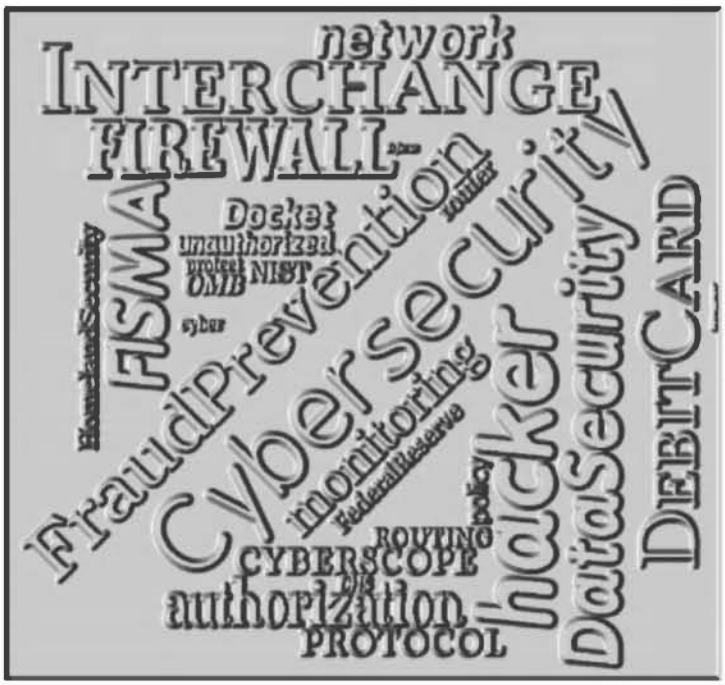
DATA SECURITY CONTINUITY:
THE NEED FOR THE DEBIT INTERCHANGE RULE TO COMPLY WITH FEDERAL CYBERSECURITY OBJECTIVES



Comments on:
Debit Card Interchange Fees and Routing
Interim Final Rule
Regulation II; Docket No. R-1404 RIN No. 7100-AD 63

September 2011

The Center for Regulatory Effectiveness
1601 Connecticut Avenue, NW
Washington, DC 20009
202.265.2383
www.TheCRE.com

DATA SECURITY CONTINUITY: THE NEED FOR THE DEBIT INTERCHANGE RULE TO COMPLY WITH FEDERAL CYBERSECURITY OBJECTIVES

Issue

The one cent/transaction data security and fraud prevention cost reimbursement factor contained in the Federal Reserve's Interim Final Rule does not allow debit card issuers to adequately recover cybersecurity costs as intended by Dodd-Frank.

Consistent with Dodd-Frank, the Federal Reserve should revise their proposal to add-in the additional data security costs estimated by merchant acquirers/processors and debit card networks. The increased cost recovery factor is needed to support cybersecurity across the chain of parties participating in transaction process.

Raising the Federal Reserve's limitation on the resources available for debit card data security is also necessary to achieve consistency with the national cybersecurity objectives set forth by the Department of Commerce's Internet Policy Task Force and the White House.

Maintaining Cybersecurity Requires End-to-End Transaction Security Continuity

In April 2010, the Secretary of Commerce created the Internet Policy Task Force (IPTF) which brought "together the technical, policy, trade, and legal expertise of the entire Department."[1] The IPTF was formed in response to the explosive growth in cyber attacks on the nation's public and private IT infrastructure. As the IPTF's report, known as the "Green Paper" explains,

> *Cyber attacks on Internet commerce, vital business sectors and government agencies have grown exponentially. Some estimates suggest that, in the first quarter of this year, security experts were seeing almost 67,000 new malware threats on the Internet every day. This means more than 45 new viruses, worms, spyware and other threats were being created every minute – more than double the number from January 2009. As these threats grow, security policy, technology and procedures need to evolve even faster to stay ahead of the threats.*[2]

The Green Paper highlights a critical shortcoming in the Board's one cent/transaction fraud prevention and data security adjustment factor; it does not take into account the interconnectedness

---

[1] Department of Commerce, Internet Policy Task Force, "Cybersecurity, Innovation and the Internet Economy," Final, June 2011, p. ii.

