Welcome to the **November** and **December** 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

20. ACCEO Tender Retail partners with system innovators

21. Apple just removed hundreds of fake shopping apps from the app store

22. Giesecke & Devrient and M2MD Technologies, Inc. form strategic relationship

23. VISA acquires CardinalCommerce to secure and push digital commerce

24. Ingenico Group to introduce its first android-based PoS at TRUSTECH

25. Samsung Pay first 'pay' to add system-specific rewards program

26. Cardtek and NXP collaborate to introduce digital payment solution for wearables

27. The weak link in the Omnicommerce Security value-chain

28. Societe Generale launches a next-generation card integrating a dynamic security code

29. Ingenico Group to launch its new mobile solution, the link2500, at TRUSTECH

30. Google Wallet adds P2P payments to web browsers

31. The fed prioritizes security as payments speed up

ACT Canada Partners

INGENICO - *Point of Sale Equipment Partner*
Ingenico Group is the global leader in seamless payment, providing smart, trusted and secure payment solutions to empower commerce across all channels, in-store, online and mobile. With the world’s largest payment acceptance network, we deliver secure solutions with a local, national and international scope in 125 countries. For over 30 years, we have been the trusted world-class partner for financial institutions and for retailers, ranging in size from small merchants to several of the world’s best known global brands. Our smart terminal and mobile solutions enable merchants to simplify payment and deliver their brand promise.

INTERAC - *Payment Network Partner*
Interac Association is a recognized world leader in debit card services. Interac Association is responsible for the development and operations of the Interac network, a national payment network that allows Canadians to access their money through Interac Cash at 60,000 Automated Banking Machines and Interac Debit at 766,000 point-of-sale terminals across Canada. Interac Flash, a secure contactless enhancement of Interac Debit allows Canadians to pay for items instantly with their Interac chip debit card at a reader that supports Interac Flash.

PAYMENTS BUSINESS - *Media Partner*

New and Renewing Members

Principal Member
CIBC ~ member since 2011
MasterCard Worldwide ~ member since 1999
Payments Canada ~ member since 1998
Walmart Canada Corp. ~ member since 2011
Verifone ~ member since 2012

General Member
4PAY Inc. ~ member since 2016
ICC Solutions Ltd ~ member since 2003
The North West Company ~ member since 2014
Vantiv Integrated Payments ~ member since 2011

Associate Member
Card Resource Group Inc. ~ member since 2010

Career Opportunities

Visit our career opportunities section for the latest opportunities - http://www.actcda.com/information/careers/

Looking for good people?
There is a lot of movement in the market, so if you are looking for new employees, we are always aware of some great people. Please contact ACT Canada for more details - postings@actcda.com

Calendar Of Events

Cardware 2017
May 1-3, 2017
Niagara Falls, Canada
www.cardware.ca
ACT Canada members receive discounts

Card Forum
May 8-10, 2016
Austin, TX, USA
www.cardforum.com
ACT Canada members receive discounts

Money2020 Europe
June 26-28, 2017
Copenhagen, Denmark
www.money2020europe.com
ACT Canada members receive discounts

Articles

1. EDITORIAL - DECISIONS, OPINIONS, PRIDE AND STUBBORNNESS

Source: Catherine Johnston, CEO, ACT Canada (12/09)

Decisions, Opinions, Pride and Stubbornness

We all make decisions based on what we know at the time, but none of us (OK – most of us) don't claim to know everything. When new information becomes available it can validate our earlier decision or cause us to change it. Many years ago I was in a closed door meeting with federal cabinet ministers. I criticized them for a decision they had made that did not sit well with Canadians. The senior minister present asked me, with more grace than I deserved, what I would have decided had I known specific information that had been available to caucus. He shared that information and I admitted, somewhat sheepishly, that I would have made the same one they did.

I learned two lessons that day. Never sit in judgement of other people's decisions unless you know what they knew at the time. I also learned that the mature thing to do is to change your mind if new information supports it. Opinions are just like decisions in this regard. This year we have been bombarded with opinions, many of them political and some of them business. We've seen people who, when provided with new information, have said, "I don't care, I'm not changing my mind". Whether it is caused by pride or stubbornness, taking that position speaks to the person's character. At best it is sad and at worst it is frightening.

One of the great promises that life holds is the possibility of continual learning. It makes life exciting and gives us a sense of hope. I only have five more editorials to share with you things that are important to me. If you know someone who struggles with this problem, please talk to them.

2. SAMSUNG CANADA PARTNERS WITH CIBC TO BRING MOBILE PAYMENTS TO CANADIANS

Source: CIBC (11/08)

Samsung Electronics Canada Inc. announced a partnership with CIBC to give its clients early access to Samsung Pay, a simple and convenient mobile payment service that works virtually anywhere you can tap or swipe your card1. This partnership marks the first time Canadians will be able to use the service, following successful launches in South Korea, the United States, Puerto Rico, Australia, China, Singapore, Spain and Brazil. "Samsung Canada and CIBC are both brands that value technology and innovation while enhancing the connected lives of Canadians," said Paul Brannen, COO and Executive Vice President of Samsung Electronics Canada. "Global adoption rates of Samsung Pay are extremely positive and the service has already seen tremendous success, redefining the way consumers pay and use their smartphones. We are excited to be partnering with CIBC to bring Samsung Pay to Canadians."

Samsung Pay has a strong alliance of partners and supports eligible credit and debit cards from more than 450 major global and regional banks. It is the most widely accepted mobile payment system and will be available for all CIBC VISA cardholders starting today2, on compatible Samsung smartphones, including the Galaxy S7 and Galaxy S7 edge, Galaxy S6, Galaxy S6 edge, Galaxy S6 edge+, and Galaxy Note5.3 This is the first step in bringing Samsung Pay to Canada and part of a larger roll-out strategy.

"We are continuously working to deliver the best mobile banking experience for our clients through strategic partnerships and innovation that meet Canadians ever-evolving digital needs," says Todd Roberts, SVP Innovation, CIBC. "We are proud to be the first in Canada to bring Samsung Pay to our clients, ensuring they have choice and convenience when it comes to mobile payments." Samsung Pay provides consumers with a seamless mobile payment solution that is designed for simplicity, security and convenience.

*CIBC is a member of ACT Canada; please visit www.cibc.com***.**

3. CPI CARD GROUP-CANADA INC. SELECTED BY ONTARIO LOTTERY AND GAMING CORPORATION AS MANUFACTURER FOR FIRST-EVER CANADIAN LOTTERY GIFT CARD PROGRAM

Source: CPI Card Group (11/22)

CPI Card Group announced that CPI Card Group in Toronto, Ontario was selected by the Ontario Lottery & Gaming Corporation (OLG) to produce more than 2.4 million lottery gift cards. The cards are part of the first-ever gift card program offered by a Canadian provincial lottery corporation and one of the first such programs offered in North America. CPI's proven track record and success providing high-quality product and services helped position CPI to gain the OLG contract. CPI will liaise directly with OLG to produce the closed-loop gift cards as part of OLG's efforts. Cards will be sold by more than 8,000 lottery retail locations province-wide and are redeemable for any lottery product, whereas those sold from gift card malls featured within mass retail stores can be redeemed for either LOTTO 6/49 or LOTTO MAX lottery games. In all cases, the cards provide a brand new experience for OLG's customers, allowing them to share the gift of lottery while enabling gift recipients to select and purchase their favorite lottery tickets.

"Our work for OLG demonstrates an area of CPI's strength, which is coordinating among many vendors to seamlessly produce and manage a high quantity of cards," said Steve Montross, president and CEO, at CPI Card Group. "OLG's new gift cards are a compelling way to deliver a convenience to customers that didn't previously exist." More information about OLG's gift cards is available on the company's website: http://www.olg.ca/lotteries/giftcards.jsp**.**

CPI Card Group is a member of ACT Canada; please visit www.cpicardgroup.com.

4. CARDTEK, DC PAYMENTS TO LAUNCH MOBILE PAYMENT SOLUTION IN CANADA

Source: Cards International (11/11)

Cardtek has collaborated with DC Payments to launch a new mobile payment solution for debit cards in Canada. The new offering, Mobile Services Manager (MSM), integrated with open wallets, will enable financial institutions' customers to make debit expenditures from a mobile phone without presenting a bank payment card. The integration of Cardtek's MSM solution into DC Payments card management ecosystem will allow the payment processor to offer secure contactless payment services to its banks customers. Cardtek said that MSM will allow advanced card credential management services, such as implementation and life cycle management - tuned for the major digital wallets available in the market. The payment solution will be available by the end 2017.

DC Payments managing director of Americas Adel Elassal said: "We are extremely pleased to use MSM as the foundation of our comprehensive digital credential enablement platform, 'DC Mobile.' MSM is designed to meet today's technology demands, while providing a broad based platform for an expanding set of future digital credentials. These credentials will be used for highly secure contactless payments through point of sale terminals, and support the new breed of in-app and secure ecommerce payments. Critically, the MSM allows our financial institution clients to engage in this new range of payment channels without the enormous in-house investment typically required," Elassal added. Cardtek executive vice president of sales and marketing for North America Emilian Elefteratos said: "We have great confidence that this partnership will bring new opportunities and benefits to DC Payments customers. Utilising our industry foresight and technical expertise, Cardtek continues to offer a dynamic competitive edge to our customers and partners."

