Regulatory and Compliance Issues Related to Data in Payments

By: Alaina Gimbert

Prepared for:
ABA Spring Meeting

Data: Navigating its Promises and Problems for Evolving Payment Services

March 2019
Topics

• Tokenization and the Travel Rule

• ISO 20022 and Data Issues
Tokenization and the Travel Rule

What is tokenization?
- Tokenization is the conversion of sensitive data to non-sensitive data
  - Use of a unique, generated numbers in place of bank account and routing information in payments
- Use of tokens in payments results in fewer databases/systems where sensitive card and account data is stored, thereby decreasing the risk of compromise of card and account numbers
- To date tokenization has mostly been used in card transactions
Tokenization and the Travel Rule

- What is the Travel Rule?
  - The Travel Rule (31 CFR § 1010.410) was implemented in 1995 as part of the BSA regulations.
  - The rule requires
    - financial institutions involved in covered funds transfers to include certain information in their payment orders in order to assist law enforcement investigations of money laundering involving funds transfers
    - the payer’s financial institution must include in a payment instruction at the time it is sent to the next bank in the funds transfer chain, the name and, if the payment is ordered from an account, the account number of the originator
  - By its terms, the travel rule does not permit the use of a token as a substitute for the payer’s account number in covered funds transfers.
  - While not the same as tokenization, the use of an alias such as an email or phone number as a substitute for the payer’s account number would also be problematic.
  - Tokenization of the payee’s account number is OK because the travel rule does not require that the payee’s account number be provided. The payer’s bank just has to include information about the payee in a payment to the extent the bank receives the information.
Tokenization and the Travel Rule

Scope of the Travel Rule

– The travel rule applies to a limited set of payment types and therefore has not been an issue for tokenization efforts to date, which have largely focused on tokenization of card numbers in mobile payments.

– Specifically, the travel rule excludes any funds transfer that is
  – less than $3,000, or
  – governed by the Electronic Funds Transfer Act (EFTA), or
  – made through an automated clearinghouse (ACH) or automated teller machine (ATM) or at point of sale (POS)*, or
  – made between certain parties, such as bank to bank transfers (see, 31 CFR Part 1010 for full list of exclusions)

– Given this long list of exclusions, the travel rule has historically only applied to wire transfers by banks and money transmissions by money services businesses.

* Most card payments fall under the POS exclusion. However, in recent years card networks have introduced “push” payments that are not usually used at POS. To the extent these non-POS push payments are not subject to EFTA and $3,000 or more, they appear to be subject to the Travel Rule.
Tokenization and the Travel Rule

- Tokenization efforts are now focusing on non-card payments such as automated clearing house (ACH) payments and real time payments through the new RTP network.
- Funds transfers through ACH are excluded from the Travel Rule.
- Transfers through the RTP network are not excluded and to the extent they are not governed by EFTA (i.e., are business-to-business payments) and are $3,000 or more, they are subject to the rule.
  - RTP system transfers that are subject to the Travel Rule must include the payer’s account number (rather than a token)
  - The current tokenization model for the RTP system allows a payer’s bank to determine on a transaction by transaction basis whether to tokenize the originator’s account number, thereby allowing compliance with the Travel Rule.
  - However, the Travel Rule requirement to include the payer’s account number is in tension with today’s cyber security concerns and the benefits of tokenization.
Tokenization and the Travel Rule

During the rule making for the Travel Rule in the mid-90s, the requirement to include the payer’s account number was viewed as very important to law enforcement while the risk of fraud due to inclusion of account numbers was deemed low.

- “Treasury has determined that the inclusion of account numbers in transmittal orders will present only a minor increase in the risk of fraudulent transfers. Banks generally have security procedures that include passwords, codewords and, in the case of electronic transmissions, confirmation to ensure that only authorized parties issue payment orders. These and other protective measures greatly reduce the potential for fraud, to a level at which that risk does not outweigh the immediate and tangible benefit to law enforcement derived from the inclusion of account information in transmittal orders.” 60 Federal Register 236 (January 3, 1995)

The requirement should be re-evaluated in light of the current prevalence of data breaches and cyber-security threats

- The data privacy protections enabled by tokenization should not be limited based on the payment system used.
- Can law enforcement needs be met by tracing the unique token and relying on the payer’s bank to provide the payer’s account number associated with the token?
ISO 20022 and Data Issues

What is ISO 20022?

– ISO 20022 is an international financial messaging standard.
– There are ISO 20022 standards for payments, securities, and trade transactions.

Today most payment systems employ their own “home grown” (proprietary) message formats.

