching a potential audience of 11 million viewers
- While breaking news around data breaches drove one-fifth of data-related conversations, another 13 percent of these conversations noted the potential of digital security technologies, including blockchain, tokenization and biometrics.

MasterCard is a Member of ACT Canada; please visit https://www.mastercard.us/en-us.html

7. GEMALTO FIRST IN THE WORLD TO MAKE 5G SIM AVAILABLE TO UNLEASH THE POTENTIAL OF NEXT GENERATION NETWORKS

Source: Gemalto (2/21)

The new 5G SIM provides improved data privacy, enhanced protection against hacking and seamless 5G global roaming. Gemalto announces the industry-first 5G SIM in order to meet operator requirements for the new generation of network deployments which will emerge in 2019. Compliant with the latest ETSI 3GPP specifications and SIMalliance recommendations, the 5G SIM is defined by them as the only solution capable of securing 5G network access. The Gemalto 5G SIM brings not only improved data privacy and seamless 5G global roaming imposed by the latest standards but is also the first to add enhanced protection against hacking to anticipate future requirements.

By 2024, 5G network coverage is expected to reach 40% of the global population, and will account for 1.5 billion subscriptions. Leveraging the benefits of 5G, key use cases of the new SIM are set to include enhanced mobile broadband, massive IoT applications, and critical communication infrastructures.

The Gemalto 5G SIM will be available in all SIM form factors (removable SIM, M2M SIM, eSIM), during the first half of 2019. Key benefits of the new 5G SIM include full anonymization of end-to-end subscriber identities thanks to onboard identity encryption; it eliminates the potential to misuse such information to locate and trace individuals, or collect personal data, and ensures mobile operators comply with regulations such as GDPR. In addition, trusted environment resilience will help operators secure the entire SIM lifecycle, eliminating exposure to hacking attacks and accidental breaches. A seamless 5G roaming experience is also supported, maximizing revenues and enhancing the customer experience. Gemalto has been working closely with key 5G industry stakeholders around the world in the development of 5G SIM, through standardization, prototyping and testing.

"The 5G SIM provides the foundation of trust in this next generation mobile network for operators and other stakeholders in the eco-system" said Emmanuel Unguran, EVP Mobile Services & IoT Business Unit, for Gemalto. "It will help operators unleash the full 5G potential, maximize their network investments, and simplify new service deployment with full backward compatibility to previous 3G/4G technology."

"Qualcomm Technologies has a longstanding relationship with Gemalto focused on delivering mobile solutions with robust security," said Gautam Sheoran, Senior Director, Product Management, Qualcomm Technologies, Inc. "We are now extending this collaboration to allow OEMs to easily develop exciting 5G devices with strong security, using both Gemalto 5G SIM and our next generation flagship Qualcomm® Snapdragon™ 855 Mobile Platform to pave the path for 5G commercialization in 2019."

Gemalto is a Member of ACT Canada; please visit https://www.gemalto.com/

8. 'MIND-BLOWING' GAFFES AT QUADRIGACX LEAVE CRYPTOCURRENCY WATCHERS 'GOBSMACKED'

Source: CBC (2/14)

Cryptocurrencies such as bitcoin were praised by their fans because they are outside the reach of central bankers, but when things go wrong, as they have at crypto exchange QuadrigaCX, users have less recourse for government help. Industry observers are in disbelief over the revelation the embattled QuadrigaCX cryptocurrency exchange recently lost track of more than $460,000 in crypto coins.

"I'm totally gobsmacked ... that such a thing could happen," says Manie Eagar, CEO of Vancouver-based DigitalFutures, a business development consultancy that focuses on digital currency and blockchain technologies.

"Whoever took over the reins and is acting as the custodian of these funds should have at least done due diligence to avoid whatever happened."

The court-appointed monitor overseeing the search for $260 million in cash and cryptocurrency owed to QuadrigaCX users revealed on Tuesday that the exchange had access to $902,743 in online digital assets, stored in so-called hot wallets as of Feb. 5.

Basically, hot wallets are storage accounts that are easy to get in and out of because they are on the internet. However, Ernst and Young said that on Feb. 6, someone working for QuadrigaCX "inadvertently" transferred 103 Bitcoins valued at $468,675 into a so-called cold wallet that remains beyond the reach of the company. Cold wallets are not fully connected to the internet, which makes them more secure but also next to impossible to access using failsafe plans. Meanwhile, lawyers were expected to gather Thursday in a Halifax courtroom, where a judge will decide who will represent QuadrigaCX's creditors. Canadian case is another warning about the murky world of cryptocurrency: Don Pittis. Insolvency expert Tim Hill said the case is highly unusual, given QuadrigaCX has no offices, employees or bank accounts.

"We certainly haven't seen anything like this in Nova Scotia — and nothing in Canada that I'm aware of," he said in an interview. The Vancouver-based exchange was shut down Jan 28 amid a flurry of speculation about the sudden death of its CEO and lone director, 30-year-old Gerald Cotten, who led his five-year-old virtual business from a home north of Halifax. Court records say Cotten, who died suddenly on Dec. 9 while travelling in India, was the only person with access to the digital keys needed to access $190 million worth of Bitcoin and other cryptocurrencies. As well, the insolvent company owes about 115,000 affected users another $70 million in cash.

"Transferring funds to wallets they can't retrieve money from is really mind-blowing," said Samir Saadi, professor of finance at the University of Ottawa's Telfer School of Management. More than $400,000 in QuadrigaCX cryptocurrency disappears into 'cold wallet'. "They know they don't have access to those cold wallets and they still managed to make that terrible mistake ... It tells us a lot about the company's practices. There's no backup plans — nothing."

The selection Thursday of representative counsel, which will be overseen by Nova Scotia Supreme Court Justice Michael Wood, is part of a court-ordered insolvency process that was set in motion when the virtual company was granted protection from its creditors on Feb. 5. The purpose of the federal law is to allow insolvent companies owing more than $5 million to continue to operate while drafting a plan to pay off creditors, thereby avoiding bankruptcy. The court order includes a standard 30-day stay of proceedings, which means creditors are prohibited from filing lawsuits against QuadrigaCX until the order expires. An extension is widely expected to be granted by the court on March 5. Hill, a Halifax lawyer who specializes in insolvency and debt restructuring, said the law firms that will be selected as representative counsel will be paid by QuadrigaCX's parent company, Quadriga Fintech Solutions.

"There's a real danger here that there's going to be no money to pay these guys," said Hill, a member of BoyneClarke's business litigation team and a former registrar in bankruptcy.

"Unless they can move quickly to identify some assets, some money, this may not go on too long. People need to be paid." The representative counsel will speak for the creditors in court, but there's nothing stopping creditors from hiring their own lawyers.

QuadrigaCX mystery deepens as court finds little evidence cold wallets ever existed

Lawyers from across the country have expressed an interest in the case. A courtroom at the Nova Scotia Supreme Court will be back in session on Thursday, trying to decide which law firms should represent the more than 115,000 victims. Much of the actual money that is owed to creditors is in the form of bank drafts, which the company has failed to deposit in a financial institution because regular banks remain leery of dealing with cryptocurrency businesses. QuadrigaCX founder Gerald Cotten, who died in December, seems to have run the company from a single laptop with minimal backup plans. "That's obviously going to be a challenge, but at some point the court will be asked to assist with that," Hill said. "The court has very broad authority in these matters." One user of the platform, Tong Zou of Orillia, Ont., submitted an affidavit to the court, saying he is owed $560,000. The professional software engineer said he had been using QuadrigaCX since 2017. His statement was part of an application to the court to have two law firms — Toronto-based Bennett Jones and Halifax-based McInnes Cooper — appointed a representative counsel.

"After speaking with various affected users, I know that the affected users are very worried, confused and in need of assistance," Zou said in the affidavit. He said he was aware of several other users who are owed more than $100,000 — but he said they have chosen to remain anonymous.

9. THE CYBER FRAUD EPIDEMIC

Source: Canadian Credit Union Association (2/6)

A report released in 2018 by the antivirus company McAfee estimated the global annual cost of cyber crime to be in the range of $600BN or just under one percent of global GDP. That's a staggering number and one that is only predicted to grow as our personal and business lives become more and more dependent on doing things online. As the McAfee report says "Cybercrime is relentless, undiminished, and unlikely to stop." Part of the problem is that advancing technology is generally available to everyone, including the bad guys, and that makes the cyber crime problem a reality for everyone. In other words, if you or your members haven't been impacted by cybercrime yet, you will be. The McAfee report highlights that "Cybercriminals at the high end are as technologically sophisticated as the most advanced information technology (IT) companies, and, like them, have moved quickly to adopt cloud computing, artificial intelligence, Software-as-a-Service, and encryption."

Even a scan of the weekend paper provides a sobering glimpse into the cyber crime problem. Headlines talk about the potential security threats posed by smart home devices, financial abuse of seniors hitting record numbers, the work being done by Google's in-house counterespionage group and the suspected national security threat posed by a certain Chinese phone manufacturer.

The world is becoming an increasingly scary place for anyone that spends time online but there are things that credit unions and their members can do to help protect themselves. Central 1's fraud team recently released a Cyber Fraud Q&A document that provides practical information that credit unions can use to answer questions from their members about cyber fraud and how they can prevent themselves from becoming a victim. A copy of the Q&A document can be found on Central 1's secure site or on CCUA's Risk Management Resources website. Also, March is Fraud Prevention Month so we'll be sharing further information soon about how credit unions can take part in that initiative and help to raise member awareness about the growing cyber fraud problem.

Canadian Credit Union Association is a Member of ACT Canada; please visit https://ccua.com/en

10. MASTERCARD AND ANGAZA PARTNER TO BRING A NEW GENERATION OF LIFE-CHANGING TECHNOLOGY SOLUTIONS TO EMERGING MARKETS AROUND THE WORLD

Source: MasterCard (2/27)

MasterCard, has signed a global Memorandum of Understanding (MoU) with Angaza, a leader in last-mile distribution technology, which will see the two companies partner to rollout an efficient digital payment solution that increases access to affordable necessities, like solar home systems and water pumps, for people and businesses in emerging markets across the globe.

Leveraging Angaza's pay-as-you-go (PAYG) embedded metering and monitoring technology and MasterCard's cutting-edge digital payment solutions and infrastructure including QR technology, this partnership will not only unlock access to the basic necessities, but will also help people without access to credit or traditional banking services start on a path to financial inclusion. The partnership follows the successful launch of MasterCard's first PAYG application programming interface in Uganda last year, which combines low cost QR technology – an open and interoperable technology, with the internet of things to lead more secure and efficient payments. PAYG business models are emerging around the globe to give people the ability to pay for what they use, as they need it. The model adopted by Angaza allows life-changing products, such as solar home systems, clean cook stoves and water pumps, to be sold at a low upfront cost. Consumers can then pay off the cost of the products over a period of time.

Currently, most payments on the Angaza platform are conducted via cash or mobile money. With the integration of MasterCard's API, the solution will provide new levels of payment flexibility and affordability impacting the lives of millions of consumers across emerging markets. Additionally, this partnership could open up fresh access to other financial services and tools. By keeping accurate records of payments that a user is making, the user is able to establish a verifiable digital identity and trackable credit history which was previously impossible to create or maintain. This data gives companies and financial service providers the ability to put underserved populations on a new path to financial inclusion.

“We are delighted to be partnering with Angaza to bring access and inclusion to people and businesses around the world. This partnership will help consumers to overcome hurdles such as the significant cash outlay required to purchase critical items by leveraging micropayments, which in turn also helps to build their credit history. All of this is being made available via the internet of things, which is a great democratizer and is playing a critical role providing safe, secure and accessible digital ecosystems”, says Jorn Lambert, Executive Vice President, Digital Solutions at MasterCard.