Cardtek and DC Payments are members of ACT Canada; please visit www.cardtek.com and www.directcash.net.

5. 2016 WILL BE REMEMBERED AS THE YEAR WHEN DATA PRIVACY WAS KILLED

Source: Let's Talk Payments (11/22)

In vocal concerns over data privacy, the general public has already shaped a tradition of picking on usual suspects and condescending over constant tracking of everything possible and impossible. To be honest, those concerns are rarely exaggerated as the list of those suspects and under-the-sheets actions towards diluting personal data privacy are accelerating.

While industry standards and regulations tend to move towards greater ‘respect’ for personal privacy in response to increasing consumer disturbance over the issue, some companies, on the contrary, are accelerating their efforts in a more precise profiling and targeting of a user. Facebook has been one of the most contradictory examples, as the company dropped a bomb on the industry back in 2014 with the announcement that it will target ads based on the browsing histories of its users. Every page that a user visits, which has the “Like” button, sends data back to Facebook regardless of whether people ‘liked’ it or not. Given the scale of the user base, the scale of business presence and ever-expanding Facebook family apps, platform capabilities and acquired companies, the precision is about to get creepy.

Google is also an extremely complex topic when it comes to privacy. There is really nothing Google doesn’t know about a particular user. Still, apparently, there are no borders in how well can any company can get to know its customers. In August this year, for example, new research from Northeastern University’s professor Guevara Noubir and colleagues have demonstrated that Android apps can be manipulated to reach inside user’s mobile phone to track person’s whereabouts and traffic patterns, all without user’s knowledge or consent. “An app, in fact, does not need your GPS or Wi-Fi to track you,” said Noubir, the Lead Researcher behind the study. But even that is not as meaningful as something happened behind curtains this summer when Google quietly dropped the ban on personally identifiable web tracking. As reported by ProPublica at the end of October, Google literally crossed out the lines in its privacy policy that promised to keep its two pots of data (Gmail’s and advertising networks’ DoubleClick, which Google acquired in 2007) separate by default. The change is enabled by default for new Google accounts. Existing users were prompted to opt-in to the change this summer.

The practical result of the change, as explained on Slashdot, is that the DoubleClick ads that follow people around on the web may now be customized to them based on the name and other information Google knows about the user. It also means that Google could now – if it wished to – build a complete portrait of a user by name, based on everything they write in email, every website they visit and the searches they conduct. Google and Facebook were not random choices as examples. A recent study by Princeton University discovered that Google Analytics, a tool used to analyze Web traffic that integrates with ad-targeting apps, was embedded in nearly 70% of the sites. Along with Google, the leading trackers identified by the study were Twitter and Facebook.

Private data is at the cornerstone of the market power of mentioned companies, one of the most (if not the ultimate) valuable assets and important area of development and growth. As a result, players in bordering industries started pursuing their interest in stretching privacy borders to compete with data-rich market participants. Mobile operators/Internet providers are extremely close to contradictory private space invasion. Verizon/AOL, for example, just at the end of last week outlined its plans to combine offline information, such as postal address, email address and device type, with AOL browser cookies, Apple and Google advertising IDs and Verizon's proprietary unique identifier header. As reported by AdExchanger, Verizon's header will be inserted into web traffic sent to Verizon-owned companies, including AOL, and certain authorized partners. The identifiers will be used to serve more personalized advertising, connect app usage with web browsing activity and identify and link users across devices. Verizon will pass what it knows about device usage patterns to AOL to power more targeted, personalized advertising.

Not to be biased against Verizon, but it is worth mentioning that AT&T is getting into hot water over its latest 'spying' scandal (aka Project Hemisphere) and the announcement at the end of October that AT&T Inc. and Time Warner Inc. (which owns CNN, HBO, TBS and TNT, and much more) have entered into a definitive agreement under which AT&T will acquire Time Warner in a stock-and-cash transaction valued at $108.7 billion, including Time Warner's net debt. As noted by Free Press, "This merger would create a media powerhouse unlike anything we've ever seen before. AT&T would control mobile and wired Internet access, cable channels, movie franchises, a film studio and more. "That means AT&T would control Internet access for hundreds of millions of people and the content they view, enabling it to prioritize its own offerings and use sneaky tricks to undermine Net Neutrality." But that's not really the biggest issue – privacy is. Given that AT&T has experience in satisfying very particular requests from security agencies to find information on a particular person with regard to any case, an extension of data accumulation capabilities of AT&T means a whole new level of access to personal behavioral data.

"Where you go, what you watch, text and share, with whom you speak, all your internet searches and preferences, all gathered and 'vertically integrated,' sold to police and perhaps, in the future, to any number of AT&T’s corporate customers,” commented Amy Goodman and Denis Moynihan of Democracy Now! One of the hallmarks of the latest ‘updates’ in privacy policies is an attempt of companies to find a loophole to solve a long-standing problem – not just knowing what you do, but knowing who are you exactly. In other words, data tracking has been taken to a whole another level, where companies can connect one’s activity and cross-device behavior with a particular name and the real person. Previously, data management companies have been applying statistical analysis to make educated guesses about user identity, but with large technology companies taking it into own hands, there is really no secret anymore on who exactly does what.

If the extent of you not being in control over personally identifiable information is not scary yet, a really simple and paranoia-inducing tool, Clickclickclick.click has been just launched by VPRO, a Dutch media company, and Studio Moniker, an interactive design company, to show how one’s online behavior is constantly being measured by the browser. The website details person’s actions in real-time, from movements on the page to the other websites the person has visited, in the hope of creating awareness on privacy in a playful manner.

6. INGENICO GROUP, OBERTHUR TECHNOLOGIES AND VODAFONE JOIN FORCES TO REVOLUTIONIZE PAYMENT TERMINAL CONNECTIVITY WITH INGENICO CONNECTIVITY/MANAGER

Source: Ingenico (11/28)

Ingenico Group, OT (Oberthur Technologies) and Vodafone announced that they have been collaborating to define a disruptive connectivity management solution based on embedded Universal Integrated Circuit Card (eUICC). This partnership brings together the best of their know-how to revolutionize payment terminal connectivity in an agile way. By joining forces, Ingenico, Vodafone and OT will make the remote management of payment terminals' cellular connectivity a reality thanks to Connectivity/Manager. This tripartite solution leverages OT's eUICC and remote subscription management solution, Ingenico's smart terminals as well as Vodafone's global IoT communications platform, and eliminates all logistic constraints toward SIM management. Enabling both the remote installation and management of operator profiles, it will dramatically improve operational efficiency, and also enhance merchants' experience with better connectivity and ready-to-use payment terminal. This pioneering solution will provide unequalled quality of service and increase opportunities for acquirers & estate owners around the globe.

“We are delighted to work with Ingenico and Vodafone to optimize global connectivity management of POS during their entire lifespan. Our solution will also simplify the worldwide distribution of the POS and enable Ingenico to deliver an improved connectivity service to acquirers and merchants thanks to primary connectivity and back-up subscriptions hosted in the same eUICC. This will increase the transaction success rate by avoiding transaction failures related to temporary loss of connectivity" said Pierre Barrial, Managing Director of the Connected Device Makers activity at OT. "This is a strategic project for us, in line with our ambition to provide our OEM and MNO customers with the best solution to manage connectivity in a secure and flexible way across the variety of devices and equipment that constitute the Internet of Things."

"Ecosystems and partnerships are going to be critical in the continued success of IoT and I believe that this relationship will prove to be a powerful and successful one for the POS industry," highlighted Vodafone head of IoT Ivo Rook. "This solution will dramatically change the way terminals estate owners manage connectivity. Nowadays, ensuring a merchant's payment terminal is operational accounts for up to 17% of the overall terminal TCO. With this new solution, the payment terminal will embed a SIM that can be set and updated over-the-air. Thus estates will be managed more efficiently. Field services around SIM card logistics will become redundant, which will save estate owners time and costs while simplifying merchants' set-up," explained Jacques Guerin, EVP Smart terminals for Ingenico Group.

Ingenico Group and Oberthur Technologies are members of ACT Canada; please visit www.ingenico.com and www.oberthur.com.

7. MASTERCARD TO USE AI FOR FRAUD DETECTION

Source: Mobile Payments Today (12/02)

MasterCard has introduced Decision Intelligence, which the company described in a press release as a comprehensive decisioning and fraud detection service. The solution uses artificial intelligence technology to help financial institutions increase the reliability of the approval process for real-time transactions and reduce the number of false declines, according to a press release. This is the first instance of AI being implemented on a global scale directly on the MasterCard network, the company said.

"We are solving a major consumer pain point of being falsely declined when trying to make a purchase," said Ajay Bhalla, president of enterprise risk and security at MasterCard. "By using AI technology on our global network, we're helping financial institutions and merchants improve approval — and the consumer experience." The smart technology behind Decision Intelligence examines patterns of use for a specific account in order to detect normal and abnormal shopping and spending behaviors, according to the announcement. In doing so, it leverages account information such as customer value segmentation, risk profiling, location, merchant, device data, time of day, and type of purchase made.

MasterCard is a member of ACT Canada; please visit www.mastercard.ca.

