

### Danish stores to avoid cash under proposal

The Danish government proposed on 6 May that certain retailers in Denmark such as clothes shops and restaurants be excluded from laws requiring them to accept cash, as part of a range of economic initiatives which, if passed by Denmark's parliament, could come into force as early as January 2016.

The proposal is intended, *inter alia*, to reduce business costs. Retailers including doctors, grocery stores and post offices would however still be required to accept cash payments.

With Denmark having one of the highest rates of credit card payments per person in the European Union, supporters claim that few would be negatively affected by the proposal. The Danish Chamber of Commerce has expressed support for the initiative; spokesman Henrik Hytolft argues that "there is no longer a need for requirements on cash payments" and describes cash as being "tremendously expensive to handle due to security reasons," according to news website The Local.

Critics of the initiative have meanwhile argued that groups such as the disabled and elderly could be negatively affected by the proposal.

**IN THIS ISSUE**

- UK** FCA Business Plan and tech concerns **03**
- Europe** Pan-EU mobile P2P solutions **04**
- Canada** Card industry Code amended **07**
- Crowdfunding** EU regulation analysed **09**
- Payday Lending** US law enforcement **13**
- Mobile Payments** Tech giant offerings **15**

## Emerging payment methods prompt EU fraud law review

The European Commission (EC) published on 28 April its 'European Agenda on Security,' which states that the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment 'no longer reflects today's realities and new challenges such as virtual currencies and mobile payment'; the EC therefore plans to review this legislation and consider changes.

The 2001 Framework Decision requires Member States to have in place criminal offences for certain payment fraud and counterfeiting acts, but currently applies to non-cash payments only if these payments are made with corporeal instruments, such as cheques or credit cards. "Mobile and online payments are capturing an increasing share of overall payments - one aspect that could hold back develop-

ment of these payment methods is the concern of potential users as to payment security," said Roger Tym, Partner at Hogan Lovells. "The legislators and regulators can help here by trying to keep the legal and regulatory framework up to date, as far as possible; this needs to be balanced to prevent over-regulation stifling innovative developments or imposing unrealistic demands on service providers."

"Currently, Bitcoin and similar virtual currencies are not affected by the rules set out in the E-Money Directive/PSD," adds Adam Pasaribu, Associate at Bird & Bird. "Yet, the European Agenda on Security seems to indicate that perhaps it is time to establish criminal sanctions with respect to the fraudulent use of virtual currencies."

The EC will now assess the level of implementation of the

current legislation and consult with stakeholders, likely focusing on newer forms of crime such as identity theft. Following this, it may extend the legislation in relation to non-cash payments, with new proposals expected in 2016. "The EC could, for instance, modify the definition of 'payment instrument' in such a way that it will also include digital payment instruments," said Pasaribu. "It could propose that Member States should provide for better criminal sanctions and it could try to bolster the position of Europol's European Cybercrime Centre."

The EC identifies cyber crime in its Strategy as a priority area, emphasising the need for the implementation of the Directive on Network and Information Security (NIS Directive) alongside other relevant legislation as a key means to combat cyber crime.

## Virginia becomes first US state to mandate enhanced card security

Virginia Governor Terry McAuliffe signed on 5 May Executive Directive 5, issuing a mandate to Virginia's state agencies to implement advanced payment card security features, generally by the end of 2015.

"Virginia is the first State to take action to implement initiatives embracing recent Executive Orders ('EO') from President Obama, including EO 13681, which required all Government agencies to 'transition payment processing terminals and credit, debit, and other

payment cards to employ enhanced security features,'" explains Kevin Petrasic, Partner at Paul Hastings. "I believe Virginia's action is likely to spur action by other states to follow suit."

The Directive contains three mandates to state Secretaries of Technology and Finance, the State Treasurer and the State Comptroller: to provide a plan to the Governor by October 2015 on enhancing the security of merchant and prepaid debit card programs; to include in Virginia's main purchasing card

program advanced chip authentication technology by December 2015; and to create and adopt electronic identity management standards, based on recent state legislation.

"Virginia's move should have a huge impact on the industry given the market share of these government payments," said Linda Odom, Counsel at Bryan Cave. "No third party vendor will implement security measures for only their government customers - they will be available to their customers at large."