“This is a pivotal collaboration for the last-mile distribution industry, bridging Angaza’s global pay-as-you-go solution with a leading digital payment provider,” said Angaza CEO Lesley Marincola. “The addition of MasterCard's QR technology to Angaza’s platform will allow solar distributors and their clients to process payments for life-changing products securely and efficiently, while opening doors to broader financial inclusion.” To date, Angaza’s technology has enabled more than five million people in emerging markets across Africa, South America and Asia to purchase over one million life-changing products like solar home systems, water pumps, and clean cookstoves. Following the completion of a successful pilot with the BOP Innovation Centre in Nigeria, MasterCard and Angaza will expand the programme to other markets in Africa and Latin-America to bring as many people as possible into the financial fold.

MasterCard is a Member of ACT Canada; please visit ***https://www.mastercard.us/en-us.html***

11. EU REACHES DEAL ON MARKETPLACE REGS

Source: PYMNTS (2/18)

As far as eCommerce drama goes, the running tension that defines the relationships among the European Union and U.S.-based companies such as Amazon, Facebook and Google has little competition. Now comes the next chapter in the story: An effort by the EU to crack down on what it views as harmful, monopolistic online marketplace practices. As part of the EU’s Digital Single Market push, regulators and politicians that are part of that body have, in the words of the EU, “reached a political deal on the first-ever rules aimed at creating a fair, transparent and predictable business environment for businesses and traders when using online platforms.”

What that means for the big online marketplace operators are more restrictions on such tasks as account suspensions and terminations, more disclosures about search engine rankings and business practices, and more power for marketplace sellers when it comes to complaints and other problems. The changes comes as those big firms face increasing pressure from European regulators and lawmakers — along with big fines — on such issues as antitrust and online privacy and security.

Marketplace Changes

According to an EU fact sheet about the new changes announced this week, the new rules "will apply 12 months after its adoption and publication, and will be subject to review within 18 months thereafter, in order to ensure that they keep pace with the rapidly developing market. The EU has also set up a dedicated Online Platform Observatory to monitor the evolution of the market and the effective implementation of the rules." The new rules are a product of deliberation among the European Parliament, the Council of the European Union and the European Commission. The meat of these new rules — and they are meant to apply to even the tiniest online marketplaces, along with operators of hotel booking platforms and app developers, according to the EU — concern those marketplaces. According to the EU, the main idea is to protect small businesses — an oft-expressed concern from that body as U.S.-based payments, commerce and tech companies keep making more inroads in Europe.

The new rules prohibit "digital platforms" from suspending or terminating "a seller's account without clear reasons, and possibilities to appeal." As well, "marketplaces and search engines need to disclose the main parameters they use to rank goods and services on their site, to help sellers understand how to optimize their presence. The rules aim to help sellers without allowing gaming of the ranking system."

Seller Concerns

Another EU rule takes aim at one of the most common complaints of marketplace sellers — even common among sellers located in the U.S. and selling mainly to consumers there. That complaint, pretty much focused on the Amazon marketplace, is that the marketplace operator competes with third-party sellers, and therefore has an inherent advantage. Research about third-party marketplace sales offer a more complicated view, as some reports and surveys have pointed out that some third-party sellers, for various reasons, actually gain a sales boost when the operators up the competition in a particular product category.

In any case, the new EU marketplace rule holds that "platforms must exhaustively disclose any advantage they may give to their own products over others. They must also disclose what data they collect, and how they use it — and in particular how such data is shared with other business partners they have. Where personal data is concerned, the rules of the GDPR apply." (GDPR, of course, is the EU's General Data Protection Regulation, an online privacy law that serves as another source of tension in that relationship between U.S. firms and European regulators.) The EU also wants marketplace sellers to have more power when it comes to complaints and problems they have, and the resolution process that follows. "All platforms must set up an internal complaint-handling system to assist business users," the rules state. "Only the smallest platforms in terms of head count or turnover will be exempt from this obligation. Platforms will have to provide businesses with more options to resolve a potential problem through mediators. This will help resolve more issues out of court, saving businesses time and money."

The fact sheet provided by the EU provided no details about fines or other punishments that companies will face for violating these rules. Nor was it immediately clear how these rules might impact the European operations of the big U.S. companies these rules clearly target. Comment from them was not immediately available as of late Friday (Feb. 15) afternoon.

Amazon Focus

But these EU rules come as other significant marketplace changes loom, at least at Amazon. The company recently teased its intention to change its marketplace fee structure, though the eCommerce operator provided no further details. More than half the units sold on the Amazon marketplace come from third-party sellers, the company said in January, and those sellers include a good number of smaller merchants. For the holiday quarter, for instance, more than 50 percent of sales on the platform came from small and medium-size businesses, Amazon said. Amazon does not breakdown how much marketplace sales it has by region or country. Overall, revenue from third-party seller services — such as commissions on sales and fulfillment and shipping fees — jumped 27 percent year over year in the fourth quarter of 2018, reaching nearly $13.4 billion, or about 19 percent of Amazon's total Q4 sales of $72.4 billion. Still, a rough picture of Amazon's European marketplace operations and its growth is possible to put together.

A recent analysis of the top 1,000 sellers on the Amazon marketplace — the metric used here is customer feedback, not sales, though the report states that feedback is an "indicator of sales volume" — found that U.S.-based sellers dominate that list, with 484 sellers (down from 584 in 2016), followed by sellers located in the U.K., which has 260 (up from 205 in 2016). Germany took the third spot (101 sellers, up from 86), and was followed by Japan, France and Italy. France, in fact, gained 18 sellers on the most recent rankings, a 90 percent increase from 2016 (though from a small initial base, of course). These new EU rules might take a while to play out, but the real-world implications — and possible backlash — will likely emerge before too long. Stayed tuned for the next chapter in this ongoing drama, one of the most important stories in the world of eCommerce in 2019.

12. CYBERATTACKS ON TRACK TO LEAD CORPORATE INSURANCE CLAIMS: STUDY

Source: PYMNTS (2/18)

The global insurance technology (InsurTech) market is slated to become a $1.1 billion industry by 2023, analysts have predicted, with growing analytics and artificial intelligence (AI) functionality accelerating innovation in the insurance market.

Corporate customers are a driving force behind the InsurTech industry's growth, with protection against cyberattack losses a popular target among InsurTech innovators and businesses alike. Despite the focus on cyber protection, however, a new report from insurance firm Allianz Global Corporate & Specialty said an unexpected category makes up the most popular type of claim filed by corporate customers of insurance products today. In analyzing 470,000 corporate insurance claims across 206 countries, totaling $66.5 billion in payouts, Allianz found in its Global Claims Review report that fire and explosions were the biggest causes of loss between 2013 and 2018. Researchers said the high costs are due to the disruptive nature of fires and explosions, including factory, gas and electrical fires.

“It's mainly [because of] two factors,” explained Allianz Global Head of Claims Philipp Cremer, according to Insurance Business Magazine last week. “One is the high concentration of value, and also the ever-increasing business interruption element of the claim. With the way production companies organize themselves, there is an increasing level of dependency in the production chain, and so business interruption claims do increase very significantly.” Aviation collisions and crashes landed at the number-two spot of most-expensed corporate insurance claims, with Cremer pointing to the lower rate of fatal air crashes and the rising cost of the rare crash that does occur. In addition to examining the most expensive types of insurance claims, Cremer explained which industries tend to have the largest losses.

“The energy industry has seen quite significant losses,” he said, “and there again, it's a high concentration of values and the volume of the business interruption which [drive] the losses. The pharmaceutical sector is another one where liability claims can be very significant, so it's very different scenarios for different sectors.” Despite the talk of natural disaster-related losses, most notably surrounding multiple deadly hurricanes in the U.S. in 2017, this category actually landed near the bottom of the list in terms of value of corporate insurance claims. Furthermore, discussion about cyberattacks, and the rise in cyber insurance products available to businesses, has not yet coincided with the emergence of cyber-related losses at the top of the list, though Cremer told the publication that rising cyberattack losses and insurance claims are likely ahead. Overall, he said, organizations have to take a holistic view of their operations and the risks they face.

“What I think is still an area where businesses can further analyze and take precautions is in their supply chains [and] contingent business interruption claims,” he said. “Understanding the supply chain, and finding ways of making it more resilient, I think, is for both our insureds and also for us something that is still an area to work on. Large corporates have thousands, and sometimes tens of thousands, of suppliers, so it is a very complex task.”

PYMNTS breaks down the numbers in the Global Claims Review report, identifying the biggest causes of financial loss for corporates, leading to massive insurance claims. $16 billion: the total value of corporate insurance claims related to fire and explosion losses. That means fire and explosions accounted for nearly one-quarter of all corporate insurance claims filed between 2013 and 2018.

Fourteen percent of the value of corporate insurance claims were linked to aviation collisions and crashes. According to Cremer, in addition to the lower frequency and higher cost of such incidents, more sophisticated (and, thus, more expensive) air equipment, and the rising disruption to broader air traffic and airport operations, have driven up losses in this category. Important to note, however, is that Allianz is one of the largest providers of insurance for the aviation space, meaning that Allianz data may not represent the whole of the insurance market. Seven percent of claims were related to natural disasters, which reports said is a particularly noteworthy finding, considering the rising talk of the impact of natural disasters on corporate and supply chain operations. Cremer predicted this figure to rise, as corporate exposure to natural disasters climbs, thanks to the “interdependency of production chains.” Even if one key supplier is in a disaster zone, he said, disruption — and losses — can be high.

13. CANADIAN STARTUP PROPERLY OFFERS NEW WAY OF BUYING AND SELLING HOMES IN CALGARY

Source: CBC (2/27)

But uncertain market conditions in Calgary have some experts worried Properly's arrival is opportunistic. A home owned in southeast Calgary just purchased by Properly, a startup tech company specializing in real estate. A Canadian tech startup is hoping a new way of buying and selling houses shaking up the U.S. real estate industry will catch on north of the border.

"We are in an era when transparency and convenience and choice is being offered to homeowners," says Properly CEO Anshul Ruparell. "And they have an opportunity to go through the transaction in a way that hasn't really been done before."

Properly is what's known as an institutional buyer or "iBuyer." Also known as direct buyers, iBuyers use algorithms to determine the market value of a home. They can make an initial offer to buy the property directly from the homeowner within 48 hours, and the whole process can be completed in a week, with the seller setting the closing date. Though based in Toronto, Properly is currently operating only in Calgary.

The company's data driven model is focused on buying only detached or semi-detached homes in the city, built after 1960 and worth $250,000 to $550,000. Anshul Ruparell, CEO and co-founder of Properly, says while innovation in real estate has happened in the U.S and other developed countries, it's been slow to arrive in Canada. Properly launched last summer with $8.5 million from investors and access to credit to buy more homes. It claims to be the first to bring this model to Canada and has big plans for 2019. Seen as disruptive players in American real estate, iBuyers first emerged in 2015. U.S companies, such as Opendoor, Offerpad and Knock, have raised hundreds of millions of dollars in investment and are operating in over a dozen markets.

How it works and what it costs

Selling a home is one of the most important financial transactions in people's lives, and one that can carry a commensurate amount of anxiety.

