PAY gov
prepaid.mobile.emerging payments.

Lead Sponsor of *Pay Gov*
incomm

Inside

TOP STORY

CFPB Issues 9 Principles for Faster Payments

By Loraine DeBonis, Editor-in-Chief

As the U.S. payments industry looks to speed up payments—NACHA and The Clearing House (TCH) each have faster payments initiatives in the works—the CFPB wants to make sure protecting consumers is top of mind. On July 9, the agency released nine guiding principles to ensure any new system is secure, transparent, accessible and affordable to consumers, with robust protections related to fraud and error resolution.

"It is a lot easier to build something right from the start than it is to retrofit it," said CFPB Director Richard Cordray. The CFPB principles include guidance on consumer control; data and privacy; fraud and error resolution protections; transparency; cost; access; funds availability; security and payment credential value; and strong accountability mechanisms to curtail misuse. On the issue of cost, the bureau didn't suggest specific pricing but said systems should be affordable and disclosed in a manner that enables consumers to see the full cost of making a payment and facilitates comparison shopping.

"The CFPB's 'principles' may foreshadow another attempt by the CFPB to take an expansive approach to its jurisdiction," according to Scott M. Pearson, partner, and Kevin D. Leitão, of counsel, Ballard Spahr LLP. In an article posted on the law firm's *CFPB Monitor* blog, the lawyers note that some payments firms, such as large banks that provide payments services, are subject to CFPB supervision and the CFPB also has the authority to enforce

continued on page 17

WASHINGTON WATCH

CFPB Turns FIVE

The CFPB turns 5 on July 21. Created by the Dodd-Frank Act of 2010, the bureau's mandate is to protect consumers by carrying out federal consumer financial laws. After a one-year standup period, the bureau began most activities, including enforcement, on July 21, 2011. From almost the outset, the bureau expressed its interest in prepaid products, culminating in the long-awaited introduction of its NPRM on Prepaid Accounts on Nov. 13, 2014. Final regulations are expected in first quarter 2016.

Director Cordray Testifies Today at Senate Banking Committee

Richard Cordray

CFPB Director Richard Cordray is scheduled to testify today before the Senate Banking Committee, starting at 10 a.m. Eastern. (Click here to link to the Webcast.)

Also expected—if this hearing follows the last one—are some pointed questioning and interesting exchanges. Sen. Richard Shelby (R-Ala.), chair of the Senate Banking Committee, is an outspoken critic of the bureau, and this is his show. But, perhaps, tempering the chairman's questioning will be equally outspoken committee members and major CFPB supporters, Senators Elizabeth Warren (D-Mass.), Sherrod Brown (D-Ohio) and Chuck Schumer (D-N.Y.).

Although the hearing may last for several hours, it's worth the time to listen in.

Dates to Note

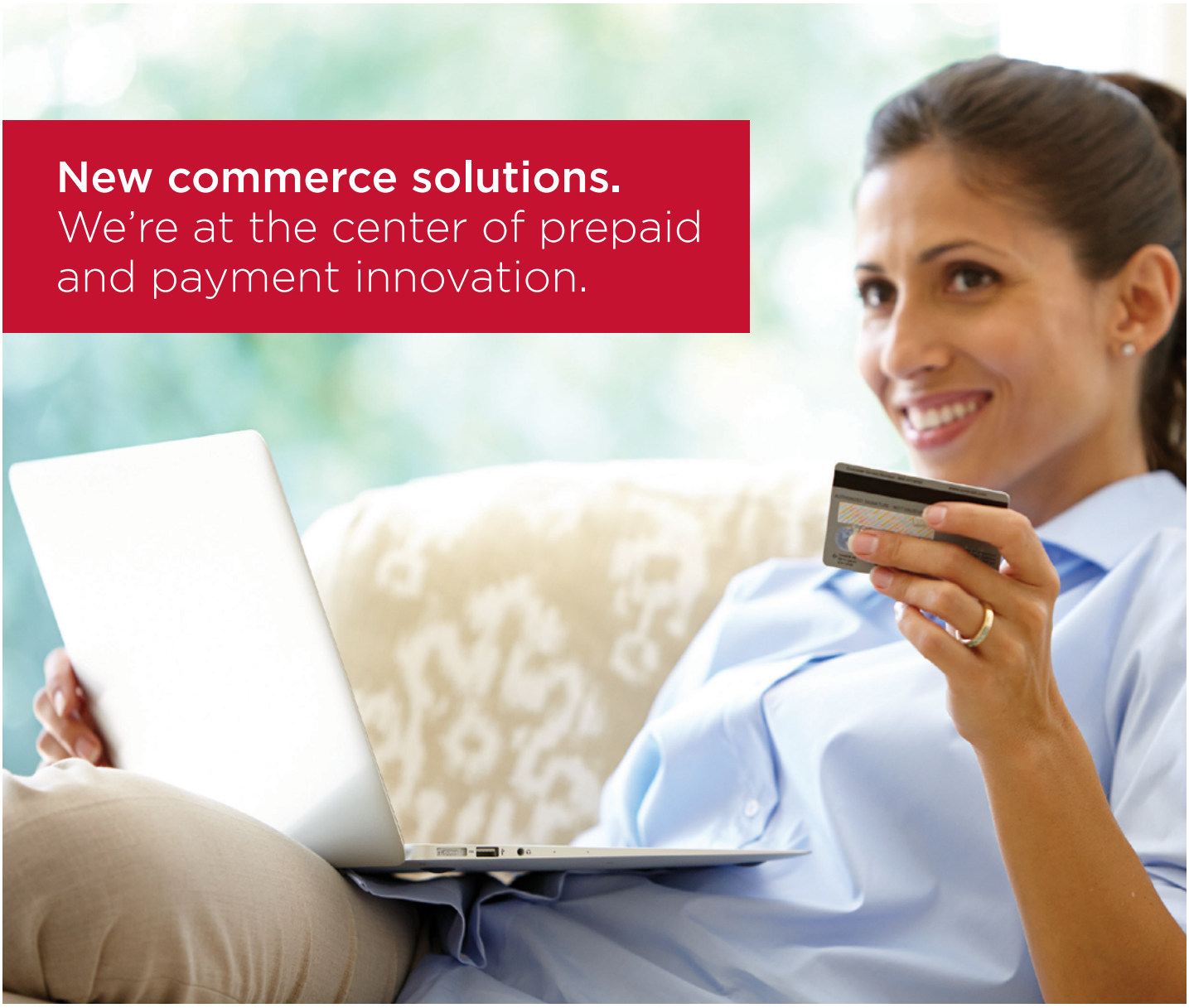
July 31: Comments due on N.Y. DOL Payroll Regs (extended)

Aug. 10: Fed must establish why tx-monitoring costs are outside fraud-prevention adjustment

Aug. 31: Comments due on CFPB's Consumer Complaint Database

Sept. 17: Comments due on U.K. Law Commission's proposal on gift cards and retailer insolvency

Oct. 2015: Network liability-shift deadline for EMV in the U.S.