– For payments such as wires that move between different payment systems this means that payments must be converted between multiple formats.
– For high value payments (wires), these different formats have been “mapped” to one another such that banks know where to put data from one format into another. Nevertheless, this need to convert payments into different formats is inefficient and also presents the risk that when converting from one format to another data may be dropped or squeezed into unexpected parts of a payment message.
– For law enforcement and others who need to decipher payment messages, these means they need to be able to read different payment “languages.”
ISO 20022 and Data Issues

- Many countries have implemented or are in the process of implementing ISO 20022 for their high value (wire) systems.
  - In the US ISO 20022 conversion is actively underway for CHIPS and Fedwire and currently expected to be completed in 2023.
  - SWIFT, which operates an international financial messaging system, is also converting to ISO 20022 and currently expected to complete its conversion before CHIPS and Fedwire.

- Conversion to ISO 20022 should enable more efficient international payments as banks will no longer need to translate between different proprietary formats.

- Other benefits of ISO 20022
  - Modern html language
  - More “transparency” (i.e., more data)
  - More structured (i.e., more specific places where data resides)
ISO 20022 and Data Issues

More about the data

- In addition to essential payment routing and party identification, ISO messages are designed to capture additional payment-related data in structured fields.
  - This additional data is either not captured in wire messages today or is included in free-format fields.
  - Additional data includes various “participants” (technical agents, instructing agents, parties to whom the originator or beneficiary owes some obligation or with whom it has some relationship), as well as remittance detail.
  - ISO provides structured address fields for all non-bank entities that are identified in a message. (Ultimate Debtor, Debtor, Initiating Party, Creditor, Ultimate Creditor, Invoicer and Invoicee in the structured remittance fields)
## ISO 20022 and Data Issues
### Comparison of Entities Identified in a Payment Message (ISO 20022 and Current CHIPS)

<table>
<thead>
<tr>
<th>ISO 20022</th>
<th>CHIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ultimate Debtor</td>
<td>&lt;UltDbtr&gt;</td>
</tr>
<tr>
<td>Debtor</td>
<td>&lt;Dbtr&gt;</td>
</tr>
<tr>
<td>Initiating Party</td>
<td>&lt;InitgPty&gt;</td>
</tr>
<tr>
<td>Debtor Agent</td>
<td>&lt;DbtrAgt&gt;</td>
</tr>
<tr>
<td>Instructing Reimbursement Agent</td>
<td>&lt;InstgRmbrsmntAgt&gt;</td>
</tr>
<tr>
<td>Instructed Reimbursement Agent</td>
<td>&lt;InstdRmbrsmntAgt&gt;</td>
</tr>
<tr>
<td>Third Reimbursement Agent</td>
<td>&lt;ThrdRmbrsmntAgt&gt;</td>
</tr>
<tr>
<td>Previous Instructing Agent</td>
<td>&lt;PrvsInstgAgt&gt;</td>
</tr>
<tr>
<td>Instructing Agent</td>
<td>&lt;InstgAgt&gt;</td>
</tr>
<tr>
<td>Instructed Agent</td>
<td>&lt;InstdAgt&gt;</td>
</tr>
<tr>
<td>Intermediary Agent 1</td>
<td>&lt;IntrmyAgt1&gt;</td>
</tr>
<tr>
<td>Creditor Agent</td>
<td>&lt;CdttrAgt&gt;</td>
</tr>
<tr>
<td>Creditor</td>
<td>&lt;Crdtr&gt;</td>
</tr>
<tr>
<td>Ultimate Creditor</td>
<td>&lt;UltCdttr&gt;</td>
</tr>
</tbody>
</table>

- Originator: [500] or [502]
- Originator’s Bank: [510] or [512]
- Instructing Bank: [520] or [522]
- CHIPS Sender: [201]
- CHIPS Receiver: [211]
- Intermediary Bank: [400], [401], or [402]
- Beneficiary Bank: [410], [411], or [412]
- Beneficiary: [420], [421], or [422]
ISO 20022 and Data Issues
Comparison of Information about Non-Bank Entities (ISO 20022 and Current CHIPS)