Properly's sales pitch is that its process can save time and reduce stress. Marie Poulin sold her house to Properly and paid a service fee of almost 7% on the transaction. She feels it was worth it. Marie Poulin was eager to offload the stress of selling her family home. She discovered Properly through a Facebook ad. After 19 years living with her husband and four children on a tidy suburban street in southeast Calgary, it was time to downsize. After she filled out an online form, Properly offered $368,000 for the family's spacious five-bedroom home and stuck with that price after its home inspection. The family rejected that offer but settled for $375,000. Poulin says she was happy to be relieved of some work. "I don't have to stage. I don't have to clean before every open house." Instead of paying an agent a commission, Poulin paid Properly a service fee.

This is the kitchen in Poulin's former home. Properly only buys detached or semi-detached homes that were built after 1960 and are worth between $250,000 to $550,000. The service fee ranges between six and 11 per cent of the offer price. It's based on the condition of the house being purchased and repairs it needs to be sale ready. Poulin's service fee was 6.6 per cent, close to what Properly says is its average seven per cent rate. So, her cost was just under $25,000, and while the combined commissions for both listing and selling agents in Calgary could have been just over $13 000 at typical local rates, Poulin was also factoring in closing costs and more.

"Going with the traditional Realtor route, we had no way of knowing how long our house would be on the market," said Poulin, who was worried about the possibility of owning two and carrying two mortgages.

Why Calgary, why now

While Poulin contacted Properly six weeks ago and is free of her old home, a neighbour who listed a similar house with a traditional agent in November has yet to sell.

It's not the only home lingering in the listings. Calgary's real estate market has suffered as the Alberta economy has struggled both in near lockstep with oil industry troubles and job losses. The Calgary Real Estate Board reports that detached home sales in the city for January 2019 were down 16 per cent from January 2018, and prices were off by four per cent in the same period. Allan Dwyer, an assistant professor in the Bissett School of Business at Mount Royal University, says making the wrong decisions on a real estate transaction can haunt a homeowner for 10-15 years. Calgary is a market that Properly's Ruparell knows well because he's from the city.

"The Calgary market today is one in which very few homes that are listed sell. Only about one in four after two months have sold," he says. "So, it's a market in which homeowners are facing more uncertainty than they ever have." The uncertain market conditions in Calgary have some experts worried Properly's arrival is opportunistic.

"Making the wrong decisions on a real estate transaction can haunt you for 10-15 years," says Allan Dwyer, an assistant professor in the Bissett School of Business at Mount Royal University. Dwyer believes that Properly's ability to move quickly will be attractive to some clients, but some of them may be in a vulnerable state.

"It reminded me a little of how the payday loan business kind of works and is very profitable around the margins of the economy," he says. "If someone was in a hurry or perhaps desperate, they could want to sell their house quickly but it's not always the best frame of mind to sell your home."

Does data mean a fair deal?

Ruparell says his company is committed to giving customers a fair price through technology.

"Our data model looks at hundreds of data points and factors things like proximity to local schools and hospitals to the level of traffic on the streets, which allows us to ensure that we give the homeowner the most accurate offer possible." Unlike a house flipper, the company's primary profit is not selling the house for a premium, but in service fees. On homes in good shape Properly says it will refund back 75 per cent of the difference if it sells a property for more than it paid.

Ruparell won't say how many transactions the company has completed since launching in June. However, in January, Properly purchased seven homes, representing about 1.5 per cent of the city's total deals on detached houses. For 2019, the company plans to buy about $50 million worth of homes in Calgary, which could add up to more than 100 houses. After that the idea is to take their real estate revolution national. Ruparell says the concept can work "not only in Calgary, but in every other city across Canada."

14. FRAUD'S NEW PARADIGM: LET FRAUDSTERS IN, BUT NEVER LET THEM LEAVE

Source: PYMNTS (2/19)

Fraud is rampant and thriving.

With a wealth of stolen credentials to pick from in the wake of several data breaches that comprised the identities of millions, fraudsters have more resources than ever. What's more, fraudsters are getting smarter, building out identities and initiating money transactions that are made to appear as legitimate as possible before making their move. Banks, financial institutions (FIs) and other members of the financial world are, thus, dealing with a rising flood of identity theft and application fraud, as bad actors look to capitalize on the email addresses, Social Security numbers, credit details and other information they have on hand. In the latest Digital Fraud Tracker™, PYMNTS examines how fraudsters are capitalizing on stolen data, as well as how banks and retailers are responding to a world where many of the credentials they use for online verification have been compromised.

Around the Digital Fraud World

With fraudsters getting bolder, banks, retailers and consumers are recognizing that stronger verification is now a necessity. Meanwhile, many of the affected brands are taking steps to win back consumers' trust.

Take Marriott, which is still dealing with the fallout of a breach that left the data of 500 million rewards customers exposed. The hotel is subsequently rebranding its rewards program, a move expected to take place within the next year. While the rebranding may help the company distance itself from the breach, affected consumers are likely to deal with the repercussions of the breach for years to come. Meanwhile, digital streaming companies are seeing an increase in fraud, with bad actors turning to phishing schemes and other tools to ensnare the identities of customers. Netflix, for one, is currently warning its customers of an email scam designed to steal payment details from users. Overall, thanks to the rise in data breaches, merchants and FIs alike are dealing with a steep increase in fraud. In one such instance, a First National Bank customer personally lost $10,000 from identity theft, after a fraudster used his name and identity to obtain and charge a credit card.

Inverting the Fraud Approach

For banks, fraud protection is a crucial part of staying competitive. Yet, how can banks protect against identity theft and application fraud with so many details compromised? First, banks need to stop thinking about fraud as an identity problem, and start thinking of it more as a money problem, according to Dickson Chu, global head of portfolio management for BBVA. Second, banks need to invert their fraud protection strategies to watch money movement, he told PYMNTS.

"It's not about putting locks on the door — it's about making sure there's no way to get the money out," Chu said. "We're perfectly happy if you're a fraudster [who's] going to move money in … because we're going to have some additional verification methods if you move the money out."

15. MASTERCARD AND DOCONOMY LAUNCH THE FUTURE OF SUSTAINABLE PAYMENTS

Source: MasterCard (2/25)

New collaboration focuses on fighting climate change and enables users to track, understand and take accountability of their carbon footprint. Doconomy and MasterCard announce their joint effort to combat climate change by enabling DO – a free and easy-to-use mobile banking service that lets users track, understand and reduce their CO2 footprints through carbon offsetting. The launch of DO sets a new standard for purpose-driven payment services and is a major step in MasterCard's commitment to drive innovation for a sustainable future.

DO Credit Card

By implementing DO MasterCard and Doconomy lets users' values guide their everyday consumption towards more sustainable choices. DO also enables carbon offsetting via UN certified projects. As part of the service DO offers a possibility to invest in funds with a positive impact on people and the planet. This way the solution gives the consumer insights into the environmental effects of their consumptions, paired with tools for creating change by making sustainable choices.

"Together with Doconomy we can engage consumers, retailers and businesses in the fight against climate change. This collaboration is an important part of our focus on sustainability, and this innovative solution offers people a simple way to take responsibility for their carbon footprint, based on what they consume," commented Mark Barnett, Divisional President of MasterCard UK, Ireland, Nordic and Baltics. In addition to offering users to make their consumption more sustainable, customers can also apply for the physical, climate-friendly and biodegradable DO MasterCard payment card. The card, which is printed with recycled pollution (Air-Ink) and with no magnetic strip is the first of its kind in the world. The DO card is the most tangible payment service effort on the global SDG 12 scene.

”Via MasterCard's global network Doconomy can reach and leverage the power of consumers all over the world and direct capital towards sustainable initiatives. For us, there is no partner better suited than MasterCard, given their sense of purpose and leading technical expertise,” says Nathalie Green, CEO at Doconomy. DO has attracted attention from some of the world’s most prominent actors. The United Nation’s UNFCCC-secretariat wants to explore a collaboration with Doconomy and MasterCard to promote climate action and awareness among citizens and organizations globally.

“DO represents a new and interesting way of bringing climate action directly to the consumer, which is one of our strategic objectives in our work on Global Climate Action.” says Niclas Svenningsen, Manager, Global Climate Action at UNFCCC. The DO app will become available during April. To join the movement and read more about how we fight climate change through consumption you can visit: https://doconomy.com.

MasterCard is a Member of ACT Canada; please visit https://www.mastercard.us/en-us.html

16. WHEN PASSWORDS BECOME CORPORATES’ OWN WORST ENEMY

Source: PYMNTS (2/8)

Cyberattacks are a massive problem for organizations today, and the threat is only growing larger. IBM data said the average cost of a data breach is $3.86 million, with U.S. companies experiencing an even higher average of $7.91 million. Rising frustrations with passwords have churned up excitement over sophisticated technologies, like biometrics, to safeguard data. However, in the enterprise world, implementation of those tools is no easy feat. OneLogin Chief Technology Officer and Founder Thomas Pedersen recently told PYMNTS why overcoming corporate security’s password hurdles doesn’t come without its own headaches. Promises among security technology providers to kill the password have been “exaggerated,” he said, so the lackluster security measure sticks around.

“The problem with passwords is that we have so many applications, and people are barely capable of remembering one password,” Pedersen added, noting that, for organizations using hundreds of applications, repeat passwords are common. Plus, professionals will often use paper or spreadsheets to keep track of those login credentials. The reliance on passwords means those credentials become more of a security liability than protector, as cyberattackers attempt to infiltrate enterprise systems. In one tactic, Pedersen explained, hackers can take the top-500 weakest (i.e., most common) passwords and check them against millions of accounts. In another, phishing scams will fraudulently request an employee login to Uber or LinkedIn to steal those credentials.

“It may not seem so risky to give up a LinkedIn credential,” said Pedersen, “but people use their password for more than one thing.” A hacker may target an executive in the finance department with a phishing scam, someone who they know is a controller, with a higher level of access to company bank accounts or other financial data. A successful email campaign that steals the password of a company’s Uber account could also compromise an organization’s online banking credentials or accounting app login information.

Considering the risks: It’s surprising that organizations remain so ill-prepared to mitigate the threat. Yet, according to Pedersen, most professionals are still not educated on how to spot a phishing attack. Furthermore, among OneLogin‘s own customer base, it’s about a 50-50 split between organizations that use multi-factor authentication — now considered an essential standard of enterprise security — and those that don’t. He pointed to organizations’ ongoing migration to the cloud as yet another trend opening up the enterprise to data security risks, a scenario that presents companies with more applications with which to repeat a password, as well as more data in the cloud — thus, leaving them open to infiltration. On the other hand, another challenge businesses currently face is their inability to migrate away from legacy infrastructures that were not built for the modern age of security threats.

“The really scary thing is that there are so many companies that have really old software, and they either don’t have the resources or budget to upgrade it,” Pedersen said. “That’s one area where you see these big breaches.” The security challenges don’t stop there. Today, organizations are tasked with not only safeguarding corporate data from outside bad actors, but managing authentication and authorization of their own employees with different levels of access to various apps. Not every employee should be authorized to approve a multimillion-dollar payment, for example. The rise of the application programming interface (API) ecosystem — as regulations like Open Banking in the U.K. create greater pressure for banks in the U.S. to open data to third-party FinTech firms — will introduce even more, less familiar challenges for enterprise security experts. As organizations migrate to the cloud and adopt more apps, cross-app integration will be essential for functionality. However, when a single-factor login process is all one needs to connect a third-party app to their bank account, managing data access can quickly get messy.