For more than 20 years, InComm has been expanding the boundaries of technology and innovation, creating empowering tools that transform the shopping experience—whether it's in stores, online or on mobile devices.

With a foundation of technology deeply integrated into retailers' point-of-sale (POS) systems, we provide connectivity to a wide range of services that benefit retailers, brands and consumers. Our leading-edge commerce solutions help retailers build prepaid card destinations, connect brands to new markets, plus help consumers enjoy greater value.

Across hundreds of thousands of global distribution points, we're at the center of modern commerce, making prepaid and payments more convenient, rewarding and secure.

To learn more, contact your InComm sales representative.

InComm

250 Williams Street | Atlanta, Georgia 30303 | 800-352-3084 | incomm.com

Viewpoint

In Viewpoints, prepaid and emerging payment professionals share their perspectives on the industry. Paybefore endeavors to present many points of view to offer readers new insights and information. The opinions expressed in Viewpoints are not necessarily those of Paybefore.

Amendments to Canada's AML Legislation: What's New and What's Next

Regulated entities that verify identity in connection with the issuance of stored value cards may find more flexibility in the principle-based approach to identity verification outlined in the proposed regulations.

By Jacqueline Shinfield, Blakes

On July 4, 2015, Canada's federal government released amended regulations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

While there are some additional regulatory burdens imposed on regulated entities in respect of domestic politically exposed persons (PEPs) and additional components to be considered in risk assessments, many of the proposed changes will be welcomed by regulated entities as they provide more principle-based regulation and less prescriptive requirements, especially in the context of verification of identity and electronic signatures. These amendments should allow regulated entities more flexibility in offering retail financial services online without the regulatory constraints that currently exist.

In addition to the amendments made to the general regulations, the Administrative and Monetary Penalties (AMPs) Regulations also have been revised to include compliance obligations that were previously unaddressed by these regulations. There also have been some amendments made to the Suspicious Transactions Reporting (STR) regulations.

Jacqueline Shinfield

*In 2015, **Jacqueline Shinfield** was recognized as a Top 10 Payments Lawyer in a poll of visitors to Paybefore.com. A partner in Blakes' financial services regulatory group, she can be reached at jacqueline.shinfield@blakes.com.*

MATERIAL AMENDMENTS

Identity Verification

One of the most challenging compliance obligations under the current regulations are the prescriptive requirements setting out how regulated entities must verify identity, especially in the non-face-to-face context. Under the current regulatory scheme (except in the credit card context) it is difficult, if not impossible, for regulated entities to verify identity on a non-face-to-face basis (for example, online or over the phone) in real time. This has proven to be a frustrating experience, especially given the growth in online and mobile commerce since the original non-face-to-face verification methods in the regulations introduced in 2008.

The proposed amendments now provide regulated entities with greater flexibility in how they carry out identity verification and are more e-commerce friendly. Interestingly, all of the current identity verification methods have been replaced by the new ones, even in the credit card context. The new permitted methods of identity verification include the following:

- Referring to an identification document containing a photograph (and a name) that is issued by a federal or provincial government (other than a municipal government) or by a foreign government, and by verifying that the name and photograph are those of that person. This requirement for a photograph is a new requirement; previously a regulated entity could rely on any government-issued identification. This is clearly a more prudent approach to identity verification from a risk-based perspective. There also is an additional requirement to actually verify that the name and photograph are those of that person.
- Referring to information concerning the individual being identified on request from a federal or provincial government body that is authorized in Canada to ascertain the identity of persons, and by verifying that either the name and address or the name and date of birth contained in the information are those of the person whose identity is being verified.
- Referring to a person's Canadian credit file that has been in existence for at least three years and verifying that the name, address and date of birth contained in the credit file are those of the person whose identity is being verified. This provision is a welcome change as under the current regulations, reference to a credit report without a secondary source is not a compliant means of identity verification.
- Confirming that an affiliated entity (including a member of the same financial services cooperative or credit union central) that is regulated under the PCMLTFA or a non-Canadian entity that carries on a similar business outside of Canada previously has ascertained the person's identity in compliance with any of the permitted methods and by verifying

VIEWPOINT CONT.

Amendments to Canada's AML Legislation: What's New and What's Next

that the name, address and date of birth contained in such entity's records are those of the person whose identity is being verified.

• By doing any *two* of the following:

– Referring to information from a reliable source containing the name and address of the person being identified and verifying that the name and address are those of the person.

– Referring to information from a reliable source that contains the name and date of birth of the person being identified and verifying that the name and date of birth are those of the person.

– Referring to information that contains the name of the person being identified and confirming that the individual has a deposit account or credit card or other loan account with a Canadian financial entity and verifying that information.

In utilizing this two-out-of-three method of identity verification, the proposed regulations require that the information that is referred to must be from different sources and that the person whose identity is being verified cannot be utilized as a source.

These provisions will allow for greater flexibility in performing identity verification and are welcome principle-based requirements. As a result of these changes, the use of a "reliable source" now will become the critical element of any identity verification. What is a "reliable source" likely will be a subject of exploration for many regulated entities, but the Impact Analysis Statement released with the Regulations indicates that this is a matter that Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) will be preparing guidance to address.

In respect of all identity verification methods outlined above, the proposed Regulations provide that where a document is used to ascertain identity under any of the above noted methods, it must be original, valid and current. Other information that is used (other than an identity document) must not include an electronic image of a document.

Other questions that arise from the foregoing methods include:

• What will be deemed to be a "reliable source"? This is one area that likely will be analyzed from many angles by regulated entities. For example, is a hydro bill containing a name and address a "reliable source"? In that regard, it is reasonable to conclude that the current acceptable methods for non-face-to-face identification verification would be viewed as "reliable sources."

• What is meant by the requirement in many of the provisions to "verify" the information? Under the current regulations, for face-to-face identity verification, the regulations require a regulated entity to refer to an identity document. The proposed regulations require regulated entities to take a further step to "verify that the name and photograph are of that person." Is there an implicit requirement to ask for another piece of identification to verify the information?

Another welcome change in the proposed regulations is the ability of a regulated entity to rely on identity verification previously undertaken by another person, even if that person is not regulated under the PCMLTFA.

Under the current regime, to rely on another person to perform identity verification, a regulated entity is required to enter into a written arrangement for that purpose where the person agrees, as agent, to undertake the identity verification.

