LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Technology Transactions Practice January 26, 2017 | Number 2069

United Arab Emirates – the New Digital Payments Regulatory Landscape

New Regulations balance innovation in the payments sector with safety, security and maintaining the public's trust in the UAE payment ecosystem.

After a long period of consultation, on 1 January 2017 the Central Bank in the United Arab Emirates (UAE) issued the Regulatory Framework for Stored Values and Electronic Payment Systems (Electronic Payment Regulation). The Electronic Payment Regulation's key message is that all eligible participating institutions (whether they are banks, payment networks, telecommunications companies, government entities or non-issuing commercial entities) must maintain necessary licenses as well as governance and operational controls to ensure the integrity of the payments system and provide a minimum level of consumer protection and clarity on consumer rights.

This *Client Alert* considers the following key aspects of the Electronic Payment Regulation:

- Regulated entities
- Non-regulated entities
- Obligations imposed on regulated entities

Which entities will be regulated?

The Electronic Payment Regulation applies to "Stored Value Facilities" (a non-cash facility in electronic or magnetic form purchased by a user and used to pay for goods and services) offering the following digital payment services:

- Cash-in services, enabling cash to be placed in a digital payment account
- Cash-out services, enabling cash withdrawals from a digital payment account
- Retail credit and debit digital payment transactions
- Government credit and debit digital payment transactions
- Peer-to-peer digital payment transactions
- Money remittances

To further classify payment service providers (PSPs) who provide such digital payment services, the Electronic Payment Regulation introduces four different types of PSP:

- **Retail PSPs**: commercial banks and other licensed entities offering retail, government and peer-to-peer digital payment services as well as money remittances
- **Micropayments PSPs:** entities offering micropayment solutions and facilitating digital payments for the unbanked or individuals with limited access to bank services (*e.g.,* telecommunications and transport companies)
- **Government PSPs:** government entities offering digital payment services
- **Non-issuing PSPs:** non-deposit taking and non-issuing institutions that offer retail, government and peer-to-peer digital payment services (*e.g.*, payment processing entities that do not issue stored value payment accounts)

PSPs may engage "Agents," subject to Central Bank approval and provided an Agent's services to a PSP are limited to registering users, providing cash-related services and facilitating the transmission of payments.

Which entities will not be subject to the Electronic Payment Regulation?

Entities providing the following payment services will not be subject to regulation:

- Payment transactions in cash with no intermediary involvement
- Payment transactions using a credit or debit card
- Payment transactions using paper cheques
- Payment instruments accepted as a means of payment only to purchase goods or services provided from an issuer — closed loop payment instruments such as loyalty cards or rewards programs that a department store issues to a user to spend only in that department store
- Payment transactions within a payment/settlement system between settlement institutions, clearing houses, central banks and PSPs
- Payment transactions related to transfer of securities/assets (including dividends, income and investment services)
- Payment transactions carried out between PSPs (including their agents/branches) for their own accounts
- "Technical Service Providers," defined as entities providing support services to PSPs but which do not handle user funds, *e.g.,* processing and storage of transactional data; privacy protection services; data and entity authentication; IT network provision; and provision and maintenance of terminals and devices used for payment services

"Virtual currencies" are also covered. These are defined as digital units used as a medium of exchange or form of stored value. However, the scope of regulation is unclear. The Electronic Payment Regulation states that these are "not recognised by the Electronic Payment Regulation" and further adds that such

currencies and transactions in such currencies are "prohibited." Whether the Electronic Payment Regulation simply excludes virtual currencies from regulation, prohibits licensed entities from dealing with virtual currencies and/or prohibits virtual currencies in the UAE entirely, is ambiguous.

What obligations are imposed on PSPs?

There are well-defined provisions imposed on PSPs across the entire payments value chain, such as:

- **Licensing:** PSPs will need to obtain licenses for their activities. Licenses will only be issued if a PSP meets the eligibility criteria for the relevant type of PSP (which may include, *e.g.*, minimum share capital, maintaining sufficient amounts of cash to liquid assets to meet full redemption value of corresponding payment instruments; corporate governance requirements mechanisms in place to safeguard funds, such as internal audit unit and dedicated compliance function).

- **Ongoing approvals:** PSPs will need to obtain approvals from the Central Bank prior to introducing significant change or enhancement to their payment systems. Outsourcing of a PSP's functions will also need prior Central Bank approval, and can only be undertaken by a UAE entity. Note that there are restrictions on outsourcing — a PSP will need to maintain and ensure compliance with relevant obligations, and if outsourcing critical operational functions, cannot do so in a manner that impairs the quality of internal controls and the ability of the Central Bank to monitor and enforce compliance.

- **Registration:** Licensed PSPs will need to comply with end user registration requirements, including know-your-customer procedures.