“These aggregators can be targets of attacks themselves,” said Pederson, who added that the API ecosystem and its impact on corporate security is an area he’s watching as it evolves. “API integrations are definitely a blind spot for many companies.” On the whole, cyberthreats continue to expand, and millions of dollars are on the line for businesses that fail to implement tactics like multi-factor authentication (MFA), instead relying on lackluster passwords to manage hundreds of account logins. While technology innovators have vowed to do away with passwords altogether and replace login processes with shiny biometric authentication tools, this change is likely to be slow, as organizations struggle to move beyond legacy infrastructures not built to support such security measures. Unfortunately, despite the warnings, Pedersen said corporates thinking about data security are often like consumers thinking about insurance: they don't realize they need it until something bad happens.

"I'm constantly surprised by how many companies take a lot of risk," he said. "We have a lot of customers not even employing MFA. How can you not do that? A lot of companies need to wake up and take it seriously, because they're very exposed."

17. WHY FASTER PAYMENTS ISN'T THE ANSWER TO ACCOUNTS RECEIVABLE DELAYS

Source: PYMNTS (2/19)

With faster payments functionality beginning to take off in the U.S., the outlook of how accelerated transaction times might impact B2B payments and, more specifically, the issue of late payments to suppliers, remains unclear.

When NACHA first released its Same Day ACH capability, only about 6 percent of the first 2 million transactions made in the service's first 11 days were B2B payments. That probably won't come as a surprise to many in the B2B payments space, considering that organizations typically try to float their capital for as long as possible, a cash management tactic that can lead to longer payment terms with small suppliers, and the prevalence of late payments.

In the U.K., the issue of late supplier payments has caught the attention of policymakers and small business (SMB) advocacy groups. This week, the U.K. Federation of Small Businesses (FSB) put added pressure on government officials, urging lawmakers to no longer award government contracts to late-paying companies. The FSB's own data found that each small supplier is owed an average of $7,391 in outstanding invoices. Rimilia, a U.K.-based cash application and accounts receivable solutions provider, said the issue of late payments is not necessarily surprising, considering the long-standing tradition of holding onto cash as long as possible and, therefore, delaying payments to suppliers. As Rimilia expands into the U.S., the company will be taking lessons it's learned from Europe's own dealings with late supplier payments and the introduction of faster payment capabilities in the market. Steve Richardson, Rimilia co-founder and chief commercial officer, told PYMNTS that faster payment initiatives like Same Day ACH are not the silver bullet of late B2B payments — though not necessarily for the reasons one may think.

"We see faster payments coming into the U.S. market, which we saw in Europe probably 10 years ago, and that made little difference [in late payments], from our point of view," Richardson said. "It actually caused problems before it solved them. Companies weren't any better off after faster payments." One of the biggest blockades is the fact that, even with the option to deploy faster payments, companies, especially the largest ones, simply won't change their behavior. Richardson likened it to "trying to right the Titanic in a canal." Large enterprises are locked into their payment habits and complex, legacy ERP systems, so initiating any change in technology or behavior is no easy feat. Yet, another key factor behind faster payments' inability to accelerate supplier payments, both across Europe and in the U.S., is a lack of remittance data, he said. Payments data is often sent separately from the funds, so even if a company receives a payment same day or in real time, information about who sent that payment, and why, still comes on a delay.

"What we found in Europe [was], in many cases, the payment would come on the hour, but organizations were receiving it with less information," explained Richardson. "They didn't know where it was coming from, what organization paid it — there was a disconnect with payments arriving and information not being there."

That disconnect can be found in many transactions, whether via faster payments infrastructure or other rails. This point of friction is particularly challenging across borders, he noted: A lack of remittance data, coupled with currency fluctuations and exchange rates, not only makes it confusing for a company to understand which invoice matches a payment it has received, but can turn accounts receivable into a cost center. The lack of visibility and data linked to payments has emerged as a focal point for many FinTech firms — with companies like ACH Alert recently announcing a new tool that enables financial institutions (FIs) to more efficiently manage ACH payment file data, or payments messaging firm SWIFT pushing for standardization of that information.

Addressing the remittance data gap may certainly help to spur adoption of digital and faster payments in the B2B arena. However, according to Richardson, it's not going to solve the issue of late payments, particularly in the U.S., where he doesn't see the same type of regulatory pressure on late payers that the U.K. and Europe have imposed. What will help, though, is the integration of technologies like artificial intelligence (AI) and predictive analytics, enabling companies to adopt what Richardson described as a "predict and prescribe" approach to accounts receivable. Technology and analysis of payment behavior can empower a business to predict when and how a corporate customer will pay. After all, a predictable delayed payment is better than an unpredictable one. Richardson said technology is able to predict about 70 percent of customers' payment behavior. For the remaining 30 percent, organizations must apply the "prescribe" strategy — that is, to require certain payment behavior from their customers before any agreement is made. Rewarding on-time payments with higher credit limits, for instance, enables businesses to become proactive with their customers' payment behavior and cash management strategies.

"If you look at performance and behavior and predictability, you can turn cash managers into front-line sales people — onboarding the right customers, offering the right credit limits," he noted. "You're turning customer behavior into a certain way that allows you to trade on a much better, even keel with them."

18. VISA: EMV CUTS CARD-PRESENT COUNTERFEIT FRAUD BY 80 PCT

Source: PYMNTS (2/13)

Merchants saw a drop in card-present fraud due to the increased adoption of Europay, MasterCard and Visa (EMV) chip cards, Visa said. Merchants who have upgraded to chip technology saw a decrease of 80 percent in counterfeit fraud dollars in September of 2018 when compared to September of 2015. Also, total counterfeit fraud dollars went down by 48 percent. More than 3.1 million merchants now accept chip cards, which is an increase of 692 percent since the beginning of EMV migration, and almost 70 percent of storefronts in the United States now accept chip cards.

The number of chip cards in the U.S. has grown from 159 million in 2015 to 511.1 million in Dec. of 2018. That's an increase of 221 percent since September of 2015. Now, 71 percent of Visa credit and debit cards have chips. Transactions on chip cards are also on the rise. About 98 percent of overall U.S. payment volume in December was done on EMV cards. In other Visa news, the company recently announced a partnership in Japan with LINE Pay Corporation, operator of the popular payment app LINE Pay.

The LINE Pay-Visa credit card is set to be released later this year, allowing consumers to make payments at merchants accepting Visa throughout Japan and around the world. Consumers can use LINE Pay through their smartphone screen, without having to present a physical credit card.

"As LINE Pay has grown, our top priority has always been providing the best possible user payment experience," LINE Pay CEO Youngsu Ko said. "We believe the launch of the LINE Pay-Visa co-branded credit card will greatly improve the entire LINE Pay platform, adding a diverse range of easy-to-use features and driving a significant increase in users." The LINE Pay-Visa co-branded credit card will also offer exclusive rewards, including the LINE Points program. Users will gain LINE Points for their spending, in combination with "My Level," an incentive program offering bigger benefits for the most active users.

MasterCard is a Member of ACT Canada; please visit https://www.mastercard.us/en-us.html

19. HOW 'DYNAMIC FRICTION' COULD BE ONLINE FRAUD'S KRYPTONITE

Source: PYMNTS (2/12)

Do you want to gain a step on fraudsters? Do you want to beat them while also making it as seamless as possible for legitimate consumers to buy from your website and contribute to your bottom line?

Then be prepared to toss out the rules.

Okay, that's hyperbolic. But it's in service of a larger, very important point: Online fraudsters are much smarter than they were just a decade ago, and slavish adherence to rule-based fraud prevention systems will, essentially, leave a door or two open for those criminals to come through. In the latest edition of the PYMNTS Masterclass video series, Kevin Lee, trust and safety architect at Sift, dives deep into the new landscape of fraud, and gives specific advice about how to best counter it. Sure, everyone knows fraudsters are becoming more sophisticated and organized — but how many know what to really do about it? Besides that Masterclass video, Lee, along with Karen Webster, will discuss this subject further in today's PYMNTS webinar entitled "Building a Trust and Safety Team from the Ground Up."

Fraud Evolution

In the new Masterclass video, Lee summed up the evolution of fraud over the past decade or so, providing an observation that might lead to some anxious nights for merchants. No longer does fraud typically mean "one individual" trying to break into an eCommerce platform. "Now, different types of bots and scripts attack platforms, not one by one but thousands at a time," he said.

And that's not all: Fraud today involves relatively complicated — compared to a decade or so ago — attempts to take over legitimate accounts or create enduring fake ones. As well, retailers handle much more than payments these days, of course: Digital commerce means delivery, content and other factors that can also give criminals an opening. That all presents numerous challenges for any retailers interested in avoiding the bad PR, litigation and loss of revenue that typically follows a breach or hack. Among them is building better fraud prevention defenses without alienating honest consumers and existing and potential customers. To put it another way, the challenge is to stop criminals without introducing too much friction that can result in customers giving up on creating accounts or abandoning online shopping carts.

Numbers Game

It's a simple matter of numbers, Lee said. Traditional fraud management "might focus on the 1 percent who are exploiting the system." That sort of fraud prevention "spends 100 percent of the time on that one aspect of fraud."

But what about the 99 percent who are on an online retail site with honest intentions, and just want to buy as quickly as possible and then get on with their lives? Well, that's where a practice he called "dynamic friction" comes into play — a concept that can not only help prevent fraud, but also builds trust in the platform and with the merchant. As Lee told it, the danger of fraud starts well before the transaction, and that knowledge can help defeat it. A fraud prevention system that is based on machine-learning algorithms — not just legacy rules that have probably been around for years — can lead to more understanding about the people who come to a particular platform. And that understanding can lead to more precise detection of fraud attempts without putting too many speed bumps in the path of honest consumers.

Digital Bread Crumbs

Consumers leave “digital bread crumbs along the way,” Lee said. Such factors as how quickly a consumer created an account, the nature of the keyboard strokes and other traits can help determine if the person’s intent is legitimate or criminal.

“Within 10 seconds, did they go to purchase three GoPros, or were they browsing?” he asked by way of example. “Did they start with GoPro accessories first? Did they put something in the cart and then remove it? All these things, from a behavior standpoint, are really telling.” A fraud prevention system that is primarily rules-based, by contrast, would not spot those traits, those complications. Rules are binary — they do only “yes” or “no.” Fraudsters — at least the successful ones — are not so dim as to be stopped by a binary fraud prevention system, Lee said. “Fraudsters learn to adapt very quickly.” Not only that, but consumers are impatient and unforgiving. Faced with too much friction, they might just leave and check out a competitor. Another goal of that machine learning model for fraud prevention is to reduce what Lee called the “insult rate” — treating legitimate customers as potential criminals, which could lead to honest accounts being shut down.

Executive Buy-In

Getting past rules-based thinking when it comes to fraud prevention requires more than a few conditions, not the least of which is what Lee called “executive buy-in.” He drew upon his spam prevention experience at Facebook to explain how various teams within a single business not only have to work together — the practice of eCommerce gets increasingly complicated, with new products coming out all the time, and online retail encompassing a variety of tasks and features — but to “evangelize” their goals and work.

As well, an organization needs a “centralized team dedicated to trust and safety,” Lee said. In short, “you need a holistic approach.” Platform operators have an advantage: The “tremendous” amounts of data they have about the “user’s entire online journey.” The key is making sure that data is fed into machine learning data-mining tools to detect those patterns that indicate fraud — and to focus not just on fraud, but the larger, potentially more lucrative concept of “trust and safety,” he said. That’s not to say rules are useless, though. “You still want rules at the end of the day,” Lee said. For instance, a good rule is to not deal with consumers who have IP addresses from North Korea. “You don’t need a machine to tell you that,” he said. Still, he said, “You are going to need to move beyond the rules, pure and simple.”