The proposed regulations significantly expand the circumstances where a regulated entity can rely on actions taken by another in the identity verification context. Specifically, a regulated entity now can rely on measures that previously were undertaken by another person (acting independently) where that person verified the identity of a person, even if the person was doing so outside of the PCMLTFA context. In addition, if a person verified identity information for another regulated entity under a previous agency relationship, then a regulated entity can rely on that identity information as well. In all circumstances, a written arrangement needs to be in place where the regulated entity appoints the person as agent and all verification information must be obtained from the agent. In addition, the regulated entity must be satisfied that the information is valid and current and that the prescribed identity verification methods were complied with. These provisions will bring more certainty in the context of portfolio acquisitions by allowing purchasers of financial assets to rely on verification previously done by the vendor. It also will provide greater flexibility for identity verification in the day-to-day assignment of financial instruments and contracts.

The one uncertainty in these provisions is the requirement for the information to be "current" in order to be relied upon. In that regard, it is unclear what is intended by this provision. If identity was verified three years ago, is it current? What about one year ago? This is something that regulated entities should consider in providing commentary under the regulations.

One of the more significant burdens under the current regulatory regime is the restriction on a regulated entity's ability to rely on previous identity verification undertaken by it in respect of its own customers in the online context. In that regard, the current regulations only allow a regulated entity to rely on previous identity verification performed on an individual in those circumstances where the regulated entity "recognizes" the individual. FINTRAC has narrowly interpreted the term "recognize" to mean visual or voice recognition. As a result, it is impossible under the current regulatory regime to "recognize" a customer online. Thankfully, this provision has been modified so that a

VIEWPOINT CONT.

Amendments to Canada's AML Legislation: What's New and What's Next

regulated entity is now permitted to rely on previous identity verification it performed, provided it does not have any doubts about the information.

The nature of the amendments made in respect of identity verification demonstrates that the government carefully took into consideration stakeholder feedback to produce a more practical and relevant regulatory approach to client identification in light of the rapid pace of technological change and the online world in which financial services are more frequently being offered. The identity verification provisions will come into force on the day on which the regulations are registered.

Electronic Signatures

Another area under the current Regulations that historically has been difficult to comply with in the online world is the requirement imposed on certain regulated entities to obtain a "signature card" when opening an account. A "signature card" is currently defined in the regulations as "a record signed by a person who is authorized to give instructions in respect of an account."

Although the term "signature" includes an "electronic signature," FINTRAC has narrowly interpreted this provision to require an actual "wet" signature, allowing for a photocopy or faxed copy of the signature but not allowing for a true "electronic" signature, as that term is commonly understood.

The proposed regulations change the definition of "signature card" to include "electronic data" that constitute the signature of a person authorized to give instructions in respect of the account. In addition, a "signature" is now defined to include an electronic signature or other information in electronic form that is created or adopted by a client and that is accepted by the regulated entity.

The effect of these changes is to allow for a true electronic signature that can be compliant with the regulations, thereby facilitating account openings in the non-face-to-face environment.

Again, as with identity verification, these proposed changes update the Regulations to be more responsive to the digital environment in which regulated entities operate.

These provisions come into force on registration of the regulations.

Politically Exposed Persons

One other matter that the proposed Regulations accomplish is the implementation of the changes made to the PCMLTFA under Bill C-31 in respect of PEPs. For more information, see Viewpoint: Important Changes to Canada's AML Laws: Here We Go Again.

In that regard, the proposed regulations expand certain of the regulatory requirements that currently apply to foreign PEPs to include domestic PEPs as well as the heads of international organizations or family members or close associates of such persons.

In respect of the requirements on account opening (for financial entities and securities dealers) the proposed regulations now require the regulated entity to take reasonable measures to determine whether the account is being opened not only for a foreign PEP, but also for a domestic PEP, a head of an international organization, a family member of one of those persons or a person who is closely associated with a PEP (PEP Related Person).

Moreover, the requirement in the regulations imposed on both financial entities and securities dealers to take reasonable measures to determine if existing high-risk account holders are foreign PEPs has been removed. Instead, financial entities and securities dealers will be required to take reasonable measures on a periodic basis, to determine if an existing account holder is a PEP Related Person. It is significant that there is no mention of "high-risk" accountholders in this provision, but rather, this periodic monitoring requirement applies in respect of all account holders. As a result, regulated entities subject to this requirement will have to build processes and procedures to address this monitoring requirement.

In addition to the foregoing, in respect of PEP Related Persons, the proposed regulations also provide that where a financial entity or securities dealer (or any of their employees) detect a fact that could reasonably be expected to raise reasonable grounds to suspect that a person who is an existing account holder is a PEP Related Person, the financial entity and securities dealer are required to take reasonable measures to determine whether the account holder is in fact such a person. Presumably, FINTRAC guidance will provide what circumstances would raise such "reasonable grounds," but it would appear that this new provision implicitly requires regulated institutions to implement additional monitoring procedures for PEP Related Persons.

While the proposed regulations require securities dealers and financial entities to implement requirements to determine if account holders are PEP Related Persons, the corresponding requirements to determine the source of funds to be deposited in the account, to obtain senior management approval to keep the account open and to engage in enhanced ongoing monitoring, only apply on an absolute basis to foreign PEPs and their family members and close associates. In respect of the requirements for domestic PEPs, heads of international organizations, family members or close associates of such persons, these additional requirements only will apply where the regulated entity considers, based on their risk assessment, that the risk of a money laundering or terrorist activity financing offense is high.

Accordingly, based on these new provisions in the regulations, it is clear that monitoring for domestic PEPs, heads of international organizations and their close associates and family members as well as the transactions that they engage in is now the "new normal" for regulated entities.

The amendments to the regulations in respect of transactions of CA$100,000 or

VIEWPOINT CONT.

Amendments to Canada's AML Legislation: What's New and What's Next

more that apply to financial entities, money services businesses and life insurance companies parallel the changes made in respect of accounts. Accordingly, regulated entities now will be required to determine if a triggering transaction for CA$100,000 or more is undertaken by any PEP Related Person. However, the accompanying requirements that apply to foreign PEPs (determining the source of funds, senior management review) will only apply to domestic PEPs, heads of international organizations and their family members and close associates, if the regulated entity, based on their risk assessment, considers that there is a high risk of money laundering or terrorist financing offence.

A final change to the PEP provisions that may help to alleviate the additional regulatory burden somewhat is in respect of timing requirements in which regulated entities are required to make a PEP determination. While the current regulations require the PEP determinations and accompanying review/approvals to be conducted within 14 days, the proposed Regulations extend this period to 30 days.

The new PEP requirements do not come into force until one year from the date of registration of the regulations.