8. CANADIAN PAYMENT METHODS AND TRENDS REPORT FINDS CASH IS KING, FOR NOW

Source: Payments Canada (11/16)

Payments Canada has released new research that reveals the changing payment behaviours of Canadian consumers and businesses. The Canadian Payment Methods and Trends (CPMT) report released today shows that cash and other paper transactions, such as cheques, are still leading, but in Canada new payment channels are a growing share of the market. These trends reinforce the need for Canada to adapt its systems as the global payments ecosystem changes, which is what Payments Canada is doing with its Modernization Initiative. “The Canadian Payment Methods and Trends report is an important window into the future of payments technology in Canada,” says Carol Ann Northcott, Payments Canada’s chief risk officer and vice-president of risk, security and research. “While paper-based payment methods continue to decline, emerging technology is shaping the Canadian payment landscape of the future.”

The CPMT research uncovered several trends between 2008 and 2015 that are relevant to Canadian consumers:

- In 2015, the payments market in Canada grew to 20.9 billion transactions, worth more than $8.9 trillion.
- Consumer demands for speed, convenience and rewards are driving many of the trends at merchant locations, including credit card, contactless (tapping your payment card or mobile device to pay) and e-commerce. In 2015, contactless payments grew by 70 per cent in both volume and value of transactions.
- Cash continues to account for the most transaction volume, but cash use is on a downward trend. Since 2011, cash use has declined by 20 per cent.
- Online transfers are the fastest growing, reaching an estimated 120 million transactions worth $45 billion in 2015.
- The use of cheques continues to decline with a 25 per cent decrease since 2011, but the value has been buoyed by continuing use by Canadian commercial enterprises, growing by more than two per cent on average each year.

Payments Canada is still in the early stages of its Modernization journey but we expect that changes to core payment systems will have an impact on the payment methods and trends in Canada. The journey to Modernization will result in faster, flexible and more secure transactions and the new core systems will serve a platform for innovation and the creation of new payments products. The CPMT report was compiled by Payments Canada with the help of payment service providers, payments consultants and researchers to help build comprehensive understanding of the Canadian payment landscape in 2015.

Payments Canada is a member of ACT Canada; please visit www.payments.ca.

9. WAL-MART PAY IN TALKS WITH SEVERAL MOBILE WALLET COMPANIES

Source: Reuters (11/07)

Wal-Mart Stores Inc is in talks with several mobile wallet companies to offer more payment options in its Wal-Mart Pay app, an executive at the world's largest retailer said, after signing up JPMorgan Chase & Co last week. Starting next year, Chase Pay will become the first third-party digital wallet on Wal-Mart's website and app, they said on Thursday. Customers can pay within the app with any major credit, debit, pre-paid or Walmart gift card.

Daniel Eckert, senior vice-president of services at Wal-Mart U.S., said in an interview late on Friday that the retailer would tweak its marketing for the app after the most frequent users turned out to be Gen X customers, born from 1965 to 1967, and baby boomers born from 1946 to 1964. "The target demographic during the launch of a technology product tends to be younger, more male, so we have had that target market in mind," Eckert said. U.S. mobile payments accounted for an estimated $67 billion in 2015, and are expected to grow this year to $83 billion, or 24 percent of all purchases made via smartphones, according to the latest Forrester Research data. Apple Inc's (AAPL.O) Apple Pay or Alphabet Inc's (GOOGL.O) Android Pay are the most popular digital wallets, and U.S. retailers have launched many mobile payment apps in the last two years. But acceptance has been slow, largely because most systems require new equipment at stores. Wal-Mart Pay was launched in December 2015 and can be used in all of the retailer's 4,600 U.S. stores. Customers at the checkout counter must choose the payment option within the app on their smartphone, and activate the camera to scan the code at the register. An e-receipt is sent to the app.

Eckert also said more than 90 percent of transactions on the app involve customers are using the service more than three to four times a month. He declined to give the overall number of users who use Wal-Mart Pay. Wal-Mart leads a consortium of U.S. retailers developing a mobile wallet app called CurrentC. The group, which includes Target Corp (TGT.N) and Best Buy Co Inc (BBY.N), said earlier this year it would delay launching the app after the project hit several roadblocks.

Walmart is a member of ACT Canada; please visit www.walmart.ca.

10. AMERICAN EXPRESS LAUNCHES NEW MOBILE CAPABILITY

Source: American Express (11/30)

American Express announces the launch of Amex Pay, a smart, secure, and simple way to pay using mobile contactless payments on eligible Android devices wherever American Express contactless payments are accepted. Amex Pay is available exclusively through the Amex App for eligible Consumer, Small Business and Corporate Cards issued by Amex Bank of Canada. "The launch of

Amex Pay is another example of our commitment to innovation and providing our Cardmembers with more ways to use their Cards," says Suat Alaybeyoglu, Vice President Consumer Acquisition & Management at American Express Canada. "Cardmembers can shop with ease using their mobile devices, while continuing to experience the service they've come to expect from American Express."

American Express, which has always been known for its exceptional service, is focusing its attention on taking that service to another level and reaching its mobile-first customers. This includes an increased focus on the Amex App (with revamped, new features, like Use Points for Purchases), and providing more options to pay with an American Express Card using a mobile device. The launch of Amex Pay allows American Express Cardmembers in Canada to shop with speed wherever American Express contactless payments are accepted using an eligible Android device. In addition, Cardmembers can rely on the trusted safety and security of American Express, whether they pay in-store with their eligible mobile devices or their plastic American Express Cards, or use their Card online. American Express' intelligent security systems can help detect fraud by spotting something unusual in a Cardmember's spending pattern, and our Fraud Protection Guarantee lets Cardmembers shop with confidence.

To get started, Cardmembers can simply activate an eligible American Express Card with Amex Pay on an eligible Android device by downloading or updating the Amex App.

Do More with the Amex App

In addition to enabling Cardmembers to make eligible purchases with an eligible Android device, the Amex App provides Cardmembers with simple convenience to access their account quickly, from virtually anywhere they go:

- Redeem Membership Rewards points for eligible travel and everyday purchases charged to the Card- right from the app.
- Manage accounts with customizable features such as payment due and statement ready alerts.
- View PDF statements and pending transactions
- Refer a Friend and you could earn a referral bonus on approved referrals using your phone.
- Enrolled Cardmembers can view and manage payments through American Express Installments.

For more information on Amex Pay please visit https://www.americanexpress.com/ca/en/content/mobile-app/

American Express is a member of ACT Canada; please visit www.americanexpress.ca.

11. SINGAPORE'S SMART NATION TESTS GIESECKE & DEVRIENT'S SEAMLESS SWITCHING CELLULAR TECHNOLOGIES

Source: Giesecke & Devrient (12/05)

Giesecke & Devrient have started the test in November this year with the Infocomm Media Development Authority (IMDA), Singapore. G&D is the lead contractor for the trial, and will provide IMDA with the test bed for Remote Provisioning of eSIM to IoT Devices. The trial will involve utility sensors belonging to the PUB, Singapore's National Water Agency. The trial started in November 2016, and will run for at least two months.

During the trial, G&D will install the eSIM in some of PUB's utility sensors, to replace existing SIM cards. These sensors will continue to collect field data and send it via the mobile network to PUB's server for monitoring and analysis. The Remote eSIM Management system will allow these sensors to be technically switched between mobile network operator (MNO) networks without direct physical intervention whenever required. One potential use is the switching of telcos networks upon expiry of the mobile network contract. All three local MNOs – M1, Singtel and StarHub – will participate in the trial, ensuring the highest level of network coverage during the process. G&D will be responsible for coordinating with all partners. The trial will also help IMDA better understand the capabilities and challenges of the Remote eSIM Management system.

Ms Aileen Chia, Assistant Chief Executive and Director-General (Telecoms and Post), IMDA, said, "The trial will explore the viability of using eSIMs to enable always-on, machine-to-machine communications without the hassle of having to physically replace SIM cards when switching operators." "This is the most advanced eSIM Management solution in the market and we are happy to support IMDA and the local telecommunications community to accomplish an important step towards realizing Singapore's Smart Nation vision", says Thomas Donle, Head of Sales Telecommunications at Giesecke & Devrient Asia. The project has the potential to have a lighthouse character for the region because one of the outcomes might be that regulation changes may be necessary.

Giesecke & Devrient is a member of ACT Canada; please visit www.gi-de.com.

12. FLEXITI FINANCIAL ANNOUNCES $5 MILLION SERIES A FUNDING

Source: Flexiti Financial (11/02)

Flexiti Financial, a leading provider of point-of-sale (POS) financing and payment technology for retailers, is excited to announce the closing of a $5M investment which includes follow-on funding by Globalive Capital. This investment will allow Flexiti Financial to continue developing the technology behind the company's award-winning POS lending platform, which is currently used in over 1000 merchant locations across Canada.

“Flexiti Financial’s mission is to be the leading provider of point-of-sale financing and payment solutions for retailers across Canada,” says Peter Kalen, Founder and CEO, Flexiti Financial. “We have built one of the most advanced POS lending platforms in North America, and this investment allows us to accelerate our growth and further invest in our technology to ensure we’re offering the quickest and easiest solution to our merchant partners, allowing them to offer more flexible sales and financing solutions to their customers.” Flexiti Financial’s credit technology and service platform allows businesses to instantly offer their customers low or no-interest financing, convert large purchases into monthly or deferred payment plans and establish a dedicated line of credit by creating a virtual private label card. The result: increased traffic, more sales and a boost to the business’s bottom line.