20. VERIDOS LEADS NEW EU RESEARCH PROJECT ON BORDER CONTROL

Source: G+D Mobile Security (2/26)

- The EU funded project is called D4Fly, short for Detecting Document frauD and iDentity on the fly
- The goal is to augment the capabilities and capacities of border authorities to counter emerging threats in document and identity verification
- Veridos will lead a team of 18 partners representing governmental organizations, research institutions, and private entities

Veridos, one of the world’s leading identity solution providers, will head a new EU-funded research project, which focuses on enhancing the quality and efficiency of verification at border crossings. The goal is to reduce the process duration to enable a non-stop border-crossing experience for travelers and to significantly decrease fraud. Veridos will act as a consortium leader and will work together with 18 partners on the project, which gets its funding through the EU Research and Innovation program Horizon 2020.

The Veridos-led project, called D4FLY, focuses on the authentication of travelers on the move and document verification with the primary goal of making border control faster and more secure. Research topics will include 3D face recognition, the use of smartphones as a means of identification, document forgery detection, and anti-spoofing. The potential benefit of blockchain technology in identity verification will also be investigated. The project is funded by the EU Horizon 2020 program “Secure societies - Protecting freedom and security of Europe and its citizens”. Dr. Silke Bargstädt-Franke, Senior Vice President and Head of Product Management at Veridos explains why the project is needed: “The use of biometrics for identification at border crossings has significantly improved security and efficiency. However, we need to continuously advance the technology in order to tackle abuse and manipulation. D4Fly will, for example, evaluate techniques to detect so called spoofing, which is the use of face masks or other artificial replicas to fool the biometric authentication”.

Frank Schmalz, Director of Innovations at Veridos, comments that “Veridos is a trusted partner for many governments around the world that expect state-of-the-art border control solutions. With research projects like D4Fly we strengthen our know-how in the latest technologies and guarantee the delivery of future-proof-solutions”. Four different border control points and one document fraud expertise center will form the project’s testing and demonstration ground including locations in Greece, Lithuania, and the Netherlands. D4Fly is the fourth EU research project for Veridos in recent years. These projects have included the PROTECT project on biometric border technology, which the European Commission has described as an EU research success story.

G+D Mobile Security is a Member of ACT Canada; please visit ***https://www.gi-de.com/en/ca/***

21. ACCENTURE, QUALCOMM AND KELLOGG COMPANY CREATE AND PILOT VIRTUAL REALITY MERCHANDISING SOLUTION TO TRANSFORM BRAND AND RETAIL STRATEGY

Source: Accenture (2/14)

Solution demonstrates business value of VR, results in 18 percent increase in brand sales during testing. Accenture, Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated and Kellogg Company have collaborated to develop and pilot a solution that embeds eye tracking technology in a mobile virtual reality (VR) headset to reinvent how brands and retailers gather critical consumer data and perform market research.

The Accenture Extended Reality (XR) practice developed the VR merchandising solution utilizing a Qualcomm® VR reference design headset, powered by Qualcomm® Snapdragon™ 845 Mobile VR Platform. The VR merchandising solution features embedded eye-tracking along with mixed reality software from InContext Solutions and eye-tracking data analytics capabilities from Cognitive3D. The resulting experience immerses consumers in a full-scale, simulated store, enabling them to move through the space, shop, pick up products and place them in carts – all while monitoring what consumers are looking at, for how long and why. The mobile solution is designed to allow companies to extend their reach to more geographically dispersed participants and perform market research faster, more affordably and on a larger scale.

The solution was tested in collaboration with Kellogg Company around the launch of its new Pop Tarts Bites product. The mobile VR eye-tracking solution provided far deeper behavioral data than standard testing, which typically relies on online surveys and in-home user tests. In fact, this new data led to an entirely different merchandising conclusion than what was determined by traditional methods. Rather than placing Pop Tarts Bites on higher shelves, which conventional testing indicated was where consumers expected to find new products, the VR solution demonstrated that optimal placement for the new product was on lower shelves. This led to an increase in brand sales of 18 percent during testing.

“Our VR merchandising solution has the potential to transform product placement by examining consumer buying behavior in a holistic way,” said Raffaella Camera, global head, Innovation & Market Strategy, Accenture Extended Reality. “By combining the power of VR with eye-tracking and analytics capabilities, it allows significant new insights to be captured while consumers shop by monitoring where and how they evaluate all products across an entire shelf or aisle. Ultimately, this enables product placement decisions to be made that can positively impact total brand sales, versus only single product sales.”

Jenny McDaniels, senior manager of Category Strategy at Kellogg Company added, “When trying to best assess a future product’s shelf placement, this new methodology provided optimal guidance from both a product and category perspective. This approach provided multiple data outputs, which in turn, created a holistic solution that would drive success for both the category and product.”

“XR provides transformative value to the enterprise,” said Patrick Costello, senior director of business development at Qualcomm Technologies, Inc., “At Qualcomm Technologies, we develop foundational XR technology through our VR reference designs that are engineered to enable companies to evaluate and quickly launch devices. This proof of concept with Accenture and Kellogg Company demonstrates the benefits of full immersion and eye-tracking and we expect several customers to follow with similar deployments.”

This new pilot solution represents an important step toward transforming retail merchandising. Brands spend considerable time, money and manual effort to determine optimal product placement and assortment on store shelves, as well as an ideal pricing strategy. However, these efforts tend to be limited in terms of the depth and quality of data garnered. The VR merchandising solution can provide deeper data while expediting the merchandising process and reducing costs at scale by:

- Expanding testing reach to diverse locations: Companies can invite geographically dispersed consumers to use the mobile VR headsets for product testing in their homes, at brick-and-mortar stores, during product roadshows or at any large consumer gatherings.
- Improving experience in branded environments: Shoppers can walk through realistic and branded virtual store models, look at shelves at their discretion, pick up and examine products, and place selections directly into their carts.
- Increasing the dataset for analytics: During the shopping process, companies can gather data using eye-tracking technology that is built into the VR headset in a manner that does not interrupt the shopping experience. The resulting analytics provide detailed insights into actual consumer behavior, such as which products attract their attention, where they look first or gaze longest, and what helps to trigger buying decisions.
- Decreasing costs while improving flexibility: The VR-based solution makes it easy to test a variety of retail designs and layouts, cost effectively. In a matter of minutes, brands and retailers can modify store and shelf layouts in the VR environment, rotate product inventory and experiment with pricing to determine an optimized plan.
- As a strategic initiative of Accenture, the Accenture Extended Reality (XR) practice uses human-centered design principles, deep industry knowledge, global scale, and expertise in combinatorial technologies such as AI and IoT, to help companies imagine, create and deliver impactful XR experiences to unlock new business value. For more information, please visit **https://www.accenture.com/us-en/insights/technology/virtual-reality-merchandising**

Accenture is a Member of ACT Canada; please visit https://www.accenture.com/

22. RESEARCHERS FIND LITTLE TRACE OF QUADRIGA'S STUCK MILLIONS ON THE BLOCKCHAIN

Source: Global News (2/9)

On Feb. 5, Nova Scotia Supreme Court Justice Michael Wood granted QuadrigaCX's application for creditor protection. The embattled cryptocurrency exchange says it cannot access some $180 million worth of customers' cyrptocurrency stored in virtual safes that may only be accessible through its defunct CEO's encrypted laptop. The court has ordered Ernst and Young, which has been appointed monitor in the proceedings, to take possession of the laptop. But experts who have analyzed publicly available cryptocurrency transfer patterns say there's little sign of digital vaults stuffed with millions and linked to Quadriga.

"All the analysis done so far has turned up no sign of the cold wallets they've been talking about," Max Galka, cofounder and CEO of Elementus, an analytics firm, told Global News.

"Cold wallets" is crypto lingo for virtual storage where companies often hold the majority of their funds. Because they're held offline, cold wallets are deemed more secure than so-called hot wallets, which are maintained on servers and generally handle day-to-day transactions, much like the cash sitting at a bank teller's desk. Instead, the company appears to have been transferring money from its hot wallets to other crypto exchanges, Galka said. While cryptocurrency exchanges like Quadriga may choose to store customers' money on other exchanges rather than in their own virtual vaults, those transfers appear to be at odds with the business model described by the company in court filings. At least one other independent analysis corroborates Galka's assertions, Global News has learned.

That research further complicates the picture around Quadriga, whose spectacular meltdown has drawn the eyes of the world to Canada's cryptocurrency sector. The crypto exchange, which launched in 2013, went into a tailspin after the sudden passing of its 30-year-old CEO, Gerald Cotten, who died unexpectedly during a trip to India in December. Quadriga ceased operations in late January, saying it was facing severe liquidity issues. It filed for creditor protection in Nova Scotia on Jan. 31. The company currently has only $375,000 in cash and owes to more than 100,000 customers a total of approximately $250 million, $180 million of which is in cryptocurrency, according to court documents. Jennifer Robertson, Cotten's widow, has taken the reins of the company but says she had no involvement in the business while her husband was alive, the filings show.

"The laptop computer from which Gerry [Gerald Cotten] carried out the [company's] business is encrypted, and I do not know the password or recovery key," Robertson's affidavit reads. "Despite repeated and diligent searches, I have not been able to find them written down anywhere." The company even engaged an expert to try and break into the laptop in order to recover access to the funds but to no avail, the documents show.

Cotten ran the company's business from his laptop and was exclusively responsible for transferring money between hot and cold wallets. He was Quadriga's sole officer and director, according to the court filings. But while the focus of attention has so far been the laptop, Galka and others have been looking at the blockchain, the digital ledger where cryptocurrency transactions are recorded. Researchers can access publicly available digital records to follow money trails. When Galka analyzed Quadriga's history of transactions in Ethereum, he found no evidence of cold wallets holding millions. There are about 60 million accounts on the Ethereum blockchain and only around 20 that hold the balance that Quadriga claims to have. But none of them seem to belong to the exchange, Galka said.

"We have looked at every single address on the blockchain that Quadriga transacted with — it's hundreds of thousands of addresses — and, in our opinion, none of them even remotely fits the profile of a cold wallet." James Edwards, an independent cryptocurrency analyst who publishes his findings on a website called Zerononcense, appears to have been the first to flag a possible lack of cold wallets associated with Quadriga.

"It appears that there are no identifiable cold wallet reserves for QuadrigaCX," Edwards concluded in a publicly available report. At Elementus, Galka said he traced some funds likely coming from Quadriga to ShapeShift, a U.S.-based cryptocurrency exchange that has been the subject of a Wall Street Journal (WSJ) investigation into money laundering. ShapeShift CEO Erik Voorhees told Global News via email that his company has found "a number of transactions potentially related to QuadrigaCX going back to 2016, though these may simply be Quadriga's customers."

As for the WSJ article, which claimed in September that "a parade of suspected criminals" had been using ShapeShift to hide funds, Voorhees said it was "nonsense." The company has published a rebuttal to the WSJ inquiry. More recently, it provided a report stating that it assisted with 60 law enforcement inquiries from around the world, a volume that it characterized as "pretty typical" for cryptocurrency businesses of its size. Voorhees said the company would be ready to help with any lawful investigation regarding Quadriga. Richard Niedermayer, a lawyer with Stewart McKelvey in Halifax who represents Robertson, declined to comment, pointing instead to Quadriga's latest update on the court proceedings. For his part, Galka said the fact that Quadriga's cryptocurrency seems to have been transferred to other exchanges instead of cold wallets may be good news for users.

"Recovering the passwords from an encrypted computer — that sounds like quite a difficult task," he said. "But it seems at least possible that the funds are just sitting in other exchanges."