Risk Assessments

The Regulations currently prescribe the factors that regulated entities must consider in performing their risk assessments, including clients and business relationships, products and delivery channels, and the geographic location of activities. The proposed regulations add two additional factors that must be considered in performing a risk assessment. These factors are:

- Any new developments in respect of, or the impact of new technologies on, the regulated entity's clients, business relationships, products or delivery channels, or the geographic location of their activities
- For a regulated entity that is a financial entity or securities dealer, any risk resulting from the activities of an affiliated Canadian financial entity or securities dealer or from the activities of an affiliated foreign entity that carries out similar activities.

While arguably the factors set out in the first item above already are encompassed by the current regulatory requirement to consider "any other relevant factor" in the risk assessment, the additional factors that apply to financial entities and securities dealers set out in the second item above may prove to be very challenging and likely will require an in-depth analysis of their global businesses. It is noted, however, that this requirement is consistent with the concept of "enterprise wide" compliance, which is becoming the regulatory expectation of regulators in Canada and globally.

These new requirements will come into force one year after registration of the regulations.

Reasonable Measures

There are numerous provisions in the Regulations that require regulated entities to take "reasonable measures" to perform certain actions or obtain certain information. Examples of these reasonable measure requirements include making third-party determinations, completing all information required on reporting forms and making PEP Related Person determinations.

The proposed amendments provide that if the reasonable measures taken are unsuccessful, regulated entities must keep a record that sets out the measures taken and why they were unsuccessful. These provisions do not come into force until one year after registration of the regulations.

Suspicious Transactions

The proposed regulations also make a few minor changes to the STR Regulations. However, amid those changes, there is one significant change that is worth noting. Currently, the requirement to file suspicious transaction reports under the STR regulations arises where a regulated entity first detects a fact "… that constitutes reasonable grounds to suspect that the transaction is related to the commission of a money laundering or terrorist activity financing offense." Accordingly, to be required to file a suspicious transaction report, a regulated entity must have a fact that constitutes reasonable grounds.

However, the amendments to the STR regulations now provide that such a report must be filed whenever a regulated entity detects a fact respecting a financial transaction "that could reasonably be expected to raise reasonable grounds" that the transaction is related to a money laundering or terrorist activity financing offense. As such, the standard for filing a suspicious transaction report changes from "constituting reasonable grounds" to "reasonably expected to raise reasonable grounds."

Although this seems like a simple wording change, in fact the new language lowers the threshold for reporting under the STR regulations. This will be something that regulated entities will need to take into consideration going forward in making determinations in respect of the filing of suspicious transaction reports. This provision comes into force on registration of the regulations.

There are other amendments made by the proposed Regulations, including modifying the requirement to obtain client credit files, a new definition of affiliated entities, some modifications to the record-keeping requirements and some transitional matters. Stakeholders have a period of 60 days to provide any comments on these regulations. As such, regulated entitles are best advised to review these provisions and submit comments to the Department of Finance if they have any material concerns.

It is noteworthy that not all of the regulatory changes addressed in Bill C-31 were made under this set of amending regulations. As such, there are clearly more amendments to come.

Viewpoint

In Viewpoints, prepaid and emerging payment professionals share their perspectives on the industry. Paybefore endeavors to present many points of view to offer readers new insights and information. The opinions expressed in Viewpoints are not necessarily those of Paybefore.

Canada's Digital Privacy Act Receives Royal Assent, but Breach Notification Provisions Lag Behind

By Wendy Mee and Dara Lambie, Blakes

After lengthy debates, the Digital Privacy Act (Bill S-4) finally received royal assent on June 18, 2015, and is now law. The federal government introduced Bill S-4 on April 8, 2014, which marked the government's third attempt since 2010 to amend Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). But despite the passing of this bill, the mandatory breach notification provisions will not come into force until regulations setting out prescribed requirements have been enacted. The key amendments to PIPEDA are discussed below.

In Force

• PIPEDA has been amended to clarify that an individual's consent is only valid if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which he/she is consenting.

• PIPEDA now contains a "business transaction" exemption that will allow organizations to use and disclose personal information without consent in connection with mergers, acquisitions, financings, etc. (both during due diligence and post-closing), provided certain conditions are met.

• Business contact information is no longer excluded from the definition of personal information. However, PIPEDA's provisions dealing with personal information will not apply to the collection, use and disclosure of business contact information by an organization solely for the purpose of communicating or facilitating communication with an individual about his/her employment, business or profession. Importantly, "business contact information" is given a broad definition and includes business email addresses, which previously was not excluded from the definition of personal information under PIPEDA. Notwithstanding this exemption, organizations should be aware that email communications must comply with requirements under Canada's Anti-Spam Legislation.

• The Privacy Commissioner of Canada now has the power to enter into a compliance agreement with an organization if the commissioner believes, on reasonable grounds, that the organization has committed, is about to commit or is likely to commit a breach of PIPEDA. A compliance agreement may contain any terms that the commissioner considers necessary to ensure compliance under PIPEDA. Failure to abide by the terms of a compliance agreement allows the commissioner to apply to the federal court for certain remedies, including an order requiring compliance, or a hearing.

• There are now several new exceptions from PIPEDA's consent requirement, including:

– Information that was produced by an individual in the course of his/her employment, business or profession may be collected, used and disclosed without consent provided the collection, use or disclosure is consistent with the purposes for which the information was produced (a so-called "work product" exemption).

– Organizations may disclose personal information to other organizations without consent where disclosure is reasonable for the purposes of investigating a breach of an agreement or contravention of the laws of Canada or a province, or for the purposes of detecting,

Wendy Mee

Wendy Mee *is a partner in the Blakes Toronto office. She practices primarily in the area of privacy law, where she advises a wide range of clients, including those in the financial services, life sciences, education, retail, food and consumer goods sectors, on a variety of privacy and data protection issues. She may be reached at wendy.mee@blakes.com.*

Dara Lambie

Dara Lambie *is an associate in the Blakes Toronto office. Dara's practice focuses on all aspects of Canadian privacy law in addition to marketing and advertising and product regulatory law in the health, drug, food and consumer product areas. She can be reached at dara.lambie@blakes.com.*

VIEWPOINT CONT.

Canada's Digital Privacy Act Receives Royal Assent

suppressing or preventing fraud, provided that in either case it is reasonable to expect that disclosure with consent would compromise the investigation or ability to detect, suppress or prevent the fraud, as applicable.

– Information contained in a witness statement may be collected, used and disclosed without consent, provided the collection, use or disclosure is necessary to assess, process or settle an insurance claim.