“Canadian consumers and businesses are looking for alternative financing options tailored to their lifestyle or business needs and we believe Flexiti Financial’s technology is uniquely positioned to capitalize on this growing market demand,” says Anthony Lacavera, Chairman, Globalive Capital Inc. “Flexiti Financial aligns with Globalive Capital’s core principle of finding companies and entrepreneurs that are breaking down barriers and challenging the status quo, and providing them with the resources they need to accelerate growth.”

Flexiti Financial is a member of ACT Canada; please visit www.flexitifinancial.com.

13. GEMALTO ANNOUNCES WORLD’S FIRST GSMA SECURITY ACCREDITATION FOR ESIM SUBSCRIPTION MANAGEMENT

Source: Gemalto (11/02)

Gemalto has become the first supplier in the world to undergo the GSMA Security Accreditation Scheme (SAS) certification for Subscription Management (GSMA SAS-SM), thereby providing MNOs with exacting standards of protection for sensitive data in M2M and IoT applications. The landmark announcement follows the recent GSMA certification process of LinqUs On-Demand Connectivity for the production and personalization of Gemalto's UpTeq eSIM (embedded SIM), in June 2016. The second SAS certification relates to the Gemalto secure data center in Tours, France for both SM-DP (Subscription Management Data Preparation) and SM-SR (Subscription Management Secure Routing) operations, and will establish Gemalto as the first company offering end-to-end GSMA SAS-SM compliant solutions for the provisioning and management of cellular subscriptions for M2M and IoT applications. As a result, Gemalto ensures MNOs can support innovative customer deployments with the required level of security and interoperability.

Cellular M2M and LPWA[i] could represent 20% of the global M2M market by 2020[ii]. The new generation of eSIM is providing a platform for dramatic growth in M2M and IoT applications such as autonomous cars, smart energy and industry 4.0. It facilitates out-of-the-box connectivity and remote subscription management of connected devices in the field, However, the threat of hacking attacks represents a major concern for OEMs and MNOs. Gemalto's comprehensive security accreditation addresses these concerns, by offering a secure end-to-end eSIM management solution. It extends from initial personalization of the eSIMs that are installed in connected devices at the manufacturing stage right through to the remote download, activation, deactivation and deletion of subscription profiles. Risk is minimized and MNOs are provided with a fully accountable record of the security measures taken to protect sensitive data.

"GSMA accreditation for both our eSIM subscription management and data provisioning capabilities confirms Gemalto's leadership position in the rapidly growing M2M and IoT markets," said Benoit Jouffrey, Vice President of On-Demand Connectivity for Gemalto. "We make it far easier for MNOs to leverage their network assets and develop valuable new income streams by creating trusted ecosystems that will resist even the most sophisticated hacking attacks."

Gemalto is a member of ACT Canada; please visit www.gemalto.com.

14. EIKA CHOOSES OT TO LAUNCH BANKAXEPT FIRST DUAL PAYMENTS CARD IN NORWAY

Source: Business Wire (12/01)

OT (Oberthur Technologies) and Eika Alliance, one of the largest players in the Norwegian financial market, with almost a million customers, announced the successful launch of the first dual payment card certified by BankAxept. This is the first step for an acceleration of the rollout of contactless payment in Norway. OT’s dual payments card leverages INTERAC Flash® technology that allows Eika to offer to its customers a contactless BankAxept certified payment card. BankAxept is the local Norwegian payment scheme and has the most widely used payment card, representing 9 out of 10 transactions in Norway. Contactless payments are available at over 100,000 merchants in the country.

OT’s dual payments card is based on the Near Field Communication technology (NFC), which allows wireless communication between both the card and the payment terminal using radio signals. Thanks to this technology, contactless cards make payments easier and faster. As users don’t need to enter their PIN codes, payments are completed in less than half a second, if the amount does not exceed NOK200. The purchase can be completed by simply waving the card over the payment terminal. However, if the store doesn’t support NFC technology, Eika’s cardholders still have the possibility to use the chip and its PIN code.

“As a result of a close and successful collaboration with Eika and BankAxept, OT is proud to deliver a product with INTERAC Flash® technology that enables contactless BankAxept payments. The first live cards already delivered are the starting point for wider contactless rollout in Norway that will bring convenience to cardholders” said Eric Duforest, Managing Director of the Financial Services Institutions activity at OT. “Thanks to OT’s support, we were able to meet the commitment made toward our customers and partners and were able to be the first bank in Norway to issue BankAxept cards using INTERAC Flash® technology supporting BankAxept Domestic contactless transactions” added Hege Toft-Karlsen, Chief Executive Officer at Eika Gruppen AS. “Eika’s strategy is to offer innovative payment solutions based on national and international standards. We believe that contactless BankAxept-cards will be a catalyst for contactless acceptance in Norway, giving consumers a faster and more convenient payment option” continued Erlend Sundvor, Vice President Payments at Eika Gruppen AS.

"The use by BankAxept of debit cards and POS devices leveraging INTERAC Flash® capabilities demonstrates our commitment to collaborating with other domestic debit networks around the world to bring secure, innovative products to market and enhance the consumer payment experience" said James Good, Head of International Business Development, Interac Association and Acxsys Corporation. “It has been a pleasure to work with OT on the successful launch of Eika contactless cards with BankAxept. Eika Gruppen has shown great commitment to the BankAxept platform and thanks to competence within OT and other partners we were able to deliver a very efficient project in short time” concluded Øyvind Apelland, CEO at BankAxept.

Interac Association and Oberthur Technologies are members of ACT Canada; please visit www.interac.ca and www.oberthur.com.

15. INTERNET OF THINGS (IOT) SECURITY TAKES CENTER STAGE AT FBI, DHS, NIST AND CONGRESS

Source: JD Supra Business Advisor (11/21)

On October 21, 2016, a domain name service host and internet management company experienced at least two waves of a distributed denial of service (DDoS) attack that impacted at least 80 websites, including those belonging to Netflix, Twitter and CNN. The attack was launched by infecting millions of American’s Internet of Things (IoT) connected devices with a variation of the Mirai malware. The Mirai malware primarily targets IoT devices such as routers, digital video records and webcams / security cameras by exploiting their use of default usernames and passwords and coordinating them into a botnet used to conduct DDoS attacks. The U.S. Federal Bureau of Investigation (FBI) does not have confirmation of a group or individual responsible for the attack. In September 2016, two of the largest IoT DDoS attacks using the same malware disrupted the operations of a gaming server and computer security blogger website.

In light of these attacks, there has been an increased focus on IoT security at the FBI, the U.S. Department of Homeland and Security (DHS), the National Institute of Standards and Technology (NIST) and Capitol Hill.

FBI Guidance

Five days after the October 21, 2016 attack, the FBI issued a Private Industry Notification, providing a list of precautionary measures stakeholders should take to mitigate “a range of potential DDoS threats and IoT compromise,” including but not limited to:

- Having a DDoS mitigation strategy ready ahead of time and keeping logs of any potential attacks;
- Implementing an incident response plan that includes DDoS mitigation. The plan may involve external organizations such as law enforcement;
- Implementing a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location;
- Reviewing reliance on easily identified internet connections for critical operations, particularly those shared with public facing web servers;
- Ensuring upstream firewalls are in place to block incoming UDP packets;
- Changing default credentials on all IoT devices; and
- Ensuring that software or firmware updates are applied as soon as the device manufacturer releases them.

DHS Guidance

On November 15, 2016, the DHS issued its own non-binding guidance for prioritizing IoT security, aimed at IoT developers, IoT manufacturers, service providers, industrial and business-level consumers. According to the DHS, there are six non-binding principles that, if followed, will help account for security as stakeholders develop, manufacture, implement or use network-connected devices.

Principle #1 – Incorporate Security at the Design Phase

The DHS notes that security should be evaluated as an integral component of any network-connected device. Building security “in at the design phase reduces potential disruptions and avoids the much more difficult and expensive endeavor of attempting to add security to products after they have been developed and deployed.” To that end, the DHS suggests the following practices:

- Enable security by default through unique, hard to crack default user names and passwords.
- Build the device using the most recent operating system that is technically viable and economically feasible.
- Use hardware that incorporates security features to strengthen the protection and integrity of the device.
- Design with system and operational disruption in mind.

Principle #2 – Advance Security Updates and Vulnerability Management

Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been sent to market. The DHS notes these flaws can be mitigated through patching, security updates, and vulnerability management strategies. Suggested practices include:

- Consider ways to secure the device over network connections or through automated means.
- Consider coordinating software updates among third-party vendors to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.
- Develop automated mechanisms for addressing vulnerabilities.
- Develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities.
- Develop an end-of-life strategy for IoT products.