[2] *Id.*

of the internet and need to maintain cybersecurity continuity across the IT environment. In explaining the need for end-to-end IT security, the Task Force's paper states,

> *Computing devices are highly and increasingly interconnected, which means security deficiencies in a limited number of systems can be exploited to launch cyber intrusions or attacks on other systems. Stated another way, poor cyber "hygiene" on one Internet-connected computer negatively impacts other connected computers.*[3]

The Dodd-Frank amendments to the Electronic Fund Transfer Act (EFTA):

1. Recognized the need for the financial services industry to maintain end-to-end cybersecurity for debit card transactions; and

2. Directed the Federal Reserve to consider the IT security and fraud prevention costs incurred by all parties involved in a debit card transaction in setting the security adjustment factor.

Specifically, the law requires the Federal Reserve, when "issuing the standards and prescribing regulations" for the data security/fraud prevention adjustment factor to consider:

> *the fraud prevention and data security costs expended by each party involved in electronic debit transactions (including consumers, persons who accept debit cards as a form of payment, financial institutions, retailers and payment card networks);*[4]

Congress directed the Board to consider the end-to-end data security costs in debit card transactions so that it could include all relevant security costs in setting the data security/fraud prevention adjustment factor. There was no reason for Congress to include the "FACTORS FOR CONSIDERATION" section of the legislation unless it was to prevent the agency from overlooking or improperly dismissing data security and fraud prevention costs that are needed to protect transaction security across the entire process.

Dodd-Frank also required that the Board only allow the adjustment factor if "such adjustment is reasonably necessary to make allowance for costs incurred by the issuer in preventing fraud in relation to electronic debit transactions involving that issuer…."

In understanding the phrase "costs incurred by the issuer in preventing fraud" the Board needs to recognize that **cybersecurity breaches of other parties to the debit card transaction become fraud prevention costs incurred by issuers** as the following two examples illustrate.

---

[3] Id., p. 7.

[4] 15 USC § 1693o-2

Example 1: Security Breach of Major Internet Merchant

In April of this year, the Sony PlayStation Network was hacked, potentially resulting in the criminals obtaining payment card data for tens of millions of customers. As a result of a third-party's data security breach, card issuers incurred the very substantial fraud prevention/data security costs associated with replacing the compromised payment cards. The Chief Executive Officer of the National Credit Union Association explained that Sony's customers

> *were correctly advised by the media to contact their bank or credit union and ask that their debit and credit cards be reissued. As I write, I know firsthand that credit unions are working with their members affected by this breach, and reissuing cards to them at no cost. Again, that's the right way to do business, and we have a legal and ethical responsibility to absorb the cost.*
>
> *But, contrary to what some might think, the expense for taking this action is not and will not be reimbursed by Sony. Rather, credit unions and banks rely on interchange revenue to cover the cost of debit program administration, including in these circumstances, reacting to a merchant data breach.*
>
> *When all is said and done, credit unions and banks will have spent millions on what appears to be a major security failure caused by Sony's inability to protect its consumer data.*[5] [Emphasis added]

As a result of the hack, card issuers had to go through the process of issuing new cards, which included the costs of addressing customer questions and concerns about the security breach, to prevent fraud from being committed with the stolen data. Thus, **card issuers paid fraud prevention costs that were caused by a third-party's cybsersecurity breach** – an illustration of the need for end-to-end data security as explained by the Department of Commerce and required by Dodd-Frank.

Example 2: Security Breach of Major Payment Card Processor

USA Today reported in January 2009 on a data security breach at card processor that "could set a record." The cyber attack on the processor was not discovered until two major payment card networks notified the firm "of suspicious transactions stemming from accounts linked to its systems."[6]

---

[5] Equity News, "Bill Cheney: Sony Data Breach: Another Case for Interchange Delay," *available at* http://www.equitynews.info/2011/05/03/bill-cheney-sony-data-breach-another-case-for-interchange-delay/

[6] Byron Acohido, USA TODAY, "Hackers breach Heartland Payment credit card system," January 21, 2009, *available at* http://abcnews.go.com/Business/PersonalFinance/story?id=6695611&page=1

> The story noted that "Forcht Bank in Kentucky last week began issuing replacement debit cards to 8,500 patrons, due to reports of fraudulent card activity. 'There are several other banks affected, and this is not isolated to Forcht Bank customers,' the bank said in a Jan. 12 statement to customers." Thus, the security breach at the processor resulted in costs to card issuers in order to prevent fraud.