Not Yet in Force

Once Bill S-4 provisions relating to mandatory breach notification are in force, they will require organizations to notify affected individuals and the commissioner of a breach of security safeguards involving personal information under the organization's control, where the breach poses a "real risk of significant harm" to the affected individuals. Government institutions and other organizations also will need to be notified in prescribed circumstances, including if the organization believes that the institution or other organization may be able to reduce or mitigate the risk of harm to the affected individuals. This standard for reportable breaches is similar to that under Alberta's Personal Information Protection Act. However, organizations also will have to keep a record of all data breaches, including those that do not meet this harm threshold, and report all breaches to the commissioner upon request. An organization that knowingly fails to report or record a breach as required by PIPEDA will be guilty of an offense punishable by fines of up to CA$100,000.

Washington WATCH

Agency & Regulator News

Consumer Financial Protection Bureau

Lessons Learned from First Administrative Appeal in PHH Corp Case

On June 4, 2015, the CFPB issued its final decision in its enforcement action against PHH Corp. While the case involved the alleged payment of kickbacks in exchange for real estate referrals in violation of the Real Estate Settlement Procedures Act (RESPA), the decision was notable for several reasons that are informative for prepaid and other payments-related businesses:

- The case is the first ruling by Director Richard Cordray in a contested administrative proceeding before the CFPB.
- The case was initially heard by an administrative law judge (ALJ), then appealed to Director Cordray on separate grounds by both the CFPB and by PHH.
- Under the Dodd-Frank Act, the CFPB has the ability to choose whether to bring claims in federal district court or before an administrative law judge and generally can receive the same remedies regardless of the forum it chooses.
- In the PHH case, instead of filing suit in federal court, as has been the common practice for most of its contested enforcement actions, the CFPB filed an administrative claim before the ALJ.
- In doing so, the CFPB used is prosecutorial discretion to avoid the three-year statute of limitations that otherwise would apply to the RESPA claim if the claim were brought in federal court. This is concerning because it demonstrates the CFPB's power to change the venue for enforcement actions to avoid otherwise applicable statutes of limitation.
- Director Cordray determined he had de novo review authority both with respect to the findings of fact and the conclusions of law. As a result, he was able to give little (or no) deference to the decision reached by the ALJ.
- In the PHH case, the ALJ initially ordered PHH to pay *$6.4 million* in disgorgement, and, on appeal, Director Cordray increased the award to more than *$109 million*.

This case serves as instructive precedence for future contested enforcement actions brought before Director Cordray. It is concerning that he was able to avoid the statute of limitations by selecting the venue for the proceeding and utilizing a de novo review standard in the appeal. It also is concerning that the CFPB effectively can serve as both the prosecutor and the judge in a case where Director Cordray hears the appeal of an ALJ, which some may see as effectively stacking the deck against the corporate defendant.

Report Highlights Need to Monitor Consumer Complaints

By Paybefore Staff

If you're not monitoring what consumers are saying about you, particularly their grievances, you're putting your financial services business at risk, so suggests the CFPB's latest supervision report, outlining illegal practices found by the bureau's examiners during Q1 2015.

While focusing heavily on mortgage, debt collection and credit reporting practices that bureau examiners have found inadequate, the report is clear that "the CFPB expects all entities under its supervision to respond to customer complaints and identify major issues and trends that may pose broader risks to their customers."

The statement highlights the importance of prepaid providers paying close attention to complaints included in the CFPB's consumer complaint database and documenting how it monitors, responds and resolves complaints it receives through direct channels. Particular attention should be paid to trends that suggest patterns of consumer dissatisfaction.

Seeking Comments on Enhanced Consumer Complaint Database

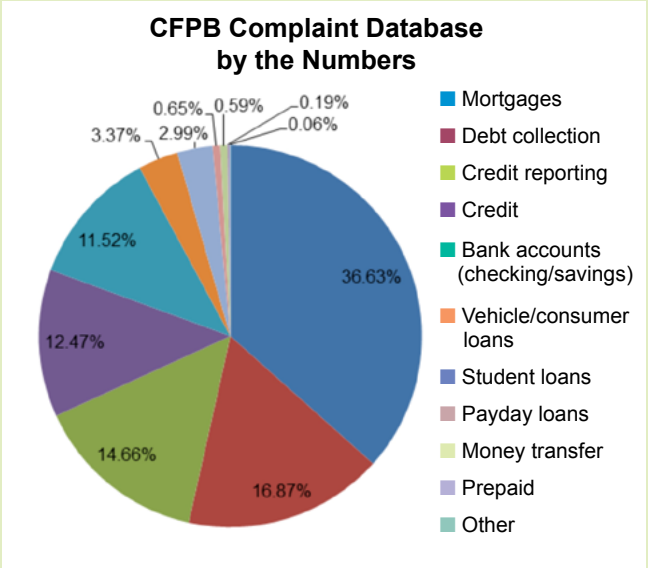
By Paybefore Staff

The CFPB is seeking input on the enhanced public-facing version of its consumer complaint database, which was launched on June 25. The database aggregates consumer complaints about financial services, such as mortgages, credit cards and debt collection. Through its request for information, the bureau hopes to determine if there are ways to help the public more easily understand the information presented in the database and how consumers can compare the information it includes. The RFI, including ways to submit information, can be found here.

Prepaid-Related Complaints: Less than a Quarter of 1 Percent of Total

By Paybefore Staff

Consumers may be complaining about financial services in general, but those complaining to the CFPB about prepaid accounts make up about 0.19 percent of the 411,434 complaints in the agency's Consumer Complaint Database. On June 25, the CFPB went live with an enhanced complaint database, which, for the first time, included consumer narratives explaining their problems with financial products and services. At that time, approximately 7,700 consumers had opted in to make public their narratives, which are scrubbed of personal information. Only 796 (0.19 percent) complaints in the



database were prepaid-related, and only 55 consumers opted to disclose their stories related to problems with prepaid products and services.

By comparison, complaints pertaining to mortgages and debt collection were the most common, with 150,708 (36.63 percent) and 69,429 (16.87 percent) complaints, respectively. Bank accounts or services—checking and savings—had 47,413 complaints. The only product with fewer complaints than prepaid was "other" at 234.

Proposes Consent Orders against Credit Card Add-On Product Vendors

The CFPB has proposed consent orders against two credit card add-on product vendors, Affinion Group Holdings Inc. and Intersections Inc. According to the proposed consent orders, the two companies unfairly charged consumers for add-on products the consumers never received, including identity theft protection and credit monitoring services. Moreover, the Affinion consent order alleges that the company misled consumers during customer service calls with inaccurate or incomplete statements and scripts about the benefits of their add-on products. For example, to avoid cancellations, Affinion retention specialists would tell consumers that Affinion could remove inaccurate information from a consumer's credit report, thereby raising their credit scores, when, in

fact, Affinion had no access to the information included in consumers' credit reports.