23. FLEXITI SIGNS LONG-TERM AGREEMENT WITH EQ3 TO OFFER ITS POINT-OF-SALE CONSUMER FINANCING SOLUTION

Source: Newswire (2/12)

Flexiti Financial announced today that EQ3, a manufacturer and retailer of custom upholstery, furniture and home accessories, has signed a long-term agreement to implement its platform. EQ3 has 14 retail locations across Canada and the United States.

"EQ3's mission is to make modern furniture accessible and that extends to the payment plans we offer our customers," said Dennis Liu, Vice President of Finance with EQ3 Ltd. "Flexiti's consumer-focused financing platform complements our commitment to provide a balance in both high-quality crafted home decor and affordability." Flexiti's mobile, fully automated and 100% paperless process allows customers to apply for a private label credit card usable within the Flexiti network at more than 3,500 retail locations across Canada. This industry-leading solution offers EQ3 a quick and easy way to drive increased sales while making purchases more affordable for customers through flexible payment plans with low interest options.

"We're thrilled to add EQ3 to our rapidly-growing roster of retail partners," said Peter Kalen, Founder and Chief Executive Officer of Flexiti. "We're confident our technology solution will bolster sales and build brand loyalty at EQ3 as it has for so many in our network."

Flexiti Financial is a Member of ACT Canada; please visit https://flexiti.com/

24. ORACLE BOOSTS BLOCKCHAIN EFFORTS

Source: PYMNTS (2/13)

Tech giants such as Oracle and IBM are expanding their features and scope of blockchain projects, with an eye on financial and logistics capabilities. Elsewhere, social media firms such as Facebook are scaling hiring efforts in the blockchain as cryptocurrency prices crash. The movement to embrace blockchain — notably, among some tech giants — has gotten some momentum in recent days, with new announcements of projects going live.

Oracle said on Tuesday (Feb. 12) that it has as many as a dozen enterprise clients using a cloud-based blockchain platform that went live in the summer of 2018. Amid the offerings, the platform helps users with development tools and data integration. Customers using the blockchain platform include the Global Shipping Business Network, which tracks cargo (the consortium includes five carriers); China Distance Education Holdings, focused on educational certificates; and SERES, which works with eDocuments, including invoices. As reported in CoinDesk, other clients at the production stage include a range of financial firms and regulatory agencies, such as Arab Jordan Investment Bank, Nigeria Customs and Certified Origins.

The site noted that, up until then, enterprise blockchains in production had relied on the IBM blockchain, and had been geared toward trade finance. In an interview with CoinDesk, Frank Xiong, group vice president of blockchain product development at Oracle, said, “Other vendors may still be experimenting, but we do have real customers in live production. I would say around 10 to a dozen are in a live situation.” He told the site that “in production” means the Oracle applications have end users in place, and are handling live transactions. Transaction numbers are on the rise.

“To start with, we were seeing transactions probably among hundreds an hour. But [we] are expecting many of them to grow to thousands of transactions per second,” he said. As CoinDesk noted, the shipping consortium exists as a competitor to IBM and Maersk’s TradeLens, which also focuses on shipping. IBM, for its own part, said its Canadian unit is partnering with pharma firm Boehringer Ingelheim to use blockchain for clinical data and record-keeping. The companies said in a press release that they are testing whether using blockchain can reduce costs, and boost data transparency and integrity.

Dr. Uli Broedl, VP of medical and regulatory affairs for Boehringer Ingelheim Canada, said in a statement accompanying the news that “the clinical trial ecosystem is highly complex, as it involves different stakeholders, resulting in limited trust, transparency and process inefficiencies without true patient empowerment.”

Crypto Losses To Mean Blockchain Gain?

Separately, CNBC reported that the drop in crypto prices translates to what seems like a bit of shift in the job market. Some blockchain startups are laying off workers as funding is harder to come by, and as proven use cases seem, thus far, out of reach. That means that, in some cases, employees are in the market. That may be of benefit to companies like Facebook, which confirmed to the site that it has hired a “handful” of employees. Though the social media giant did not confirm which firms (or employees) made leaps to Facebook’s ranks, CNBC noted companies such as Chainspace, a crypto startup that now has two founders listed as Facebook employees. At least one observer has seen blockchain as a threat to Facebook: RBC Internet Equity Researcher Zachary Schwartzman wrote that the internet is at the “embryonic stages of a potential massive paradigm shift” to public blockchains.

RBC is a Member of ACT Canada; please visit ***https://www.rbc.com/***

25. GLOBAL CYBER ALLIANCE AND MASTERCARD LAUNCH CYBERSECURITY TOOLKIT TO ENABLE SMALL BUSINESSES TO STAY PROTECTED

Source: MasterCard (2/19)

The Global Cyber Alliance (GCA) and MasterCard today released a new Cybersecurity Toolkit specifically designed for small and medium businesses. This free online resource is available worldwide and offers actionable guidance and tools with clear directions to combat the increasing volume of cyberattacks.

GCA Toolkit

Some estimates indicate that 58 percent of cyberattacks are targeted against small businesses. These attacks include phishing, malware and ransomware – all of which can have devastating financial consequences. According to the Organisation for Economic Co-operation and Development (OECD):

- Small businesses account for 99 percent of businesses globally, including businesses in the US, EU, and the UK.
- Small businesses account for 70 percent of jobs, on average.
- Small businesses generate more than half of the value added by most economies.
- Resourcing small businesses with tools to protect themselves from ever-evolving cyber risks not only strengthens their individual businesses but also supports the health of the entire commercial ecosystem, including governments and larger companies. Helping these small businesses be more secure by taking a few reasonable steps will significantly reduce risk for both the small business and its partners, no matter their size or resources.

The GCA Cybersecurity Toolkit arms small business owners with basic security controls and guidance, including:

- Operational tools that help them take inventory of their cyber-related assets, create and maintain strong passwords, use multi-factor authentication, perform backups of critical data, prevent phishing and viruses, and more
- How-to materials, such as template policies and forms, training videos, and other foundational documents they can customize for their organizations
- Recognized best practices from leading organizations in the industry including the Center for Internet Security Controls, the UK's National Cyber Security Centre Cyber Essentials, the Australian Cyber Security Centre's Essential Eight, and MasterCard

"What sets the Global Cyber Alliance Cybersecurity Toolkit apart is that it is an action kit," said Philip Reitinger, president and CEO of Global Cyber Alliance. "Our focus is on producing a dynamic clearinghouse of operational tools that help small and medium businesses address risk and improve their cybersecurity posture, leveraging the deep expertise of our network of global partners, such as MasterCard, and the experiences of actual GCA toolkit users." As a Development

Sponsor, MasterCard has shaped the priorities and early success of the GCA Cybersecurity Toolkit, helping to make it accessible to millions around the globe.

“Safety and security are core to our brand,” says Ron Green, chief security officer, MasterCard. “Every day, we are committed to developing new and better ways to keep payments safe – especially for small businesses, the lifeblood of any economy. By partnering with the Global Cyber Alliance, we’re helping entrepreneurs and business owners to better protect themselves. In that way, they can stay focused on what they do best: running and growing their business.” The Global Cyber Alliance has partnered with several additional organizations to create the GCA Cybersecurity Toolkit, including the Center for Internet Security, the Cyber Readiness Institute, the City of London and the City of New York. The toolkit will also be regularly updated with input from users, industry experts, and public and private partners across the globe.

“I applaud the deployment of a cyber toolkit for small and medium businesses. This support is of critical importance to help smaller organizations effectively deal with increasingly complex and more frequent cyber threats,” said John Gilligan, president and CEO of the Center for Internet Security. City of London Police Commissioner Ian Dyson said, “As the national lead force for fraud and a founding member of the Global Cyber Alliance, we are always pleased to see new initiatives that will assist businesses in improving their cyber security. Businesses lost £6.7 million as a result of social media and email accounts being compromised between April and September 2018. It’s therefore essential that we, as a force, continue to work closely with businesses as well as the organisations that serve to protect them.”

“When we launched the Global Cyber Alliance we set out to empower organizations of all sizes with the tools they need to prevent cybercrime. The Global Cyber Alliance’s free Cybersecurity Toolkit provides small- and medium-sized businesses with immediate, concrete steps to protect their companies and customers against crippling cyberattacks, and I thank each of the public and private partners who contributed their world-class expertise,” said Cyrus Vance, Jr., Manhattan District Attorney.

“NYCEDC is proud to partner with the Global Cyber Alliance on the Cybersecurity Toolkit to better educate small businesses about the risks of cyberattacks. Small businesses play a critical role in New York City’s economy and represent an underserved customer base for cyber education and technologies,” said Nicholas Lalla, project lead for Cyber NYC, at the New York City Economic Development Corporation (NYCEDC).

Cyber NYC is a $100 million public-private investment to build a vibrant and inclusive cybersecurity ecosystem. On November 1, 2018, the NYCEDC launched their Cybersecurity Moonshot Challenge, asking the industry to develop and deliver affordable and scalable cybersecurity solutions for small businesses. As part of their partnership with the Global Cyber Alliance, finalists will be considered for inclusion in the GCA Cybersecurity Toolkit. New York City will promote the free toolkit to New York City businesses through NYC Secure.

Managing Director of the Cyber Readiness Institute Kiersten Todt said, “The Cyber Readiness Institute is so pleased to support and collaborate with the Global Cyber Alliance on helping small businesses reduce their cyber risk. Our approaches are complementary, and our partnership highlights the importance of integrating the multiple cybersecurity efforts that exist to ensure efficiency and effectiveness for small businesses. I look forward to what our organizations will achieve together.” The Global Cyber Alliance will expand the Cybersecurity Toolkit to help other sectors address the changing cyber threat landscape. Additional launches are planned this year with support from the District Attorney of New York, Craig Newmark Philanthropies, Corporation of London, Center for Internet Security and others.

To access the GCA Cybersecurity Toolkit, visit
https://gcatoolkit.org/smallbusiness.

MasterCard is a Member of ACT Canada; please visit
https://www.mastercard.us/en-us.html

26. CITY OF MARKHAM AND BELL PARTNER FOR SMART CITY INITIATIVE

Source: ITbusiness (2/7)

The City of Markham has announced plans to integrate Bell’s Smart City platform, a collection of interconnected Internet of Things (IoT) sensors and technologies. Markham will use the platform’s IoT applications to monitor a range of infrastructure functions including equipment tracking, water leak detection, storm/flood monitoring, weather monitoring, and energy management. The data will be used for environmental studies and efficiency improvements, the city said Wednesday. One such benefit could be early flood warnings. For example, Richmond Hill uses sensors to monitor its stormwater pond and warn its city workers in case of an overflow. Similarly, Seattle flood monitoring stations can send SMS alerts to nearby property owners when it detects dangerous water levels. Another is preventing water loss from leakage. According to a Bell report, 20 per cent of treated water is lost to leaking pipes. Early detection and repairs could minimize water loss, service discontinuity, and road erosion. Markham mayor Frank Scarpitti described Markham as the “living lab” and an “incubator for innovation” in the heart of Canada’s innovation corridor that spans the Toronto region and Waterloo.

“By embracing smart city technologies, we will continue to deliver exceptional services to our residents at lower costs and improve the quality of life,” he said in a statement. “This partnership with Bell speaks to Markham’s commitment to leveraging the latest digital tools and assets; keeping us connected in an age of great transformation while reinforcing Markham's position as a municipal leader in the heart of Canada's innovation corridor." Gary Semplonius, Bell senior vice-president, said the city's critical infrastructure and services will operate more efficiently through the Bell Smart City platform.

"We're proud to partner with Markham to extend the City's technology leadership in the management of municipal operations and enhanced delivery of city services," he said. To keep tabs on the sensors and collected data, Bell is working with IBM Canada to create a centralized management solution. In addition to Markham, Bell is partnering up with the City of Kingston to provide energy management and digital kiosks. The digital kiosks can provide Wi-Fi hotspots and cellphone charging stations in public areas.