Principle #3 – Build on Proven Security Practices

According to the DHS, many tested practices used in traditional IT and network security can be applied to IoT, and can help identify vulnerabilities, detect irregularities, respond to potential incidents and recover from damage or disruption to IoT devices. The DHS recommends NIST's framework for cybersecurity risk management, which has widely been adopted by private industry and integrated across sectors. Other suggested practices include:

- Start with basic software security and cyber security practices, and apply them to the IoT ecosystem in flexible, adaptive and innovative ways.
- Refer to relevant Sector-Specific Guidance, where it exists, as a starting point from which to consider security practices (e.g., the National Highway Traffic Safety Administration recently released guidance on Cybersecurity Best Practices for Modern Vehicles and the Food and Drug Administration released draft guidance on Postmarket Management of Cybersecurity in Medical Devices).
- Practice defense in depth.
- Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

Principle #4 – Prioritize Security Measures According to Potential Impact

The DHS recognizes that risk models differ substantially across the IoT ecosystem, and the consequences of a security failure will vary significantly. The DHS therefore recommends:

- Knowing a device's intended use and environment, where possible;
- Performing a "red-teaming" exercise where developers actively try to bypass the security measures needed at the application, network, data or physical layers; and
- Identifying and authenticating the devices connected to the network, especially for industrial consumers and business networks.

Principle #5 – Promote Transparency Across IoT

Where possible, the DHS recommends that developers and manufacturers know their supply chain, and whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. This increased awareness could help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies. Recommended practices include:

- Conduct end-to-end risk assessments that account for both internal and third party vendor risks, where possible.
- Consider the creation of a publicly disclosed mechanism for using vulnerability reports.
- Consider developing and employing a software bill of materials that can be used as a means of building shared trust among vendors and manufacturers.

Principle #6 – Connect Carefully and Deliberately

The DHS notes that consumers, particularly in the industrial context, should “deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption.” To that end, suggested practices include:

- Advise IoT consumers on the intended purpose of any network connections
- Making intentional connections.
- Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable selective connectivity.

NIST Guidelines

On November 15, 2016, NIST released its own guidance advising IoT manufacturers and developers to implement security safeguards and to monitor those systems on a regular basis. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. The new NIST Special Publication 800-160 is the product of four years of research and development, and focuses largely on engineering actions that are required to ensure connected devices are able to prevent and recover from cyber attacks, and lays out dozens of technical standards and security principles for developers to consider.

Congressional Hearing

One day after the DHS and NIST guidance was released, on November 16, 2016, the House Committee on Energy and Commerce’s Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology held a hearing on “Understanding the Role of Connected Devices in Recent Cyber Attacks.” The witnesses were Dale Drew of Level 3 Communications, Kevin Fu of Virta Labs and the University of Michigan, and Bruce

Schneier from the Berkman Klein Center at Harvard University. The witnesses uniformly recommended that while the DDos attack in October was just on popular websites, and not critical infrastructure, attacks toward critical infrastructure, including public safety and hospital systems, are likely. Each witness stressed the importance of addressing the vulnerabilities at the onset of developing technology, and urged greater oversight by lawmakers.

16. A NEW, IMPROVED 3-D SECURE DEBUTS

Source: Digital Transactions (12/01)

It's Round 2 for the online-authentication technology known as 3-D Secure, and security experts say it stands a good chance of being more popular than the original version. EMVCo, the chip card standards body owned by the world's six leading payment card networks, released 3-D Secure 2.0 in late October. Visa Inc. originally developed the 3-D Secure technology for protecting e-commerce transactions about 15 years ago and branded it "Verified by Visa." The company offered the underlying technology to other networks, which put their own brands on it. But many merchants refused to use 3-D Secure because of the "friction" it generated by having a buyer leave the merchant's Web site to complete authentication steps on a pop-up window, leading to abandoned transactions.

Over the years, card issuers and processors worked out protocols that reduced the friction, but merchants didn't shake their fears about lost sales. That prompted the networks to take 3-D Secure into EMVCo's shop for a reboot ("Securing the Future of 3-D Secure," July). Boston-based research firm Aite Group LLC estimates that only 18% of U.S. e-commerce transactions used 3-D Secure in 2015—not many, though far better than the 6% in 2013.

Transaction abandonment should be much less of an issue with version 2.0, says Mike Keresman, founder and chief executive of CardinalCommerce Corp., a Mentor, Ohio-based e-commerce-services firm. The new specification puts the complexities of online authentication behind the scenes, he says. "It will address quite a few of the issues, and yes, merchants will adopt, because they're going to get higher authorization rates," says Keresman. "It is designed to be smoother, a friction-free environment for the consumers." "I do think we'll see an uptick in use of 3DS 2.0," Julie Conroy, research director at Aite, says by email.

The new spec is more than 200 pages long, but Conroy says "there were no big surprises in it. The networks have been talking about the direction this is going in for quite some time." The specification addresses security for technologies that have bloomed since 3-D Secure first appeared, including app-based purchases on smart phones and other mobile devices, as well as traditional browser-based e-commerce channels. It also addresses so-called step-up authentication systems such as one-time passcodes and biometrics. "Besides security, the consumer experience is central to EMVCo's work," Jonathan Main, chairman of the EMVCo Board of Managers, said in a news release. “In addition to engaging with industry experts, we conducted user testing in multiple markets to understand consumer preferences for verifying their identity online. Feedback has been incorporated into the new global specification to also accommodate country-specific preferences and regulatory requirements.”

While one-time passcodes, which could be sent by text message to the buyer and entered into the checkout page to confirm the transaction, are seen by many in the payments industry as more secure than static passwords, they aren’t invulnerable, according to Conroy. “We are seeing criminals have success in compromising that in a number of countries,” she says. “This highlights the importance of looking to other capabilities, such as biometrics, as the stepped-up form factor.” CardinalCommerce developed the online security service called Cardinal Consumer Authentication, which uses 3-D Secure protocols when appropriate, according to Keresman. But the service goes beyond 3-D Secure in assessing variables about the device used for an e-commerce transaction, as well as data from merchants about their customers and from issuers about their cardholders, says Keresman. “The prevailing thought is we’ve got to make sure the good guys can buy,” says Keresman.

Visa is a member of ACT Canada; please visit www.visa.ca.

17. LEADING DANISH RETAILERS SELECT VERIFONE TO GIVE MILLIONS OF CONSUMERS MORE CASHLESS PAY OPTIONS AT CHECKOUT

Source: Verifone (11/28)

Verifone announced that Dagrofa, Denmark’s third largest retail company, and REMA 1000, the country’s fastest growing discount chain, have recently selected Verifone to enable more options for the way consumers shop and pay in their stores. Dagrofa and REMA 1000 represent significant wins and growing market share for Verifone. With its chamber of commerce proposing to make all money transactions electronic, Denmark is a leader in the world’s shift towards cashless societies with approximately 80 percent adoption of non-cash payments. The country is also home to one of the world’s most progressive and widely adopted mobile payment schemes. MobilePay, created by Danske Bank, is installed in more than 90 percent of Danish consumer smartphones, and is only surpassed by Facebook and Messenger in app acceptance.

By upgrading to Verifone, Dagrofa and REMA 1000 will be playing a significant role in driving consumer adoption for mobile payment in the country, as it is ready for future mobile payment options such as plans by Dankort, the country’s national debit card, to enable payments through consumer mobile devices. ”We already support MobilePay, but now we are first in Denmark to integrate mobile payment with card payment in just one piece of hardware. We want to make it even easier for our customers to make digital payments. Verifone has all the necessary functionality and provides an open and very straightforward solution at the cash register. Combining every type of payment in the same device makes life easier for both customers and our employees. Our goal is to deliver excellent experiences related to food, and Verifone's solution will help us deliver on this goal," says CEO Per Thau from Dagrofa.

"With the Verifone device upgrade, we can ensure our customers will have an easy and convenient experience using their preferred payment method whether it is a Danish or international card, Dankort or MobilePay," says CFO, Torben L. Sorensen from REMA 1000. "We are very proud that Dagrofa and REMA 1000 have selected Verifone as its payment solution provider. Our solution benefits both our clients and their customers alike as it can handle many payment methods including all payment cards and many mobile apps," says General Manager of Denmark Chris Lund-Hansen from Verifone.

Verifone is a member of ACT Canada; please visit www.verifone.com.

18. GEMALTO SAFENET HSM DELIVERS HIGHEST LEVEL OF DIGITAL TRUST TO SECURE SENSITIVE COMMUNICATIONS THROUGH THE SYMPHONY PLATFORM

Source: Gemalto (11/15)

Gemalto announced the integration of its industry-leading SafeNet Hardware Security Modules (HSM) with Symphony Communication Services' secure cloud-based communications platform. As an integrated offering, the SafeNet HSM protects the cryptographic root of trust for secure and confidential communications for highly-regulated organizations using the Symphony platform. Gemalto recently presented its contribution to the platform at Symphony Innovate 2016, an invite-only industry conference dedicated to strategizing on the future of work and how enterprises are driving this transformation through Symphony's communications platform.

"Symphony delivers a secure compliant productivity and collaboration platform whose entire ecosystem—from content owners, to trading platforms, to finserv companies—depends on the best security available," says Frederic Stemmelin, Symphony's Vice President of Business Development. "Gemalto's state-of-the-art encryption technology meets the modern standard of security that our platform demands." Data security is one of the primary challenges facing the financial services industry. According to Gemalto's latest Breach Level Index report, breaches affecting the industry accounted for 12 percent of all breaches during the first six months of 2016, a period during which the total number of data breaches rose by 15 percent compared to the last six months of 2015.