- **Operational obligations:** Licensed PSPs will be required to comply with a number of obligations, which are aimed at combating money laundering and fraud and providing consumers with transparency regarding their stored value and transactions, including:

    - Ensuring the PSP has systems in place capable of screening transactions to comply with anti-money laundering and counter-terrorism financing laws, including capability to block transactions that exhibit suspicious patterns or exceed particular thresholds

    - Ensuring that all transactions are settled through a UAE settlement institution

    - Imposing account funding limits, transactional limits and spending limits on customers

    - Providing a minimum level of information to a user with respect to a transaction, *e.g.*, reference number to allow identification or a transaction, transaction amount, applicable fees and identity of a payer and payee

    - Ensuring that systems are interoperable with other UAE payment systems

- **Consumer protection mechanisms**: Licensed PSPs will need to implement certain safeguards with a view to protecting consumers, including:

    - Entering into an agreement with each end user

    - Providing customer service support and dispute resolution details to end users

Important to note are the **data protection and privacy** obligations imposed on PSPs, which include**:**

- Storing all transactional records and user data for a minimum retention period, and importantly, storing such data in the UAE only (but not in a financial free zone)

- Not disclosing any personal consumer data to third parties, although disclosure is permitted to the Central Bank, by court order or to another regulatory authority if the Central Bank approves

These obligations add another layer to UAE's complex data protection landscape and must be considered alongside existing laws (*e.g.*, financial services and telecommunications laws concerning consumer data, specific laws (such as cybercrime laws) and general obligations under the constitution and penal code).

Enforcement and compliance

The Central Bank will be responsible for enforcing the Electronic Payment Regulation, and has broad powers to impose financial penalties on non-compliant entities as well as other orders (*e.g.,* revoking or suspending licenses, accessing a regulated payment system if the Central Bank considers it reasonable under the circumstances, such as on public interest grounds).

PSPs that commenced providing digital payments prior to 1 January 2017 will have one year from this date to ensure compliance with the Electronic Payment Regulation.

Conclusion

The Central Bank has clearly sought to curb the creation and operation of "shadow payment systems" outside of the existing regulatory landscape. While the Central Bank clearly understands the increasingly significant role non-financial institutions play in payment services, it seeks to balance innovation with fundamental assurance to consumers that market players operate in a safe and secure environment, and serves to maintain the public's trust in the payment ecosystem.

The scope is unprecedented — catching non-financial institutions and imposing requirements traditionally imposed on financial institutions. However, there are a number of areas the Central Bank needs to clarify and/or address further. Some key matters include:

- How international providers of stored value facilities can make their existing services available locally to their existing customer base (*e.g.,* a tourist visiting UAE using a foreign e-wallet to purchase goods from a local merchant). The Electronic Payment Regulation focuses on local presence and local ownership across the licensing categories. Clarity is required on whether Agents could possibly include local entities facilitating the processing of transactions locally via a user's stored value account provided by an international provider

- A clearer position on virtual currencies. As noted earlier, there is ambiguity on whether these are prohibited entirely in the UAE or whether licensed entities are prohibited from transacting in such currencies.

- The level of flexibility regarding compliance that the Central Bank is willing to adopt with respect to reputable international companies seeking to enter the market. For example, if a global provider of e-wallet services has global operating standards (*e.g.,* provision of transactional data, account loading limits and transaction limits) that nonetheless offer a similar degree of protection to users in the UAE or are otherwise reasonable (*e.g.,* account set up fees and transaction processing fees), will these need to be adjusted to meet the Electronic Payment Regulation requirements?

- Licensing requirements for PSP categories. These will be specified under a separate licensing manual the Central Bank is currently developing. Clarity is required on whether the one-year transition period will be adjusted to commence from publication of this manual to allow sufficient time for concerned entities to comply.

- The range of penalties the Central Bank may impose on non-compliant entities, including the basis of calculating penalties, *e.g.,* whether these will be fixed amounts or percentages of generated/anticipated revenue.

Despite the lack of clarity on the above, existing payment service providers and new market entrants need to appreciate the wide scope and requirements of the Electronic Payment Regulation, and should consider compliance measures as soon as possible.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Brian Meenagh
brian.meenagh@lw.com
+971.4.704.6344
Dubai

Madonna Kobayssi
madonna.kobayssi@lw.com
+971.4.704.6307
Dubai

You Might Also Be Interested In

New EU Data Protection Rules Move the M&A Goalposts

"Yarovaya" Law – New Data Retention Obligations for Telecom Providers and Arrangers in Russia

Are Changes in Store for the Stored Communications Act?

What You Need to Know About the Cybersecurity Act of 2015

5 Preventative Steps to Manage Legal Risk Following a Cybersecurity Breach

---