27. CENTRAL 1 LAUNCHES INTEGRATION FOR SECURE DIGITAL SOLUTION FOR FINANCIAL INSTITUTIONS

Source: Central 1 (2/5)

Central 1 today announces the launch of technology that allows financial institutions to offer SecureKey ConciergeTM, a single sign-on authentication service, to their members. The seamless integration of Central 1's product means financial institution customers can access additional online services using their existing digital banking credentials, providing fewer complex logins to remember and simplifying login access for over 80 government websites. Vancity credit union and Conexus Credit Union are launching the integration of SecureKey Concierge into their systems, providing the convenient and secure service to their members.

"Canadians have come to expect new digital products and services that make their lives easier and, once again, Central 1 is proud to be delivering just that with SecureKey Concierge integration for financial institutions," says Mark Blucher, President and CEO of Central 1. "We're pleased to be launching the service with Vancity and Conexus credit unions and bringing increased security and ease to their customers." SecureKey, a globally renowned Canadian company with over 10 million Canadian users, provides a secure digital ID solution that is not only easy to adopt and use, but has proven capabilities in keeping incidents of phishing fraud at bay. Using a TRIPLE-BLINDTM configuration, SecureKey has integrated heightened security measures to ensure that unintended parties are not privy to users' sensitive or personal information. Central 1 developed the product to simplify the integration of SecureKey Concierge for credit unions and financial institutions. By building the technology to allow a seamless connection to SecureKey Concierge, it enables financial institutions to offer this service to their customers without needing to develop any software.

"We're pleased to have worked with Central 1 to develop this product, which not only benefits our members by making life easier and saving them time, but also helps the wider credit union community access an important digital service," says

Atul Varde, Senior Vice President of Digital Solutions and Business Technology at Vancity.

“The launch of SecureKey Concierge brings new digital functionalities right to our members’ fingertips, while making their online life safer and easier,” says Conexus’ Chief Digital Officer, Jeremy Trask. “We are continually looking for ways to serve our members’ needs and provide solutions that are timely and relevant. SecureKey Concierge enables just that for our members, especially with tax season just around the corner.”

Central 1 and SecureKey Technologies are Members of ACT Canada; please visit https://www.central1.com/ and ***https://securekey.com/***

28. DIGITAL SERVICES AND THEIR IMPACT

Source: PYMNTS (2/15)

From getting an entertainment fix on Netflix and finding new artists on Spotify to making the commute to work with Lyft, consumers are gradually turning to digital services to fill their personal needs.

That spike in digital offerings has come with increased competition, though. Card volume for on-demand, live-streamed and game or software content increased by 35 percent between 2017 and 2018, according to a First Data SpendTrend report. Regular retail experienced just 14 percent growth year-over-year, suggesting on-demand is fast emerging as a developing segment for digital commerce brands. Overall, transactions for digital goods and services are growing at 45 percent, according to FDC estimates, with on-demand services, games and software two of the fastest areas for this growth. Customers are not only becoming more comfortable with viewing content from on-demand and streaming services, but also actively paying for it. Spending on digital goods and services is responsible for $90 billion in U.S. TPV, or about 20 percent of online retailing, according to FDC estimates. This is essential to keep in mind as providers compete with both online content platforms — like the ever-present Netflix — and those like YouTube, which has long relied on a “freemium” model to capture users and boost subscriptions. The key to success is making the payment as frictionless as possible.

Consumers’ attachment to their smartphones means they more frequently turn to mobile devices for content instead of larger screens. Most ads are now viewed on smartphones rather than laptops, tablets or TVs, according to a Comcast report, and 60 percent came from smartphones in Q4 2018 compared to 44 percent the year before. The study found online ad views rose by 26 percent in this same period. Consumers are also showing interest in streaming all types of content, from live events to on-demand shows. This makes streaming a key focus area for advertisers as traditional channel viewing wanes. Ad views for live-streamed content account for 33 percent of total views, up from 23 percent in 2017. This suggests that more customers are turning to digital platforms for live programming.

Notably, certain platforms — like Netflix — still don't have ads, a hotly debated topic as the firm continues to fiddle with its business model.

Viewers now expect more on-demand and streaming options, too. Platforms like Netflix, Hulu and HBO still boast large viewership, but are beginning to allow other providers to share their content on outside streaming platforms. This strategy allows consumers to find the content they crave through a variety of outlets, while also enabling subscription services like Netflix to capitalize on licensing fees. Even legacy television providers are muscling into the on-demand arena, with NBC Universal looking to launch its own ad-supported streaming platform in early 2020. The Comcast subsidiary has access to a large pool of content, including shows that appear on Hulu — in which Comcast has a 30 percent stake. The service will also provide users a tiered ad or ad-free approach, like YouTube's own free versus paid offerings, with the ad-free option presumably more expensive.

As on-demand's popularity grows and customers begin to change how they interact with such platforms, businesses and streaming service providers seem to be rethinking their content approaches. Some companies, like Samsung, are using their resources and infrastructure to quickly capitalize on the niche's growth. The technology firm has announced it is launching its own platform in the Middle East and North Africa (MENA), a region currently seeing high on-demand content growth. Revenues totaled $523 million there in 2018, a 21 percent increase over 2017 figures. Samsung will be working with three established local providers to break into the market, rather than crafting its own platform from scratch. Other providers are starting over as on-demand content becomes more difficult to produce, market and maintain. Many are having a tough time adapting to the segment's rise, including those that originally saw success with the model.

AT&T supports the DirecTV on-demand service, for example, but is now considering selling the platform despite initially using it to grow usership. The telecommunications company would create another streaming service following said sale, offering on-demand content from HBO, Warner Bros. and Turner and effectively rendering the DirecTV platform obsolete. It's clear the on-demand space is growing to encompass the digital content with which users interact. What's less clear is which providers will be able to evolve and maintain the highest usership, particularly in a world that sees customers only getting more, well, demanding. One thing is certain, the winners in the market for on-demand services will make payments seamless, frictionless and global so that they completely fade into the background of the overall experience.

29. G+D MOBILE SECURITY TO ACCELERATE THE IOT BUSINESS THROUGH COLLABORATION WITH ARM

Source: G+D Mobile Security (2/25)

G+D Mobile Security integrates AirOn eSIM management solution with Pelion IoT platform for quick and secure IoT device onboarding. Giesecke+Devrient (G+D)

Mobile Security has agreed on a cooperation with Arm to provide GSMA-compliant remote provisioning and management of mobility provider data and the ability to transfer IoT device profiles using eSIM. AirOn was developed by G+D Mobile Security to secure the lifecycle management of eSIMs and complies with the remote provisioning specifications for SIM data defined by the GSMA.

G+D Mobile Security's eSIM management solution enables secure activation, provisioning, management and deactivation of eSIM profiles on mobile devices. Key components of G+D Mobile Security's AirOn offering are its SM-DP (Subscription Manager - Data Preparation) and SM-SR (Subscription Manager - Secure Routing) services. These services will enable Arm not only to onboard mobile network operators worldwide and provide subscriptions, but also to download and activate profiles through the Arm® Pelion™ IoT platform.

The combined solution by G+D and Arm offers a secure, efficient and interoperable remote management of IoT devices. Another benefit is easy scaling of IoT environments, as new devices can be directly connected and provisioned via the mobile network (over-the-air). Furthermore, secure re-provisioning is guaranteed over the entire lifecycle of the IoT devices through the Pelion IoT platform. This continues to accelerate the adoption of eSIM for IoT.

“G+D Mobile Security is a key eSIM partner in our mission of providing organizations with flexible and secure solutions and remote SIM provisioning options to quickly and securely connect, onboard and provision their IoT devices at scale,” said Nigel Chadwick, general manager of connectivity, IoT Services Group, Arm. “With our combined expertise, manufacturers of IoT devices now have access to an expanded ecosystem for the use of connectivity services from mobile network operators."

"As the Internet of Things grows exponentially, connectivity is becoming increasingly important for almost every industry. There is no way around eSIM to meet the increasing demand for flexible and global connectivity," emphasizes Carsten Ahrens, CEO of G+D Mobile Security. "With our market-leading eSIM management solution, we are in a strong position. The fact that G+D Mobile Security is now also an Arm partner is both a confirmation and an incentive for us to further expand our innovation leadership in this area.”

G+D Mobile Security will showcase its solutions at the Mobile World Congress at Stand 7A41 in Hall 7.

G+D Mobile Security is a Member of ACT Canada; please visit https://www.gi-de.com/en/ca/

30. GEMALTO LAUNCHES ONE-STOP SERVICES PLATFORM TO DIGITALIZE MOBILE SUBSCRIBER ENROLLMENT

Source: Gemalto (2/25)

- Trusted Digital Identity Services Platform addresses the multiple challenges of streamlining customer onboarding
- Draws on Gemalto's extensive portfolio of proven identity technologies, including biometric authentication
- Enables efficient and convenient capture, verification and digitalization of customer data
- Trusted Digital Identity

Amsterdam, 25 February 2019 - Gemalto announces today its Trusted Digital Identity Services Platform, which orchestrates everything needed by mobile operators to digitalize customer enrollment, including the capture, verification and authentication of customer credentials and biometrics. Drawing on Gemalto's in-depth experience and expertise in these fields, as well as complementary services from trusted partners worldwide, the platform enables streamlined customer enrollment, both in-store and online. With Gemalto Trusted Digital Identity Services Platform, mobile network operators (MNOs) can address challenges such as compliance with anti-fraud regulations as well as the need to implement far more efficient processes for customer enrollment. Solutions can be tailored precisely to the specific requirements of each individual MNO, and its subscribers. The first stage is to capture the customer's personal details, using supporting evidence from a diversity of ID documents or other types of customer credentials, along with biometrics, including fingerprints and facial capture with liveness detection. Relevant personal details are extracted automatically from the customer's documents, speeding the process of form filling and minimizing any risk of errors. All the captured information is verified in real time using Gemalto Trusted Digital Identity Services Platform and, if required, third party checks can also be integrated. With the customer's details authenticated, the enrollment is completed with the creation of a Trusted Digital Identity that provides customers with seamless and secure access to new services. This 'create once, use many times' model means that MNOs can continue to improve customer experience.

"Anti-fraud regulations, the search for more streamlined processes, and customer expectations of convenient experience across all onboarding channels are driving the trend for digitalization of customer enrollment, ," said Guillaume Lafaix, senior vice president Embedded Software, Mobile & IoT Services at Gemalto. "What sets Gemalto apart is our ability to orchestrate a highly personalized solution, capturing the identity characteristics required by each particular MNO, addressing relevant legislation, and integrating all the technologies and services needed."

Gemalto is a Member of ACT Canada; please visit https://www.gemalto.com/

31. HOW INNOVATIVE MPOS IS PAVING THE WAY TO A SELF-CHECKOUT FUTURE

Source: PYMNTS (2/4)

To serve customers who want to shop in stores and online, retailers and solution providers are working to offer a unified retail experience across multiple channels. They aim to help shoppers move seamlessly from browsing a merchant's website to perusing the aisles of brick-and-mortar stores through shared carts and other digital payment experiences. In some cases, brands like Loblaw and Nike are letting shoppers use their mobile phones to pay for their purchases at their physical stores. According to the latest PYMNTS mPOS Tracker, almost two thirds – or 63 percent – of retailers plan to offer this option within the next three years.