The Gemalto SafeNet HSM is a dedicated crypto processor that securely manages, processes and stores cryptographic keys inside of a hardened, tamperresistant device. Symphony's customers can deploy a SafeNet Network HSM in their data center or purchase Cloud HSM in an Amazon Web Services (AWS) cloud environment or through Google Cloud Platform, using it to manage and secure encryption keys and cryptographic operations in order to protect communications and maintain compliance. Whether it's via secure text, chat, email, voice, or video, Symphony with Gemalto secures communications with FIPS 104-2 Level 3 assurances, ensuring regulatory compliance and protection for data in motion and at rest. Symphony's integration with the SafeNet HSM gives the customer the ability to manage access to specific conversations by assigning or revoking credentials for appropriate participants as needed.

"Working with Symphony is the logical choice for helping financial institutions protect all sensitive data, regardless of where it's stored or how it gets shared," said Todd Moore, Senior Vice President for Encryption Products at Gemalto. "These organizations now have the ability to fully own the keys that encrypt data in every environment in their infrastructure where the Symphony platform is deployed, all while employees enjoy the convenience and productivity capabilities of a streamlined workflow."

Gemalto is a member of ACT Canada; please visit www.gemalto.com.

19. SECURITY FOR THE SMART HOME: INFINEON TEAMS UP WITH CHINESE APPLIANCE MANUFACTURERS FOR SOLUTIONS

Source: Infineon (11/24)

Secured Smart Home Appliances in China: In the so-called Internet of Things (IoT) unauthorized access has to be prevented. Together with partners Infineon Technologies AG founded the "Open Laboratory for Smart Home Interconnection Security" in Beijing. Infineon is the only non-Chinese company among the founding members which include Midea, Huawei Consumer BG, Tencent and CESI, the China Electronics Standardization Institute supervised by the Ministry of industry and information technology. The partners are aiming at jointly developing security technologies for smart home appliances that are manufactured and used in China.

“The joint project underlines our competence in the development of security solutions for the connected world,” said Helmut Gassel, member of the management board of Infineon Technologies. “We are very pleased to team up with Chinese partners to set up the ‘Open Laboratory for Smart Home Interconnection Security’. Together, we want to develop standards to better protect connected smart home appliances that are increasingly part of the Internet of Things. The joint lab is a major step forward in increasing consumers’ privacy.” Smart devices and home appliances are the building blocks of a smart home. They range from basic sensors used in refrigerators or lighting to powerful computing devices with a full operating system and user interface such as smart home gateways, controls or entertainment systems. Every smart device can be connected to the internet using an IP address. Unsecured, this makes them vulnerable to attacks. China is the fastest growing market for smart home appliances. Researchers forecast an exponential growth potential for smart home appliances at an annual growth rate of 97 percent between 2016 and 2020. Shipments of smart home appliances are expected to grow from 15 million units to 223 million units in the same timeframe (IHS Markit 2016).

Infineon is a member of ACT Canada; please visit www.infineon.com.

20. ACCEO TENDER RETAIL PARTNERS WITH SYSTEM INNOVATORS

Source: Acceo (10/31)

System Innovators (SI), a leading provider of centralized cashiering and enterprise revenue management (ERM), and ACCEO Solutions, a leader in payment solutions, have partnered to offer government clients an EMV-certified, semi-integrated point-of-sale (POS) middleware solution with end-to-end encryption (E2EE). iNovah EMV Direct combines SI's iNovah ERM point-of-sale solution with the ability to accept EMV transactions from multiple credit card processors while securely encrypting customer data to mitigate clients' risk of card-present fraud utilizing E2EE. The semi-integrated solution offers clients with increased fraud protection, greater operational efficiency, secure transactions and the ability to route transactions directly to their processor of choice.

"ACCEO's knowledge and years of experience in developing payment-processing middleware were key criteria for selecting their middleware solution to bring EMV-processing capabilities to our clients. The new module for iNovah, "EMV Direct", allows our clients to accept EMV transactions from many top-tier credit card processors in North America. This partnership aligns us with our goal of providing the freedom to aggregate credit card processing with a vendor of choice to our clients", said Greg Whitnell, Vice President of Sales and Marketing at System Innovators.

The flexibility and scalability of iNovah EMV Direct put government clients in control of their enterprise, with the ability to integrate seamlessly into any infrastructure and choose the terminal software that best suits clients' needs and budgets. Not only will the semi-integrated solution support payment from cards embedded with chip and PIN technology, but consumers will benefit from the freedom to use multiple payment methods, such as using contactless, smartphone, mobile POS, debit and credit payments. "We pride ourselves as being one of the leading payment solution providers in North America. However, this being said, we would not have achieved the significant growth and success we are experiencing in the US market without great partnerships. We are extremely pleased to be associated with System Innovators. Their complementary expertise and solutions enhance the value proposition for clients, which is always the ultimate goal", said

Joey Vaccaro, Vice President, Business Development and Strategic Alliances at ACCEO. The partnership enables choice among government clients and paves the way to further drive the adoption of processors and terminals.

ACCEO Solutions Inc. is a member of ACT Canada; please visit www.acceo.com and www.tender-retail.com

21. APPLE JUST REMOVED HUNDREDS OF FAKE SHOPPING APPS FROM THE APP STORE

Source: Network World (11/07)

Just in time for the holiday shopping season, the iOS App Store is seeing a deluge of fake shopping apps branding themselves with designer names in hopes of trapping gullible buyers. Apple is now stepping in to remove the counterfeit apps, which are sneaking in by changing the content after Apple's approval or by resubmitting apps under different names and credentials after being outed as fraudulent. After reports of apps using reputable companies' names to shill their fake wares in the App Store surfaced in the New York Times and New York Post, Apple removed hundreds of offenders. But hucksters keep coming back: The Times found that an app called Overstock Inc. was trying to convince shoppers that it was Overstock.com by selling clothes and Ugg boots. Apple killed the app, only to see it return the next day, because sketchy developers are finding new ways to bypass the company's traditionally tough app review process.

INSIDER: 5 ways to prepare for Internet of Things security threats

But the company is doing its best to crack down on developers who use existing brands' names to submit fake apps, an Apple spokesperson told the Times. "We strive to offer customers the best experience possible, and we take their security very seriously," said Apple's Tom Neumayr. "We've set up ways for customers and developers to flag fraudulent or suspicious apps, which we promptly investigate to ensure the App Store is safe and secure. We've removed these offending apps and will continue to be vigilant about looking for apps that might put our users at risk."

Shopper beware

So what's the harm of installing a fake app? If you try to buy a product, at best you'll be frustrated by app crashes or annoying pop-up ads. At worst, you'll hand over your credit card info to a sketchy company and never receive the item you ordered. How to tell if a retail app is legit: How many reviews does it have? How many previous versions have been released? Does the language sound like it was written by an adult professional with a good grasp of English? If any of the above seem suspect, go to the store's website and see if you can find an App Store link directly from the source.

22. GIESECKE & DEVRIENT AND M2MD TECHNOLOGIES, INC. FORM STRATEGIC RELATIONSHIP

Source: Giesecke & Devrient (11/17)

Giesecke & Devrient (G&D) and M2MD Technologies (M2MD) announced a strategic partnership to offer a more secure, faster and cost effective method for an automaker to communicate with its vehicles. Today, most automotive manufacturers offer telematics packages that connect the vehicle through a cellular module to a broad set of safety, diagnostic, and convenience services. With connectivity comes the need for strong security and efficient communications – both of which have troubled the industry for years. G&D and M2MD are cooperating to deploy a Communications Gateway that will join M2MD's proprietary security and quick connect solutions with the robust capabilities of G&D's SIM. "The partnership of M2MD and G&D brings together innovative solutions, deep expertise, brand strength and global relationships to solve these critical industry challenges," said Chuck Link, President and CTO of M2MD Technologies. "The Communications Gateway will be architected with the most progressive technology available and customized specifically for the connected car."

Automakers will benefit from the partnership which joins the expertise from the M2MD innovations with the proven security solutions from G&D. "We can significantly impact the security of the vehicle while positively enhancing the customer experience with a much faster connection," said Scott Marquardt, President of G&D's US Mobile Security business. "We are excited to work with M2MD to deliver solutions that strengthen the automakers telematics solution and are more cost effective to operate." The Communications Gateway is expected to launch in early 2017. As the connected car expands globally, the companies expect to offer the Gateway in other markets as well.

Giesecke & Devrient is a member of ACT Canada; please visit www.gi-de.com.

23. VISA ACQUIRES CARDINALCOMMERCE TO SECURE AND PUSH DIGITAL COMMERCE

Source: Mobile Payments Today (12/02)

Visa has announced an agreement to acquire CardinalCommerce, a company that specializes in e-commerce payment authentication, according to a press release. Financial terms of the transaction were not disclosed. The transaction, which is subject to the customary closing conditions, is expected to close in Visa's second fiscal quarter 2017. Visa said in the announcement that the acquisition will result in easier, more secure payments, whether through a browser, mobile app or connected device, and will help the company's clients and merchant partners accelerate digital commerce.

"This strategic acquisition combines Visa's industry expertise and Cardinal's critical role in payment authentication to bring added security to online transactions, reduce fraud, and support digital commerce, which is the fastest growing commerce segment today," said Mark Nelsen, senior vice president of risk and authentication products at Visa. "By helping merchants, acquirers and issuers better distinguish between good and bad transactions, Visa is in an even better position to strengthen consumer trust in digital payments, help merchants grow their businesses and accelerate innovation in commerce." Visa already provides Cardinal services to merchants and acquirers through its CyberSource merchant and acquirer enablement platform, according to the announcement.