Since card issuers bear the costs of preventing fraud following data security lapses by third-parties, the fraud protection and data security adjustment factor should reflect these additional costs, as authorized by Dodd-Frank which directed the Board to consider the security costs across the entire transaction chain. The fraud prevention/data security cost to card issuers may be estimated by combining the fraud prevention/data security cost of all parties with debit card transaction responsibilities after the payment is accepted by the merchant.

The Federal Reserve conducted three surveys related to debit card interchange in preparation for the rulemaking, one each for debit card issuers, debit card processors and debit card networks.[7] Each of the surveys asked similar questions about the recipients' fraud prevention and data security costs. Thus, the Board has the data to allow it to estimate the end-to-end data security and fraud prevention costs for debit card transactions. It is this combined, end-to-end cost which should be reflected in the adjustment factor.

Protecting Small Debit Card Issuers Requires End-to-End Security Continuity

In addition to demonstrating the need for end-to-end data security to prevent fraud, the successful hack attacks on Sony and Heartland also illustrated another point directly relevant to the Federal Reserve's rulemaking on the allowable data security/fraud prevention adjustment factor – the need to protect small banks and credit unions.

It wasn't simply large card issuers that incurred costs as a result of data security lapses, so did small banks, credit unions and other small card issuers. The EFTA amendments contain an exemption for small issuers, those with assets less than $10,000,000,000.

Unless the Federal Reserve sets a data security/fraud prevention adjustment factor which covers **all** the fraud prevention costs card issuers bear as a result of third-party data breaches, card issuers will pay the price, in direct contravention to the intent of Dodd-Frank. Thus, the cost to issuers should be understood to also include the fraud prevention/data security costs to debit card processors and debit card networks.

The need for ensuring that debit card issuers – including small financial institutions – are fully compensated for fraud prevention costs incurred because of third-party data security breaches is also in keeping with the Department of Commerce's Green Paper which discusses payment card industry

---

[7] The survey instruments may be found at http://www.federalreserve.gov/newsevents/files/card_issuer_survey_20100920.pdf, http://www.federalreserve.gov/newsevents/files/payment_card_network_survey_20100920.pdf, and http://www.federalreserve.gov/newsevents/files/merchant_acquirer_survey_20100920.pdf.

security standards. The paper explains that the Payment Card Industry Data Security Standard (PCI DSS) "is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures."[8]

The Task Force discussed some of the challenges associated with implementing PCI DSS, two of which should inform the Board's decision. One of the security challenges cited in the Green Paper was the "[p]erception that the PCI DSS requirements are too expensive to implement...."[9] Setting the data security reimbursement costs too low, by not including all of card issuers' fraud prevention/data security costs, can only diminish support for full implementation of the standards.

The Task Force also noted that, through the Department's notice-and-comment process used in developing the final version of the Green Paper, some commentors "felt that the standard provides excellent advice, but may require more time and resources not available to small businesses and entrepreneurs that may act as a barrier to entry for small and medium sized businesses."[10]

The tentative one cent/transaction adjustment for fraud prevention and data security costs, based on the narrowest interpretation of the term "costs incurred by the issuer" would only exacerbate the problem of insufficient data security resources, particularly for small card issuers who are nominally exempt from the Dodd-Frank debit interchange provisions.

The Green Paper repeatedly calls for cybersecurity policy coordination across the federal government as well as with the private sector. For example, Policy Recommendation A2 states that the "Department of Commerce should work with other government, private sector, and non-government organizations to proactively promote keystone standards and practices."