Under the proposed consent orders, Affinion will pay $6.8 million of monetary relief to eligible consumers and a civil money penalty of $1.9 million. In addition, Intersections will pay approximately $55,000 in monetary relief to eligible consumers and pay a civil money penalty of $1.2 million.

The proposed consent orders evidence the CFPB's focus on being completely accurate in all dealings with consumers. Providers should review any scripts and statements made to consumers not only in their marketing but by their customer service representatives as well. Providers also should review any product add-ons they offer to ensure consumers both understand when they have opted to include these add-on services, and that such add-on services actually are received by the consumers.

Dept. of Education

NBPCA Calls for Withdrawal of DOE Campus Card Rule

By Paybefore Staff

The NBPCA took a hard line with the Department of Education in response to the agency's proposed rulemaking on campus cards, urging the DOE to withdraw its proposal and seek guidance from prudential financial services regulators. As previously reported, the proposed regulations would put in place major restrictions on fees providers may charge for ATM usage, account maintenance and overdraft fees on cards used to disburse federal student aid funds.

"The Department of Education's proposed rule on the disbursement of Title IV funds clearly oversteps the department's authority by attempting to regulate financial services, which should instead be left to prudential financial regulators," said Brad Fauss, president and CEO of NBPCA. "Further, the department lacks the experience and expertise to effectively regulate the financial products that receive Title IV fund disbursements as evidenced by the fact that the proposed rule will ultimately increase costs and limit choices for schools and students alike as well as move the entire process back to a paper check-based system," he continued. "To mitigate the damage caused by this cumbersome proposal, we urge the department to withdraw the proposed rule."

The comment period ended on July 2. The final rule is slated for adoption by Nov. 1 and would go into effect July 1, 2016.

Several members of Congress have sent letters to the DOE Secretary Arne Duncan expressing concerns about the rule. In a letter signed by seven Democrats, the members praised the rule's consumer protection efforts but raised concerns over unintended consequences and urged the DOE to ensure that third-party servicers could continue to operate in the market. Senior Democratic Whip Alcee Hastings (Fla.) also wrote to Secretary Duncan outlining several concerns with the proposal, including the possibility of increasing fraud risk by prohibiting third-party servicers from accessing student identification data. "The NPRM raises a number of serious questions that throw into doubt the ability of these third parties to continue to offer services for the benefit of students and the institutions which they attend," Hastings wrote. "If the NPRM remains as is, institutions will face serious administrative challenges in disbursing student loans and students will likely be forced to go back to standing in lines on campus to receive their funds via paper checks." Congressman David Trott (R-Mich.) raised similar concerns in his letter to Secretary Duncan, saying the rule could eliminate affordable services for students.

The NBPCA says it will continue its outreach to D.C. lawmakers about the harmful consequences of the proposal and encourages industry members to contact their representatives on Capitol Hill as well.

Federal Trade Commission

Bitcoin Use Warning

In a blog entry posted on June 22, the FTC warned consumers who shop with bitcoin and other cryptocurrencies. The post notes the increasing prevalence of merchants accepting virtual currencies, like bitcoin, for payment but warns consumers that they come with several risks, including sharply fluctuating value and not having the same legal protections as traditional methods of payment. The FTC notes it has received hundreds of complaints involving virtual currencies and advises consumers to research where their virtual currency is going, whether directly to a merchant or through a processor, and what the refund policy of the merchant is prior to making a payment or purchase. Finally, the FTC notes that virtual currency transactions raise privacy concerns as transactions are publicly posted on a ledger and consumers are therefore advised to review the merchant's privacy policy.

While the blog post is directed at consumers, it serves as guidance to merchants and processors accepting virtual currencies as well. It would appear from the FTC's post that merchants and processors accepting virtual currencies should make consumers aware of all of the terms and conditions related to their use of this payment method as well as the

merchant's return and refund policies. Similarly, merchants and processors accepting virtual currencies should make sure their privacy policies are updated to sufficiently address any concerns that may arise from accepting this form of payment may raise. Finally, the fact the FTC has received hundreds of consumer complaints related to virtual currencies possibly suggests enforcement actions may not be far behind.

Federal Reserve Board

Signature Authentication Isn't Enough

In a speech at the Federal Reserve Bank of Kansas City's conference, Federal Reserve Governor Jerome Powell expressed concern that banks continue to issue chip and signature cards to consumers, rather than the "more secure" chip-and-PIN cards, ahead of the October 2015 liability shift deadline. Gov. Powell noted that the use of signatures as a means of authentication should be reviewed in light of other technologies at banks' disposal. He advised banks to layer security tools and procedures and to increase the use of tokenization and encryption to prevent data breaches.

Office of the Comptroller of the Currency

Compliance Risks Remain High: BSA/AML, Cybersecurity and Third Parties Top List

By Paybefore Staff

In its spring 2015 Semiannual Risk Perspective, the OCC's National Risk Committee (NRC), which monitors the condition of the federal banking system and emerging threats to the system's safety and soundness, characterizes the large banks it supervises as, overall, being in "in sound financial condition," with the financial condition of its community and midsized banks improving but with variable earnings outlooks—based on data as of year-end 2014. Despite the relatively good news on banks' financial rebound from the financial crisis of 2008, the report details a laundry list of risks banks face looking forward. Regardless of the size of the bank, compliance risk involving payments is a top concern, especially relating to BSA/AML compliance, cybersecurity and the use of third parties.

Based on this report, if you're expecting an OCC exam in the next year, you can be assured these are areas your examiners will focus on:

BSA/AML Risk. The NRC contends that technological developments that benefit customers through enhanced products and greater access to financial services are vulnerable to criminals who continue to exploit such innovations. Its concern is that BSA programs at some banks have failed to develop or incorporate appropriate controls as products and services have evolved, and some banks have devoted insufficient resources and expertise have been devoted to BSA/AML issues. It suggests that as BSA/AML risks continue to increase, banks must properly manage risks associated with customers with higher BSA/AML risk and their transactions by assessing customers on a case-by-case basis and instituting commensurate controls.

The NRC advises that bank BSA/AML programs and controls should continually evolve to address changing customer profiles, advanced money laundering schemes, the rapid pace of technological change, and the overall risk that money laundering and terrorist financing activities create. OCC supervisory staff, it says, will assess bank management's efforts to maintain an effective, well-staffed program.

Further addressing risks associated with new services (although not strictly relating to BSA/AML issues), the NRC comments: "OCC supervisory staff will coordinate with the CFPB to determine compliance with consumer laws, regulations and guidance … and will focus on the adequacy of enterprise-wide compliance risk management." It adds, "OCC staff will also assess banks' effectiveness in identifying and responding to applicable risks posed by new products and services or terms."