Cardinal will continue to operate and serve clients as a wholly owned subsidiary of Visa, and its authentication platform will continue to support a broad range of payment brands and partners across the industry. Co-founders Tim Sherwin and Chandra Balasubramanian will remain as leaders of the Cardinal team, which is based in Mentor, Ohio. "We are excited to embark on this next chapter of Cardinal's growth with Visa," said Mike Keresman, founder and CEO of Cardinal. "By combining our authentication expertise and role in supporting both merchants and issuers, and Visa's payments expertise and global reach, our two companies will be able to fast-track the next-generation of digital authentication."

Visa is a member of ACT Canada; please visit www.visa.ca.

24. INGENICO GROUP TO INTRODUCE ITS FIRST ANDROID-BASED POS AT TRUSTECH

Source: Ingenico (11/23)

Ingenico Group announced that it will present the APOS, its new Android-based payment terminal, at the upcoming Trustech event in Cannes, France. This device was designed to complement the Telium Tetra offer and further integrate the business and payment ecosystems. This launch represents the third stage of a strategy to achieve greater integration of payment acceptance solutions and business services. Ingenico first opened its Telium Tetra OS to HTML5 apps, then launched the Integrated POS combining a Telium Tetra terminal and any tablet on the market. Soon the Group will extend its offer with an all-in-one solution available to the entire Android community.

The APOS is Android-based and portable. It features a 5.5 full touchscreen, a front and rear camera and enables all payment methods (EMV chip and pin, mag stripe and contactless/NFC). Secure at its core and PCI 4.1 certified, the APOS protects card holders' data while remaining open to business apps developed on web standards and addresses a wide range of use cases. "We are pleased to introduce this first Android-based payment terminal. The APOS demonstrates Ingenico Group's ability to offer acquirers an ever more relevant and comprehensive range of payment acceptance devices to help merchants increase their business efficiency thanks to seamless integration of payment and business services", said Jacques Guerin, EVP Smart Terminals & Mobile Solutions.

Ingenico Group is a member of ACT Canada; please visit www.ingenico.com.

25. SAMSUNG PAY FIRST 'PAY' TO ADD SYSTEM-SPECIFIC REWARDS PROGRAM

Source: Mobile Payments Today (11/15)

It was at last month's Money20/20 conference in Las Vegas that Samsung's Haley Kim told Mobile Payments Today about the company's desire to turn Samsung Pay into a mobile wallet that, at its core, is about convenience and loyalty benefits and not necessarily about payments. Samsung accomplished the convenience part (and made Samsung Pay more versatile) by enabling users to store more than just traditional payment cards in the mobile wallet. This included the ability for users to add retailer gift cards as well as loyalty and memberships cards.

At Money20/20, Samsung announced the availability of a nearby deals feature that gives consumers the opportunity to benefit from discounts wherever they go, Kim said. On Monday, Samsung Pay took another step forward as the most well-rounded mobile wallet on the market with its announcement of the upcoming availability of a system-specific loyalty program called Samsung Rewards. Android Pay and Apple Pay both lack such a program.

Samsung Pay users enrolled in the rewards program will earn points for every Samsung Pay transaction and eventually will have the opportunity to redeem their stash for retailer gift cards, prepaid Samsung Rewards Visa gift cards, Samsung products and more, according to a press release. "As we enter the new year, and look to the future of mobile payments, we want to build on the success of Samsung Pay by giving new users even more reasons to try it out — not to mention, thank our existing customers for using a service they already love," Nana Murugesan, vice president and general manager of services and new business at Samsung Electronics America, wrote in a company blog post accompanying the announcement. "That's why we're excited to offer Samsung Pay users a first-of-its-kind rewards program for a mobile payments platform: Samsung Rewards." Samsung will launch the loyalty program later this week.

The company’s decision to introduce a mobile wallet-specific loyalty program comes at a time when industry observers are pleading for mobile payments providers to place rewards centerstage in order to drive increased consumer adoption. "The perception of getting a bargain is maybe the most compelling carrot for driving consumer behavior in general — and mobile payments are no exception," Tim Spenny, vice president of financial services consulting at GfK Research, wrote last month in a blog post about Kohl's Pay.

"Combining a loyal customer base with attractive offers, via coupons, has worked well for Starbucks – and Kohl's is betting it can do the same." While Spenny's comment was directed toward retailer-specific programs, the Pays have faced difficulty growing their user base. The industry views rewards as a way to reverse that trend.

Samsung Rewards is structured like a typical credit card rewards program with a few bonuses here and there. "You can get even more points through limited-time bonus offers," Murugesan wrote. "Samsung Rewards will partner with retailers and small businesses and give users seasonal opportunities to earn additional points — anyone who joins Samsung Rewards in November or December, for example, will receive double points on purchases made in those months. "Users can then redeem their points for Samsung products, vouchers for Samsung.com, Samsung Rewards Visa Prepaid Card value, and gifts cards to some of the country's leading retailers. Users can also be eligible for additional prize giveaways — called 'Instant Wins' — that include things like trips to Napa Valley and Las Vegas that surprise and delight." Samsung Rewards will also feature user tiers.

For instance, a user who completes five Samsung Pay transactions in one month will achieve "silver" status and earn twice the points for transactions using Samsung Pay. Twenty monthly transactions gets the user to "gold" status, which awards triple points; 30 monthly Samsung Pay transactions puts a user in the "Platinum" tier earning quadruple points, according to the announcement.

26. CARDTEK AND NXP COLLABORATE TO INTRODUCE DIGITAL PAYMENT SOLUTION FOR WEARABLES

Source: Cardtek (11/11)

Cardtek has partnered with NXP Semiconductors to introduce an innovative payment system for wearables, Digital Enablement Platform. The payments industry is increasingly focused on wearables; according to a recent CCS Insight report, there will be 411 million wearables in 2020 and a transaction volume of $34.2 billion. Most recently, wearables were introduced at the Olympic Games in Rio. Cardtek's Digital Enablement Platform allows consumers to make safer and easier transactions in a convenient wearables solution. This includes easily on-boarding payment cards, transit tickets, access cards and any other services in wearable devices. Cardtek has implemented a payment system infrastructure, integrating NXP PN66T and P60 wearable chips, to help issuers, wearable OEMs and other service providers enable payment and non-payment services in wearables, as well as activation and deactivation of services. Cardtek offers Mobile SDK, enabling any party to develop user interfaces to have their own mobile wallet. The solution incorporates tokenization services to securely integrate tokenized payment credentials into the wearable. Cardtek also offers Instant Issuance solutions for the personalization of P60 wearable chips with printers.

“Wearables bring many advantages to the payments industry, one of the key benefits is that issuers or service providers will have full ownership of their own wallets without being dependent on third-party providers,” said Emilian Elefteratos, Cardtek EVP sales & marketing for North America. “Built-in NFC wearables will allow consumers to leave their wallet at home and make transactions simpler and safer than ever before. Cardtek is pleased to play a leading role in helping drive the rapidly emerging wearable payments market.” “The integration of contactless secure applications in wearable devices can be a significant business opportunity for hardware and service providers,” said Charles Dach, vice president of transactions at NXP. “With NXP’s PN66T loader service feature, implementation of new services on wearables is simple and secure – opening the door for more convenience in being able to use your wearable for identification, banking, ticketing, access and more.”

Cardtek is a member of ACT Canada; please visit www.cardtek.com.

27. THE WEAK LINK IN THE OMNICOMMERCE SECURITY VALUE-CHAIN

Source: Let's Talk Payments (11/02)

A far cry from the first ARPANET e-commerce transaction is omnichannel digital commerce or omnicommerce. As e-commerce matures, mobile devices become the second brain in our hands, and connectivity steadily improves, retailers and service providers are leveraging every asset available to them to improve engagement with customers and drive repeat sales. It is now typical for a retailer to leverage their physical world presence for providing customers with the comforting touch and feel of their products, their websites for browsing, comparing product specifications and competitor pricing, and their mobile apps for reaching out and enticing customers based on time, location and context. Collectively, all these channels or the omnichannel approach, supported by consumer profiling and behavioral data analytics, is helping providers auto-populate consumer shopping carts, close out a long contemplated acquisition by enticing the consumer with favorable financing, or force an impulse buy through a too-good-to-be-passed promotion just as the consumer walks by the store.

Along with the physical world and the virtual world, there is now a third front – namely media – that is poised to start driving transactions. Increasingly all media, user-generated or curated, will become launch pads and conduits for transactions. While this is clearly a categorization under the virtual channel, its growing importance as a channel and depth of engagement warrants special treatment. As the front-end of the commerce equation evolves between the consumer and providers, the back-end payment and settlement network continues to evolve more or less in lockstep. First came the ability to process existing credit, debit and gift or prepaid cards online, followed by virtualization of the payment products themselves. The supporting networks continued to evolve, ensuring that they could handle transactions initiated in the real as well as the virtual world, and more importantly ensure that certain aspects of these transactions could leverage economies of scale while others continued to treat them differently, insulating them from systemic abuse and misuse.