<table>
<thead>
<tr>
<th>ISO 20022</th>
<th>CHIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Ult. Debtor, Debtor, Initiating Party, Creditor, Ult. Creditor)</td>
<td>(Originator and Beneficiary)</td>
</tr>
<tr>
<td>Name</td>
<td>Name<em>Information</em>Information</td>
</tr>
<tr>
<td>Street Address</td>
<td>(233 characters)</td>
</tr>
<tr>
<td>Building Number</td>
<td></td>
</tr>
<tr>
<td>Postal Code</td>
<td></td>
</tr>
<tr>
<td>Town Name</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
<tr>
<td>Birth Date</td>
<td></td>
</tr>
<tr>
<td>Province of Birth</td>
<td></td>
</tr>
<tr>
<td>City of Birth</td>
<td></td>
</tr>
<tr>
<td>Country of Birth</td>
<td></td>
</tr>
<tr>
<td>Other Identification</td>
<td></td>
</tr>
<tr>
<td>Country of Residence</td>
<td></td>
</tr>
<tr>
<td>Phone Number</td>
<td></td>
</tr>
<tr>
<td>Mobile Number</td>
<td></td>
</tr>
<tr>
<td>Fax number</td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td></td>
</tr>
<tr>
<td>Other Contact Details</td>
<td></td>
</tr>
</tbody>
</table>
ISO 20022 and Data Issues

What’s the problem with more data?

While there are benefits to more entities and more data about entities being included in wires, there is an inherent tension between additional data and the regulatory and compliance implications of the data.

For example, the common OFAC screening approach for wires is to screen everything in the payment message.

But not all entities identified in an ISO 20022 payment message have a property interest in the payment and may not be relevant to OFAC screening.

Screening of the entire ISO 20022 message may result in more false hits than current formats and slow the speed of legitimate commerce.

If AML or OFAC compliance staff are not familiar with the new kinds of entities that are identified in ISO 20022 payments, they may have difficulty determining the relevance of “hits” or other alerts involving the entities.

Do these additional entities become “noise” in screening and monitoring systems? Might a more targeted screening and monitoring approach be needed to address more data rich payment types?
ISO 20022 and Data Issues

➢ What’s the problem with more data?
   – There are also compliance issues when banks must convert from ISO 20022 to “smaller” payment formats information must be truncated, inserted into “catch all” fields, or dropped.
   – If SWIFT completes its conversion before CHIPS and Fedwire, banks will face this issue for their inbound, international SWIFT payment messages.
   – The Federal Reserve has proposed that it would permit two versions of ISO 20022, one which is “bigger” than the other, to coexist in the US market for Fedwire participants. (See, “New Message Format for the Fedwire Funds Service,” 83 Federal Register 31391 (July 5, 2018))
   – This may become the source of regulatory criticism for banks that choose to stay with the “smaller” version (which may be appropriate for the kinds of payments they make) or for correspondent banks that accept payments from their respondent customers in the “smaller” version.
   – Many fields within ISO 20022 are optional and only intended to be used for particular use cases. However, regulators may not understand this and view “blank” fields as problematic.
ISO 20022 and Data Issues

What’s the problem with more data?

- Evolving privacy expectations appear to be at odds with the identification of and data related to persons who are not parties to the payment.
- If you are not the payer or payee of the payment, would you expect that your name, address, and other identifying information is being included in a payment merely because you have some relationship to or perform some service for the payer or payee?
- While payment data is generally protected from disclosure under the Gramm Leach Bliley Act (so long as it is held by entities subject to the Act), payment data is subject to bank OFAC screening and AML monitoring as well as disclosure under law enforcement and civil subpoenas.
HOW MODERNIZED LEGAL FRAMEWORKS CAN ACCELERATE DATA-DRIVEN INNOVATION: CHALLENGES AND OPPORTUNITIES

By Ross Leckow and Jess Cheng

The following discussion was adapted from an article by the authors above, for inclusion in the materials pertaining to the March 2019 Continuing Legal Education Program, Data: Navigating Its Promises and Problems for Evolving Payment Services, at the American Bar Association’s Business Law Section Spring Meeting. Additional contextual discussion has been added below specifically for the purposes of this CLE program.

The Bali Fintech Agenda, jointly launched by the International Monetary Fund and World Bank at the 2018 Annual Meetings, offers a blueprint to guide national authorities in harnessing fintech’s opportunities while managing the risks. For authorities in the early stages of formulating their fintech strategies, as well as for those well into their digital journeys, a key consideration is the modernization of legal frameworks. What happens when financial products, business models, and market practices evolve to the point that existing legislation, which may not have been designed with them in mind, is no longer a good fit? The resulting lack of legal clarity and certainty can needlessly create inefficiencies and barriers to innovation.

Two recent trends in financial sector legislation illustrate how legal frameworks can be modernized in response to emerging technologies, changing consumer expectations, and new market dynamics. The Payment Services Directive 2 (PSD2) and the General Data Protection Regulation (GDPR) are the European Union’s two most important responses to these developments. They are also drivers of change in their own right, giving individuals greater control over their data. The PSD2 calls for banks to open access to customer account and transaction data, with a customer’s consent, to third-party service providers, such as fintech companies and other banks, with the goal of improving competition and innovation in the EU market for payment services. Its scope is limited to payment services, with a focus on facilitating the provision of innovative payment services and new actors, among other goals. In contrast, the GDPR is devoted to protecting personal data on a more general level, irrespective of business line or industry. The GDPR requires companies, including banks, to protect and handle more carefully what personal data they have, with the aim, in particular, of giving more control to individuals over their personal information.