For retailers that struggle to maintain a seamless experience through multiple channels, solution providers are rolling out new tools such as software development kits (SDKs). From Dollar General to Roche Bros., these are some of the ways that retailers are integrating cross-channel POS experiences into their stores: More than six in 10 — or 63 percent — of North American retailers plan to provide mPOS solutions that leverage customers' own mobile devices within three years. Last year, Dollar General rolled out a new mobile app that enables customers to scan and pay for items in the store using their smartphones. The app, which was released in May, is available in Apple's App Store and on Google Play. Shoppers scan their selections as digital coupons are automatically applied, and can pay by scanning a quick response (QR) code at a dedicated checkout tablet at the front of the store. Customers bag their purchases at a checkout station, and a receipt is available through the app or via email.

The projected value of the global POS software market by 2024 is said to be $30.9 billion. And retailers are integrating new POS solutions into their brick-and-mortar stores: Toshiba Global Commerce Solutions recently announced that its TCx™ 300 system would arrive in all of Roche Bros.' Massachusetts locations. To begin the process, the retailer was said to bring 100 POS systems and accompanying TCx displays into seven of its stores. By March, 200 additional lanes are set to arrive at the company's other 13 stores. Roche Bros. Chief Information Officer John Lauderbach said in a press release in early January, "Our adoption of the company's premium point-of-sale technology has already proven successful by enabling faster, more frictionless transactions for both our associates and customers." The approximate value of Fiserv's stock-based acquisition deal for First Data was $22 billion. The deal, which was announced by the company in January, marked a landmark occasion in the FinTech sector. Fiserv CEO Jeffery Yabuki was set to be CEO of the merged firms. In addition, First Data CEO Frank Bisignano was set to be president and COO. The firms said in a statement at the time that end users would benefit from a "highly complementary combination" that offers a range of payments and financial services spanning integrated payments, account processing and digital banking, as well as the Clover POS system, among other offerings.

Almost six in 10 — or 56 percent — of consumers are more likely to shop at a retailer that enables them to share a cart across channels. The finding was reported by Boston Retail Partners in its 20th annual POS/Customer Engagement Benchmark Survey. Moreover, the survey found that half of consumers indicated they would probably let merchants save their preferences, personal history and personal details in the event that the process would help give them individualized deals and an easier checkout. BRP Senior VP and Practice Lead Perry Kramer said, according to the reports, “As customer expectations for an increasingly customized experience increase and evolve, retailers are adopting new ways to identify customers and personalize their shopping journey.”

And nearly three quarters — or 73 percent — of consumers want self-service technology, such as self-checkout. Online furniture startup Tudecora is taking clerk-less commerce into its store in Madrid, Spain. To gain access to the store, shoppers log into the retailer’s app and ask for entry to the space. After the company reviews the request, its system generates an “open” message that unlocks the shop. When a customer is ready to make a purchase, the store guides them to a set of custom touchscreens that will walk them through the purchase process. The shop, which is unstaffed, is open at all hours of the day and on holidays. (The furniture itself is protected by an array of sensor technologies and security cameras.)

From Tudecora to Dollar General, retailers with brick-and-mortar locations are creating new cross-channel experiences with the help of mPOS technology. And these implementations are not limited to retailers with physical stores: As consumers turn away from cash, mobile retailers such as food trucks are also turning to POS technology, as they head into a future of digital payments.

32. NEW APP LETS USERS TIP ON TWITTER WITH BITCOIN

Source: PYMNTS (2/18)

Twitter users can now send small bitcoin transactions as a tip if they like a tweet, according to reports. A new app called Tippin has been released as a Chrome extension, and is currently available to the browser’s users. The app lets people send bitcoin payments over the Lightning Network, which is an instantaneous and inexpensive way for people to send and receive bitcoin. The Lightning Network is a way to make bitcoin transfers and transactions easy and manageable at a large scale. Although it was originally developed for bitcoin, the network can also be developed for use with other cryptocurrencies.

When someone enables the extension, a lightning bolt logo will appear inside every tweet, next to the “like” and “retweet” buttons. The app builds on the idea of one of bitcoin’s main selling points: sending small payments to other people. Sergio Abril, a Tippin engineer, said the app is incredibly user-friendly. “In my opinion, tipping is going to be incredibly popular with the lightning network,” he said. “It’s the first time we can send small amounts at no cost, and we can do it incredibly fast.” All someone needs to use Tippin is a Twitter account.

“Tippin started as a personal side project a couple months ago, so I could understand Lightning Network a bit more, and or course help push adoption, but it’s starting to get big,” Abril said. There are plans for Tippin’s future, too. Abril said he wants to eventually add support on other social media platforms. Right now, the app is custodial, meaning users don’t completely have control over their funds, which makes the app much easier to use. However, non-custodial options are not off the table.

“Of course, Lightning Network itself is still in beta,” Abril noted. “So we have time to make this happen until it’s fully ready.”

33. PATRIOT SOFTWARE EASES DIRECT DEPOSIT PAYROLL ONBOARDING FRICTION

Source: PYMNTS (2/19)

Payroll and accounting software company Patriot Software is addressing the friction of onboarding employees to receive wages via direct deposit. In an announcement on Monday (Feb. 18), Patriot Software said it is rolling out Patriot Direct Deposit, a way to streamline employee onboarding to direct deposit via standard four-day ACH or bank wire transfers.

“Patriot Direct Deposit streamlines the onboarding process for our customers,” said Patriot Software Operations Manager Michael Streb in a statement. “The entire onboarding process is completed within our web-based software application, and is entirely paperless. Reducing the time it takes to complete the direct deposit process has resulted in a much smoother onboarding experience, which our customers love.” The solution is now integrated into Patriot Software’s existing Basic Payroll and Full Service Payroll tools, the company noted. Furthermore, it plans to add direct deposit onboarding functionality in the year’s second quarter for employers that hire on-demand workers and contractors.

While direct deposit is a popular payroll method for employers, paper checks also remain commonplace. In 2016, Patriot Software introduced a feature that allows businesses to use black check stock to print their own payroll checks, a signal that payroll service providers must also adhere to companies’ demands for legacy payroll tools. In an interview with PYMNTS at the time, Streb explained that customers had continually requested the service, pointing to the “unbankable” employee segment.

“There is a segment of people who can’t get bank accounts, and there is also a segment of people [who] don’t trust banks. They’d rather take a check to a cashing place or Walmart and have cash in-hand,” he said. However, demand for paper checks is likely declining. PYMNTS data published last year found that 53.7

percent of employees prefer direct deposit as their top preference when it comes to receiving wages, with more than 14 percent noting they are dissatisfied with paper checks.

34. RUSSIA'S TWIST ON CYBER MONDAY

Source: Worldpay (1/24)

Russian retailers are putting their own twist on a Western shopping tradition.

The original Cyber Monday follows the US Thanksgiving weekend. In the West, Cyber Monday caps the weekend that begins with Black Friday and represents one of the year's biggest shopping periods globally. Retailers often offer deep discounts to lure shoppers in hopes of having a strong start to the holiday season. Since its beginning in 2005, Cyber Monday has grown to become one of the biggest days on the global eCommerce shopping calendar. In 2018, Cyber Monday was the single largest shopping day in history in the US with online sales topping $7.8 billion. Cyber Monday has spread throughout the Americas and Europe with more local and global eCommerce retailers offering sales and specials. Russian Cyber Monday falls on the last Monday in January.

"Worldpay's 2018 Global Payments Report estimates total Russian eCommerce turnover of $38 billion for 2018" Unlike the holiday kickoff event in the West, Russian Cyber Monday is a post-holiday sales event. In Russia, the first ten days of the year are celebrated as the New Year's holiday, including Russian Christmas that's celebrated on January 7. The annual event aims to boost sales following the busy pre-holiday shopping season and the extended holiday itself. The first Russian Cyber Monday was held in 2013 and was organized by the Russian Association of Internet Trade Companies, the AITC. The 2019 event on January 28 will see deep discounts offered by many of the largest eCommerce sites operating in Russia including Ulmart, Media Markt, M.video, Eldorado, and Detsky Mir.

Overall eCommerce still represents a relatively small percentage of the Russian economy, about 3%. Yet the opportunity for online sales in Russia is growing. Worldpay's 2018 Global Payments Report estimates total Russian eCommerce turnover of $38 billion for 2018. The report projects a 9% eCom compound annual growth rate, projecting a $54 billion market opportunity by 2022. A 2018 report by Morgan Stanley included a similar estimate of $52 billion by 2023. In addition to its growing size, the Russian eCommerce market is notable for its lack of single dominant retailer. Russians have their own twists on payments as well. Russians prefer debit and credit cards when shopping online, with Central Bank of Russia's Mir system competing with global brands like Visa and MasterCard. The use of alternative payment methods are growing in Russia. Led by eWallets like Yandex.Money, WebMoney and Qiwi, alternative payments accounted for 24% of Russian eCommerce sales in 2018 according the 2018 Global Payments Report.

MasterCard and Worldpay are Members of ACT Canada; please visit https://www.mastercard.us/en-us.html and https://www.worldpay.com/global

35. ALPHABET SEEKS SHARE OF TAXES FOR TORONTO 'SMART CITY'

Source: PYMNTS (2/15)

To create a smart city on the waterfront of Toronto, Alphabet's Sidewalk Labs is reportedly looking for a share of development fees, increased land value and property taxes for the project in the Canadian city. The funds would reach roughly $6 billion over a period spanning three decades, CNBC reported. Sidewalk Labs CEO Dan Doctoroff told The Toronto Star newspaper of the project, "We're going to be spending a lot of money in advancing the infrastructure." He added, "And where we do that and there are new property tax revenues or developer charges, we only want to get paid back a reasonable return for our investment in that infrastructure."

The organization reportedly is seeking to finance projects such as waste removal and a Toronto light rail addition. However, Doctoroff told the news outlet that the light rail would still be a public entity with the addition. He also told the paper, "This is a way of actually enabling critical infrastructure that isn't happening. What we hope to do is accelerate the development of this whole area by years and years." The news comes after Toronto development officials signed a development agreement involving a "smart city" concept backed by Alphabet. A government-created organization focused on the renewal of the city's waterfront called Waterfront Toronto is also involved in the project. According to reports last year, the two entities call for the "revitalization of Quayside, located at Lake Shore Boulevard East and Parliament Street in Toronto."

Sidewalk Labs' role is to bring smart-city technology to the mixed-use development — enhancements such as robotic garbage collection and self-driving vehicles as well as sensors to monitor when pedestrians want to cross streets. If the development proves to be successful, it could reportedly provide a model for sustainable urban neighborhoods — as well as showcase how Alphabet and its technology can bring that aim to fruition.

ACT Canada helps members understand complex issues and filter truth from market noise for current and emerging commerce trends. Through a consultative approach with all stakeholder groups, the association provides knowledge and expertise to help members leverage opportunities, confront challenges and advance their businesses. Please visit www.actcda.com or contact our office at 1 (905) 426-6360.

Please forward any comments, suggestions, questions or articles to andrea.mcmullen@actcda.com. Please note that articles contained in this newsletter have been edited for length, and are for information purposes only. If you would like to be removed from our newsletter distribution list please follow the unsubscribe instructions at the bottom of the email.

Andrea McMullen
President | ACT Canada
905 426-6360 ext. 124 **|**
andrea.mcmullen@actcda.com **|** www.actcda.com **|** http://ca.linkedin.com/in/andreamcmullen

ACT Canada helps members to:
Engage - Grow the commerce community via stakeholder contributions, collaboration and networking
Enable - Provide access to the expertise of the member community to gain insights that will help strategic decision-making
Evolve - Drive positive change in the increasingly complex commerce environment