Encryption of payment credentials has steadily improved over the years, not only in terms of entropy but also in terms of the overarching security business model. Security from a technology perspective is a function of time and computing power, essentially indicating that by increasing time or computing power any level of encryption can be compromised. As the science of encryption and cryptography continues to advance, the more pragmatic approach is to combine the best possible security technology with a business model that ensures all the players in the value-chain are equally incentivized to repel fraud. It is obvious that the weakest link introduces the most vulnerability into the overall system, and it is safe to assume that the weakest link is the one that is not appropriately compensated for ensuring that the highest level of security technology and processes are in place. Effectively the weakest link in the omnicommerce security value chain is not a technology component, but the underlying business model.

While there is always more work to be done on both fronts, technology and business, it is safe to say that the ecosystem has been sensitized. There is genuine hope that with more collaboration – at the consumer, the enterprise, and the government level – the overall ecosystem will be in a lot better position to thwart abuses by negative players. That said, beyond security, privacy continues to be challenged.

28. SOCIETE GENERALE LAUNCHES A NEXT-GENERATION CARD INTEGRATING A DYNAMIC SECURITY CODE

Source: Oberthur Technologies (11/16)

As a leading e-commerce bank1 in France, Societe Generale's priority is to continuously strengthen the security of online payments while making its customers' everyday lives easier. Following successful testing among more than 500 people, Societe Generale is one of the first global banks to offer its retail customers in France these next-generation cards featuring a dynamic security code. This innovative solution, OT MOTION CODETM, developed by Oberthur Technologies2, consists in replacing the 3-digit security code usually printed on the back of the card with a mini-screen displaying a new "dynamic" code which is refreshed automatically and randomly every hour3. Thus, if the card data gets stolen, the 3-digit security code becomes useless within an hour, preventing fraudsters from re-using the information on e-commerce sites. Designed to help fight cyber crime, this solution is also very simple as it changes nothing on the online purchasing process.

Responding to the constant growth of online purchases, this next-generation card broadens Societe Generale's range of payment solutions, already the most comprehensive one in the market, both for e-merchant clients (3D Secure, One-Click, Paylib) and retail customers (Pass securite, e-carte Bleue).

Oberthur Technologies is a member of ACT Canada; please visit www.oberthur.com.

29. INGENICO GROUP TO LAUNCH ITS NEW MOBILE SOLUTION, THE LINK2500, AT TRUSTECH

Source: Ingenico (11/25)

Ingenico Group announced the launch of its new mobile point of sale at the upcoming Trustech show in Cannes, France. Available in two versions, companion or standalone, the Link/2500 was designed to address small merchants' payment needs in mobility. The Link/2500 enables estate owners to offer their clients (micro and small merchants) a new generation mobile solution and the benefits of its broad range of services. This new device is compatible with Ingenico's suite of cost optimization services (estate management or digital receipt management). The Link/2500 covers the full spectrum of wireless connectivity (3G, fallback GPRS, Dual SIM, Bluetooth and Wi-Fi), offering flexibility to mobile merchants, while reducing communication costs and maximizing network availability.

Based on the Telium Tetra operating system, it is highly secure and supports all Ingenico payment applications, which is a key asset to Ingenico existing customers who can leverage Ingenico's unique portfolio of payment applications in one click. In addition to EMV Chip & PIN and swipe, the Link/2500 supports all payment methods including NFC/contactless, Apple Pay and Samsung Pay. Thanks to an integrated speaker providing vocal assistance and a real mechanical keypad with raised marking, the Link/2500 is built for accessibility. It is also available as a companion to pair with any smart device. This slim version is the thinnest mobile device on the market.

"The new Link/2500 completes Ingenico's extensive mobile solution offering to address all merchants' needs and mobility use cases. The cutting-edge and compact Link/2500 is aimed at small merchants, while the recently introduced iSMP4 offers an enterprise mobility solution for the most demanding retail environments. Our new comprehensive range of mobile POS illustrates our commitment to offering tailored solutions and cost optimization tools for all mobile environments." said Jacques Guerin, EVP Smart Terminals and Mobile Solutions.

Ingenico Group is a member of ACT Canada; please visit www.ingenico.com.

30. GOOGLE WALLET ADDS P2P PAYMENTS TO WEB BROWSERS

Source: Mobile Payments Today (11/10)

Google Wallet users now can send and receive funds transfers through a web browser app, according to a blog post from the company. "The new Google Wallet web app is here," Google wrote in the blog post. "[The app is] a fast and free way to pay friends and family, even if they don't have the Wallet app. Now, receive money instantly with only a debit card."

Google rebranded Google Wallet as a P2P mobile app last year to make way for Android Pay.

31. THE FED PRIORITIZES SECURITY AS PAYMENTS SPEED UP

Source: PYMNTS.com (11/07)

Last week, the Fed's Secure Payments Task Force called for comment from industry stakeholders about what challenges they face when it comes to payments security. The task force, made up of about 160 members, will explore areas of payments security, like identity management and data protection, in hopes the survey will help guide its plan of action for 2017 as it moves through its three objectives: represent views on future needs for more secure payments, address other issues to ensure the development of effective payments security and assess alternative approaches to security when it comes to faster payments capabilities.

"Tackling today's security challenges will require the commitment of all payment system participants," said Gordon Werkema, the Fed's payments strategy director, in a statement last week. "The Secure Payments Task Force is particularly interested in understanding any barriers that may exist to implementing the planned solutions." Todd Aadland, the Fed's SVP and payments security strategy leader, and Connie Theien, VP of industry relations at the Fed, offered PYMNTS more insight into how the Federal Reserve will tackle the issue of payments security, especially as faster payments initiatives from the Fed and other players change the game. "We looked broadly across what's going on in other countries in terms of their migration towards faster payments," Aadland said. "As they move to faster payments, criminals take advantage of the speed and actually circumvent controls at the weakest link."

With that in mind, the Federal Reserve's Secure Payments Task Force has developed various work streams on which its members can focus, with payments security in the context of faster and real-time payments a key theme. "The key is," explained Aadland, "without having that post-transaction security net that you don't get with real-time payments, it's really imperative that we enhance the controls upstream from final payment settlement to identification management and data protection." Theien added that the Fed's Faster Payments Task Force is collaborating with the payments security team for this very reason. She noted that

11 of the criteria issued by the Fed for what constitutes effective faster payments involve payments security.

"The Secure Payments Task Force is playing an important role in advising the Faster Payments Task Force," she stated. "Both task forces recognize the importance that we design future payment systems of ensuring that security is built in and designed on the front end to address specifically some of those risks that are unique to a real-time payment environment." In any payment environment, corporate payments face a broad range of security threats. There are those high-profile credit card data breaches that create massive headaches for merchants, while the Federal Bureau of Investigation has continually warned the nation about corporate phishing attacks that specifically target the B2B and supplier payment process, convincing businesses to pay a fake supplier. These are the types of scenarios that led the Secure Payments Task Force to zero in on focuses like identification management and data protection.

"We're looking at identification weaknesses in how to authenticate and ID end users, providers and devices," Aadland noted, adding that this is crucial for B2B and B2C transactions. "The scope of another working group is data protection, how to go about identifying what data of a B2B transaction needs to be protected and how best to protect it." Theien added other sources of uncertainty in payments security, like transaction authorization, enrollment and account takeovers. With the survey out by the Fed, the Secure Payments Task Force will be looking for commentary about these questions and others. After aggregating the responses, the task force will then look to see whether it needs to pivot in any certain direction to ensure all areas of payments security are covered. It's just the first steps in creating real change in the national payments landscape, but according to Theien and Aadland, even the preliminary results of the survey can have real impacts on payments innovation today. "Hopefully, a benefit of [this survey] would be that some of these products and vendors and providers would look at the output of these work streams, as far as the controls that the industry is saying they would need to be present and start to look at these as indicators to what to start building in their own product set," explained Aadland. With some payment service and product providers acting as members of the task force, the industry may have a lot to learn from the survey's eventual feedback. With such a fluid and rapidly evolving space like FinTech, the latest insight about security needs and concerns could be the competitive edge one innovator needs.

"There is a lot of exciting innovation happening in the payments industry," Theien said. "And we have lots of folks who are guiding that innovation at the table. I think, across the board, everyone recognizes that, while we want to develop and advance the capabilities that better service their needs, the security of payments is job one."

Since 1989, ACT Canada has been the internationally recognized authority in the market. As the eyes, ears and voice for stakeholders focused on secure payment, mobile, NFC, loyalty, secure identity, and leveraging EMV, we promote knowledge transfer, thought leadership and networking. We help members protect their interests, advance their causes, build their business and grow the market. We take a neutral and non-partisan approach to all issues, facilitating collaboration among issuers, brands, acquirers, merchants, regulators, solution providers, governments and other stakeholders. Over 50% of our members have been with us for more than 5 years, enjoying ongoing value from their affiliation with ACT Canada. Please visit www.actcda.com or contact our office at 1 (905) 426-6360.

Please forward any comments, suggestions, questions or articles to andrea@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
tel: 905 426-6360 ext. 124
fax: 905 619-3275
email: andrea@actcda.com
web: www.actcda.com
mail: 85 Mullen Drive, Ajax, ON, L1T 2B3
http://ca.linkedin.com/in/andreamcmullen

Insights • Networking • Visibility

ACT Canada is the place to be to:

Filter the truth from market noise
Understand complex issues
Facilitate problem resolution

Because stakeholder dialogue helps you make profitable decisions.