For many jurisdictions looking to keep apace of rapid technological changes, modernized laws like the PSD2 and the GDPR are helpful comparison points. These two legislative initiatives

1 Ross Leckow is Deputy General Counsel at the IMF; Jess Cheng is counsel at the IMF.
are each separately underpinned by worthy rationales; and each reflect a careful balance between multiple competing policy interests. However, they do not exist in a vacuum and, in implantation, must be considered together. Particularly at their intersection in the sharing of an individual’s payments and account data, thorny questions may arise. How does one reconcile the interaction between the PSD2, aimed at increasing the seamless sharing of payment data, and the GDPR, aimed at regulating the processing of personal data?

Important legislative initiatives at this very intersection are being considered around the world, in recognition that a global economy increasingly driven by digital data presents new risks and opportunities. Countries such as Japan and Brazil, as well as the U.S. state of California, have recently announced new data privacy rules in line with the GDPR. At the same time, some jurisdictions are considering laws to address aspects covered in PSD2. Mexico’s recently enacted FinTech Law mandates the use of application programing interfaces (APIs) for sharing financial, aggregate, and transaction data of customers (with their prior consent) between financial institutions, including fintech companies. Australia has announced plans to implement a similar open banking initiative that would enable customers of banks to share their financial transactional data more easily with third parties online. The Canadian government recently announced a policy review of open banking, examining its potential positive impact on consumers while considering the risks to privacy, data security, and financial stability. Of course, modernized financial legislation comes in many flavors, reflecting a diversity of national priorities and circumstances that call for different responses. For example, authorities can pursue data-sharing initiatives without a legislative mandate for an open banking ecosystem, as authorities in Singapore, Hong Kong, and Malaysia have opted, subject to limitations under their respective data privacy regimes.

What has changed?

These legislative initiatives are in response to three mutually reinforcing recent developments: digitization, changing customer expectations, and new market dynamics. The cost of collecting, transmitting, and storing vast amounts of data has sharply declined. Hand-in-hand with the new abundance of data, related technologies like automation and data analytics extract more value, more efficiently and at lower costs. In the financial sector, technological advances—such as digital wallets, mobile banking, distributed ledgers (blockchain), APIs, cloud technology, and the “Internet of Things”—are creating new ways to pay, data-driven personalized financial services, and a digitalized end-to-end payments chain.

Just as the uptake in digital payments enables the capture of much more data (such as location, transaction counterparties, and shopping patterns), consumer attitudes are changing too. Beyond expectations of greater speed and convenience in the payments experience, a greater tolerance may be emerging among consumers for the amassing and sharing of data that once might have been perceived intrusive. Such qualms may gradually, if not already, be outweighed by the immediate benefits of personalized and seamless financial services.
New companies are emerging to meet these evolving consumer expectations, using innovative financial technologies to focus on improving specific inefficiencies and frictions. This strategy of offering a superior niche alternative stands in contrast to the traditional banking model of providing a broad array of products and services, as a one-stop shop for a customer’s financial needs. However, these newcomers may initially lack network reach and market adoption that established incumbents enjoy, with the result that some may partner with banks that already possess the scale of customers.

The General Data Protection Regulation

The GDPR, which entered into force in 2018, reflects modernization of data privacy legislation in response to technological change. A key aim of the GDPR is to empower individuals and give them control over their personal data in today’s data-driven world. Under its principle of data minimization, data handling should only involve as much personal data as is required to successfully accomplish a lawful purpose. Moreover, data collected for such purposes cannot—in principle—be repurposed without further consent.

The GDPR also gives individuals new, expanded rights over their personal data, including a new “right to be forgotten” and a “right to erasure” (that is, to have one’s personal data erased, the dissemination and processing of such data terminated, with such rights balanced against “the public interest in the availability of the data”), a “right to rectification” (that is, to ask for information to be corrected), and a “right to portability” (that is, to retrieve or have transferred one’s personal data, free of charge, in an electronic format).

There are important consequences for not complying with the GDPR: in addition to heightening the responsibilities of companies handling personal data, the GDPR is also significant in heightening their liabilities—with fines of up to €20 million or 4% of global annual revenue, whichever is higher. These consequences hold for companies regardless of their place of establishment. Indeed, the GDPR applies not only to organizations located within the EU, but also those located outside of the EU that offer goods or services to, or monitor the behavior of, a person residing in the EU.