Similarly, Policy Recommendation C1 also stresses interagency and private sector cooperation and coordination in stating,

> *The Department of Commerce should work across government and with the private sector to build a stronger understanding (at both the firm and at the macro-economic level) of the costs of cyber threats and the benefits of greater security to the [Internet and Information Innovation Sector] I3S.*

To ensure that the Federal Reserve's cybersecurity for debit card issuers are consistent with the cybersecurity policies being developed by the rest of the government, the Board should consult with Commerce's Internet Policy Task Force on the data security cost adjustment factor.

---

[8] Commerce at p. 54.

[9] Id at p. 55.

[10] Id.

The Federal Reserve's Debit Interchange Data Security Policy Should be in Accord with Administration Cybersecurity Objectives

The Green Paper focuses on non-critical infrastructure. By all accounts, the financial system is a component of the nation's critical infrastructure which calls for even higher levels of protection than the economic segments which are the focus of the paper. Critical infrastructure is defined by statute as the "systems and assets...so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on...national economic security...." 42 U.S.C. 5195c(e). Pursuant to Homeland Security Presidential Directive 7 (HSPD-7), both the Department of Homeland Security (DHS) and the Treasury Department have oversight responsibilities for protecting the banking and finance sector's critical infrastructure.[11]

The Obama Administration has proposed cybersecurity legislation designed to protect critical private sector IT infrastructure. The proposal builds on legislation that has been introduced in the House and Senate, including the Lieberman-Carper-Collins Cybersecurity and Internet Freedom Act of 2011 (S. 413) and Rep. Thompson's Homeland Security Cyber and Physical Infrastructure Protection Act of 2011 (H.R. 1740).

The Administration's proposal contains provisions specific to preventing the unauthorized use of payment cards. As the Administration's Section by Section analysis of the legislative proposal explains, the legislation would encourage businesses to participate "in a security program that effectively blocks the use of the [sensitive personally identifiable information] SPII to initiate unauthorized financial transactions before they are charged to the account of the individual...."[12]

<u>If the Federal Reserve caps debit card issuers' ability to recover fraud prevention expenses at a less than full cost level, the Board would impede the ability of financial institutions to meet the President's cybersecurity goals for preventing payment card fraud</u>.

The significance of the Administration's cybersecurity proposal to the instant rulemaking goes beyond any single provision. Even though the President's proposal emphasizes cost effective approaches to cybersecurity, upgrades to the protection of critical cyber infrastructure would take resources. The data security/fraud prevention adjustment factor in the Interim Final Rule would function as a *de facto* cap on the ability of financial institutions to upgrade their debit-card related cyber protections.

---

[11] The DHS/Treasury sector-specific plan for banking and finance that is a component of the National Infrastructure Protection Plan required by HSPD-7 is available at http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf.

[12] The Administration's cybersecurity legislative proposal is available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf. The Section by Section analysis of the proposal is available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill-section-by-section-analysis.pdf.

Since, as the Green Paper noted, the cyber world is "highly and increasingly interconnected," the Board may be inadvertently creating a drag on the ability of the financial services industry to respond to new cybersecurity initiatives and requirements. Thus, in addition to coordinating their data security reimbursement limitation with the Department of Commerce, the Board should also work with the White House and DHS (which would be granted additional authorities and responsibilities for cyber infrastructure protection under the Administration's proposal as well as the pending House and Senate legislation) to ensure that the limitation does not conflict with national cybersecurity objectives.

Conclusions

1. The Federal Reserve is establishing a *de facto* cap on the resources available to debit card issuers for data security and fraud prevention activities.

2. Data security lapses by any of the parties involved in debit card transactions flow through as fraud prevention costs to the debit card issuer.

3. The one cent/transaction data security cost recovery cap in the Interim Final Rule is inadequate to achieve either Dodd-Frank's debit card fraud prevention goals or national cybersecurity objectives.

Recommendations

1. The data security cost reimbursement cap should be increased to include the data security costs incurred by all organizations who participate in processing debit card transactions including merchant acquirers/processors and card networks.

2. The Federal Reserve should consult with the Department of Commerce's Internet Policy Task Force, the White House and the Department of Homeland Security to prevent its data security resource limitation cap from conflicting with national cybersecurity objectives.