Trends in OCC BSA-Related Enforcement Actions

Fiscal year	2010	2011	2012	2013	2014	2015	Total
Formal enforcement actions	14	10	15	16	16	6	77
Civil money penalties	2	2	0	4	3	1	12
Dollar amount ($millions)	$5.2	$15.0	$0.0	$551.6	$351	$0.5	$923.3

Source: FinCEN Consolidated Quarterly Reports
Note: Data for 2015 include enforcement actions issued through February 27. All other data as of year-end.

Third-Party Risk. As part of the NRC's concern with operational risk, it says that OCC supervisory staff will focus on third-party risk management. While calling out consumer credit-related products specifically, it's not a stretch to recognize that the NRC's concerns apply across the board: "The NRC finds that the use of third parties to conduct all or a portion of consumer credit-related product development, implementation and fulfillment can substantially increase the risk of unfair or deceptive practices. In recent years, a number of banks that failed to exercise adequate risk management and controls when developing and offering various add-on products to customers have been the subject of OCC enforcement actions."

Examiners' focus, the report suggests, will include assessing each bank management's plans to respond to increasing operational risk through the introduction of new or revised business products, processes, delivery channels or third-party providers.

Cyberthreats. The NRC notes: "OCC supervisory staff will review banks' programs for assessing and mitigating the evolving threat environment and cyber resilience. These reviews will include assessments of data and network protection practices, business continuity practices, risks from vendors."

Offices of Inspector General

Process for Notifying Prudential Regulators

By Paybefore Staff

The OIG for the federal prudential regulators have recommended that the CFPB enhance and revise its existing policy regarding incoming and outgoing civil referrals to ensure compliance with the Dodd-Frank provision that requires the bureau to coordinate its supervisory activities and avoid duplicating regulatory oversight responsibilities. In a letter response, CFPB Deputy Director and Associate Director Steven L. Antonakes agreed with the recommendations. He wrote: "In particular, CFPB will require the tracking of written notifications and recommendations to the prudential regulators and the corresponding written responses received from the prudential regulators."

The OIG noted that the CFPB and the prudential regulators generally were coordinating their regulatory oversight activities consistent with Dodd-Frank requirements.

The recommendations were a result of a report issued in June by the OIG for the FDIC, Fed, OCC and NCUA.

Dept. of Treasury

Reports Find Gov't AML, CTF Efforts Have Been Effective

By Paybefore Staff

Government efforts to combat money laundering and terrorist financing have succeeded in making life difficult for criminals seeking to engage in those activities, according to a pair of reports from the Treasury Department. The National Money Laundering Risk Assessment (NMLRA) and National Terrorist Financing Risk Assessment (NTFRA) were based on guidance set forth in 2013 by the Financial Action Task Force, the international standard-setting body for AML and CTF standards, of which the U.S. is the founding member. The NTFRA is the first of its kind, while the NMLRA follows a previous report Treasury issued in 2005.

The NMLRA concluded that the U.S. government has kept pace with innovation in money laundering techniques, forcing criminals attempting to launder money to rely on costly and burdensome methods to mask their identities when opening and managing accounts. Those methods include using cash, conducting smaller transactions below customer identification thresholds and using shell companies. Meanwhile, AML efforts have succeeded in narrowing the vulnerabilities that money launderers seek to exploit using tools, such as targeted financial sanctions, law enforcement investigations and prosecutions, as well as working to enhance international AML standards.

The U.S. government also has made terrorism financing more difficult, according to the NTFRA. Efforts in that area have "made it substantially more difficult" for terrorist groups to raise and move money through the U.S. financial system since the attacks of Sept. 11, 2001. Since those efforts began, terrorists haven't been as able to use the banking system to finance illegal activities, instead relying on more expensive and less efficient methods, such as cash smuggling. The risk assessment cautioned, however, that officials must remain vigilant, as the wealth and resources of the U.S. will "continue to make it an attractive target for a wide range of terrorist organizations seeking to fund their activities."

"Today's assessments underscore our dedication to better understand and address the risk of illicit finance," said Acting Under Secretary for Terrorism and Financial Intelligence Adam Szubin. "This comprehensive review will better inform the U.S. government and our private sector partners about how to further safeguard and strengthen the U.S. economy and national security."

The review for the assessments was led by the Treasury Department's Office of Terrorist Financing and Financial Crimes and developed in coordination with offices and bureaus in the Treasury Department, the Department of Justice, the Department of Homeland Security, the Department of State and across the intelligence community and federal regulators.

WASHINGTON WATCH

Federal Bills Paybefore Is Following

There has been no movement in the federal bills Paybefore is following since the last issue of *Pay Gov*, published on June 24. To review the six House and four Senate bills we're tracking, please see Pay Gov—Issue XI, pages 4 and 5.

Follow Paybefore on Twitter

State TRACKER

N.Y. DOL Extends Comment Period for Payroll Card Regs

By Paybefore Staff

Payroll card providers now have until July 31, 2015, to respond to the New York Department of Labor's proposed payroll card regulations, which prohibit fees for inactivity, overdraft, declined transactions or receiving written transaction statements and require a seven-day waiting period before seeking an employee's consent to pay wages by a payroll card, among other mandates. The original deadline was July 10. Submit comments to Michael Paglialonga, NYS Department of Labor, Building 12, State Office Campus, Room 509, Albany, N.Y. 12240, email: regulations@labor.ny.gov.

What's Trending in State Laws and Regulations

Activity continues to slow as more state houses go into recess. To that point, there are no "passed" bills to report and a number of bills have died, most notably in New York, because the legislative term ended without the bills having been signed into law. Movement in EBT (New Hampshire, Rhode Island and Washington) and payroll-related bills (Rhode Island and Washington) top the chart in this issue. And the North Carolina bill relating to money transmitter rules (and touching on virtual currency) continues to be active.

For Paybefore's take on each bill (what happened, what you should know, relevance to the industry) and links to the bill text, please view our State Tracker section online.

Movement in Pending Bills/ Regulations

New Hampshire: EBT **NH H 219**—Restricts Use of EBT Cards
EBT **NH S 169**—Restricts Use of EBT Cards

North Carolina: **NC H 289**—Enacts New North Carolina Money Transmitter Act, Proposes Regulatory Coverage for Virtual Currency, and Repeals Existing Money Transmitter Act

Rhode Island: EBT **RI S 312** and **RI H 5018**—Restrict Use of EBT Cards
RI S 351 and **RI H 5590**—Provide for Payroll Cards

Washington: **WA H 1211**—Requires Second Option for Wage Payment in Addition to Payroll Card Option
EBT **WA H 1820**—Use of EBT on College Campuses
EBT **WA S 1908**—Requiring Photo ID on EBT Cards

State Bills Graveyard

The following bill recently died and is no longer up for consideration.