The Payment Services Directive 2

Like the GDPR, the PSD2 is a modernization effort to update the legal framework to account for new types of data-driven developments, specifically in the context of retail payment services. The PSD2, a directive with a transposition deadline of January 13, 2018 for member states to implement it into national laws, repeals the Payment Services Directive of 2007. It addresses the emergence of two new types of payments-related service providers: (i) those that enable customers to more conveniently initiate a payment from their account with a different bank and (ii) account aggregators that enable customers can use to pull together data—such as transaction histories and balances—from their accounts at several other banks, giving a broad view of their finances in one consolidated place. A range of services can be layered upon this dashboard: analyses of spending habits, financial advice, and personalized advertisements or
offers. Payments data can also be transferred to other third parties that combine it with data from other sources to yield enhanced benefits to customers.

In this way, the PSD2 could strengthen an individual's ownership of their personal data. It enables individuals to easily and securely share data held by their bank with other licensed service providers, such as other banks or fintech companies. The PSD2's rationale is unique: its legal framework has been specifically designed to foster competition and innovation in payments services. It grants payment service providers a fundamentally new legal right of access to information relating to the accounts of customers with banks—for the purposes of their contractual relationship with the customer. As a result, banks lose their historic monopoly on their customers' transaction data. In this way, PSD2 aims to open up the payments market for innovative bank and non-bank payment services providers, legislatively accelerating competition and innovation.

The Intersection Between GDPR and PSD2

Within their respective regimes, the GDPR and the PSD2 each separately reflect a careful balance between competing policy interests and the pursuit of worthy policy goals. Yet they must be interpreted alongside each other. Under the PSD2, payment service providers (which may include banks) require access to a customer’s account information at other banks to provide their services; this access entails the handling of the customer’s personal data (such as the name, account number, and transaction information) that is subject to the GDPR. While the PSD2 requires banks to open access to customer account and transaction data for third party service providers (to the extent needed to provide the payment service and with the customer’s consent), the GDPR imposes on them rigorous requirements to protect customer data, paired with severe penalties for failure to do so.

The European Commission has provided some useful clarifications with regard to this intersection. For example, it is of the view that the provisions of the PSD2 on data protection must be interpreted in light of the GDPR and are subject to its terms. Indeed, in the spirit of the GDPR’s data minimization principle, the PSD2 prohibits a service provider from using the personal data it has obtained for purposes other than performing the specified service. However, might a clever service provider circumvent this limitation by simply broadly defining the service it offers: for example, not only account aggregation, but also personalized offers for other products and services? If customers were to sign up for that package and consent to such purposes, the service provider would as a practical matter have broadened grounds for the lawful processing of their personal data.

Nevertheless, thorny questions may nevertheless remain in applying the two modernized laws in practice and balancing the development of a competitive market for payment services with the protection of personal data. A bank may appropriately opt not to provide a customer’s chosen service provider access to transaction data out of fear of breaching the customer’s privacy rights under the GDPR, if in particular the service provider might be unreliable or the
authentication processes insufficient to prevent fraud. However, to avoid having the risk of such action from being construed as an illegal restriction of competition, the bank must establish that it has reasoned doubts justifying its refusal to grant access. Any such decision would be subject to judicial review under the PSD2.

Interestingly, the third-party service providers that have access to customer data under the PSD2 can include large technology companies entering into the payment services market. Applications of PSD2 in this asymmetric context may have unintended consequences for competition—particularly as such non-bank technology companies and internet platforms do not have a similar requirement to share customer information.

**Conclusion: A way forward**

Many of these details remain a work in progress and will be refined as the market impacts of open banking play out and the refinement of modernized legal principles continues. The weight given to competition, data protection, and privacy, as well as how policy choices are implemented in practice, will vary across countries. It is clear, however, that in an increasingly information-driven economy, legal frameworks governing the sharing and use of data are of critical importance.

These issues do not merely represent theoretical concerns. Rather, they impact us directly, our money, and our identity. Therefore, there is one critical element to achieving success in catalyzing competition and innovation in the financial sector by facilitating the entry of new players while, at the same time, pursuing important data protection priorities: increasing awareness among individuals of their rights to privacy and data protection in the digital world. PSD2 empowers individuals to share their account information, removing the bank’s role as gatekeeper. Individuals cannot effectively exert control or exercise rights under the GDPR if they do not attach due value and sensitivity to their personal data. More fundamentally, however, it is essential that they know their rights under the law.