Maine: EBT **ME S 505, ME H 420**—Would Have Restricted EBT Card Use

New York: **NY A 5968**—Provides for Payroll Cards Subject to Significant Conditions
NY S 2590—Would have Provided for Payroll Cards Subject to Conditions
NY S 5281—Would have Provided for Payroll Cards Subject to Conditions

See State Legislative Session Chart to see which states currently are in or out of session.

Litigation NEWS

Banks Continue to Pursue Home Depot and Target in Data Breach Cases

Litigation between several banks and Home Depot and Target relating to separate data breaches occurring at the two retailers continues. Target is currently in the midst of negotiating a settlement with banks over a 2013 data breach in which the banks lost millions of dollars reimbursing customers for fraudulent transactions and reissuing cards. Several banks disputing the settlement currently are seeking class certification from a Minnesota federal judge. The class certification filing comes after a judge ordered Target to disclose the existence of any prior data breaches and, if any existed, how Target responded.

In the Home Depot case, where the banks involved have formed a consolidated class action, Home Depot is seeking to have the banks' claims thrown out. Specifically, Home Depot argues that the banks have failed to show that the expenses they incurred in bolstering their security after the Home Depot breach—including the costs of replacing cards, offering free credit monitoring and investigating potential fraud—were not traceable to the Home Depot data breach. Home Depot further argues that the banks in question have not gone through the payment network mechanisms for recovering expenses stemming from a data breach and any claim by the banks against Home Depot is not ripe until such mechanisms are followed.

Other TOPICS OF INTEREST

AAF Opinion: Durbin Amendment Reduces Low Income Americans' Access to Checking; Proposed CFPB Rules Threaten Access to Prepaid Alternative

Research into the impact of the Durbin Amendment to the Dodd-Frank Act suggests the amendment is inhibiting the ability of low-income Americans to obtain access to traditional banking services, according to the American Action Forum. The "center-right" group also concludes that prepaid cards were "doing just fine" without the CFPB's proposed rules and when those rule become effective, low-income Americans will have even fewer options to manage their finances.

According to the forum, the Durbin Amendment, which caps interchange fees on debit transactions, for cards issued by financial institutions with more than $10 billion in assets, has forced a significant number of banks that previously relied on higher debit interchange to cover debit card operations to cut services and end free checking. It supports its position citing a Bankrate.com study, which reported that in 2009 (pre-Durbin), 76 percent of all "bank accounts" were free to consumers; yet, in 2013 (post-Durbin), only 38 percent of "bank accounts" were free.

The forum contends the reduction in the availability of free checking negatively affects low-income Americans disproportionately, causing them to abandon checking accounts and "forcing" them into alternative financial services, including nonbank money orders, nonbank check cashing and nonbank remittances. Recognizing prepaid cards as an alternative for those disintermediated from the financial system, the forum cautions the CFPB's new regulations may have a "significant impact on the availability of prepaid cards [and their benefits]."

The forum article concludes, citing language from the American Bankers Association's comment letter on the CFPB's NPRM on prepaid cards that suggests the costs and risks of proposed rules "will significantly hinder banks' ability to offer prepaid cards [resulting in] the suppression of a promising option to move people without bank accounts into financial products offered by insured depository institutions."

The American Action Forum describes itself as an independent "center-right," nonprofit 501(c)(3) organization that is not affiliated with or controlled by any political group. It says its focus is to educate the public about the complex policy choices now facing the country and explain why solutions grounded in the center-right values represent the best way forward for America's future. It is headed by Douglas Holtz-Eakin, former director of the Congressional Budget Office.

OTHER TOPICS OF INTEREST CONT.

Paybefore Stories You May Have Missed

Click on the title to read the story.

- Pew: GPR Usage Grows 50 Percent over Last Three Years
- Visa Research Shows Payroll Cards Score Big with Employees
- Q&A with Brad Fauss, NBPCA
- Boston Fed: GPR Research in Line with Industry Expectations
- Supreme Court Upholds Affordable Care Act Tax Credits
- Europol Busts Cybercrime Ring, Enlists Barclays to Fight Attacks
- Chase Adds Bill Pay to Liquid, Expands Checking Access

TOP STORY CONT. FROM PAGE 1

CFPB Issues 9 Principles for Faster Payments

the Electronic Fund Transfer Act. "However, many payments firms are not subject to CFPB supervision, and the CFPB's payments principles go beyond the requirements established by Congress in the EFTA and elsewhere. Based on the CFPB's history, we would not be surprised to see attempts to legislate through enforcement actions in this area." The authors also question whether banks will invest in faster payments when their debit interchange revenue has been cut.

In its report, "Strategies for Improving the U.S. Payment System," the Fed estimates the cumulative implementation costs of a faster payments system could be anywhere from $3.8 billion to $7.2 billion. However, the net business case could be between negative $0.9 billion and positive $1.8 billion, according to the Fed research.

Meanwhile, TCH welcomed the principles, saying: "The banking industry is making great strides in developing a secure, real-time payment system to better meet consumers' and businesses' needs." Steve Ledford, senior vice president for product and strategy, TCH, tells Paybefore that many banks view real-time payments as a strategic investment. That said, ROI is still important, he notes. "We believe that if you design a payment system with the idea of getting a ROI, you will come up with features that are more valuable to end users."

PAY gov

Lindsay Tis
Managing Director
ltis@iirusa.com

Loraine DeBonis
Editor-in-Chief
ldebonis@paybefore.com

Matthew J. Middleton
Business Development
mmiddleton@iirusa.com

Bill Grabarek
Senior Editor
bgrabarek@paybefore.com

Kate Fitzgerald
Emerging Payments Editor
kfitzgerald@paybefore.com

Adam Perrotta
Assistant Editor
aperrotta@paybefore.com

Robin Chalmers Mason
Production Editor
rmason@paybefore.com

Doris Kwok
Marketing Assistant

Joanne S. Butler
Graphic Designer

Contributing Editors

Eli A. Rosenberg
Associate, Baird Holm LLP

Grayson J. Derrick
Partner, Baird Holm LLP

Marilyn Bochicchio
Government Editor

Pay Gov is published 20 times a year for Paybefore subscribers. *Pay Gov* is available only through subscription to registered users of Paybefore.com. For renewals, address changes or reprints, contact info@paybefore.com.

To subscribe or to advertise, contact Matthew Middleton at mmiddleton@iirusa.com or +1 646.616.7604.

Learn more about Paybefore sponsors: www.paybeforebuyersguide.com

PAYBEFORE MEDIA PROPERTIES

Pay Magazine | Pay Connect | Pay News | Pay Gov | Pay Op-Ed | Pay Week | Paybefore.com