Richard Dzina: Luncheon remarks at the Community Bankers Conference

Remarks by Mr Richard Dzina, Executive Vice President of the Financial Services Group of the Federal Reserve Bank of New York, at the Community Bankers Conference, Federal Reserve Bank of New York, New York City, 18 April 2018.

* * *

Good afternoon. I am conscious that I am the concluding speaker for today's conference, a line usually followed by "and the only thing that separates you from the bar." In this case, I'm the only thing that separates you from the gold vault, which may be even more compelling, so I'll keep things brief, but hopefully meaningful.

Allow me to share two preliminary comments as prelude to formal remarks:

First, convening this conference underscores for me and my colleagues that fulfillment of Federal Reserve mandates in monetary policy, supervision, and financial services does not constitute an end to itself, but a means to an end. The end is to foster conditions and to provide services that support robust and sustainable economic activity on which our nation depends and in which community banks play an integral, indeed indispensable, role.

May those of us who have the privilege of serving this great institution, and working within these walls, never forget the ultimate object of our mandate, at which you sit at the center.

Second, my perspective in addressing you today is not as overseer, or as policy maker, but as head of Financial Services at the Federal Reserve Bank of New York. In other words, perhaps uniquely in the constellation of the Federal Reserve System, my colleagues and I work for you. My standing before you represents a visceral reminder of our accountability to depository institutions, independent of size, which rely upon our services to send and receive time critical payments; to maintain and permit the transfer of Fedwire eligible securities; and to provide cash services to support the needs of consumers and commercial establishments.

It is with this orientation that I offer these remarks today, which reflect my own views and do not necessarily represent those of the Federal Reserve Bank of New York or the Federal Reserve System.

The theme of today's conference, appropriately, has been "Navigating Future Risks for Community Banks". Allow me to elaborate upon the single risk that dominates from my vantage, regrettably not a "future risk" but an all too present one, and to highlight some of the measures that we are taking in response. The risk to which I refer is not a function of regulatory pressure, or capital demands, or an evolving economy, or compliance challenges, or the proliferation of new technologies, or an unprecedented season of payments innovation, or the challenging competitive landscape. All of these may represent very real risks, and no doubt occupy your consciousness, to borrow the lyrics of a prior generation, "eight days a week".

Rather, building upon the theme of your prior panel discussion, the risk that dominates from my parochial view is the escalating and evolving cyber threat to our financial and payment systems, representing the challenge of our generation. The orientation that I want to pursue, reflecting this audience, is not what we are doing within the Federal Reserve to harden our critical infrastructure. While that is a manic and consuming preoccupation it is not my focus today. Instead, I want to concentrate on endpoint security vulnerabilities to the payments system, in which partnership with the institutions in this room represents an indispensable element of success.

Historically, market infrastructures have operated on the presumption that endpoint security is

principally the responsibility of the endpoint, and infrastructure security is principally the responsibility of the operator. In the United States, the legal framework for wholesale funds transfers codifies that presumption, with each actor assigned responsibility for that part of security most within its control. Yet, in the present environment endpoint security breaches can have serious implications for public confidence in the integrity of the network as a whole, even in circumstances when the operator's infrastructure, applications, and security perimeter have not been compromised. A series of recent high profile events have underscored dramatically this endpoint security risk, a theme that has also captured the attention of global policy makers.

As operator of a payment system in which a Fedwire Funds transfer is immediate, final, and irrevocable, and for which a single transfer can be affected for a penny shy of $10 billion, the Federal Reserve Banks recognize that the stakes for public confidence are incomprehensibly large; as users of said payment system, you realize the stakes for endpoints in terms of reputational risk and financial viability are equally profound. Our fates in this domain are inextricably linked.

Work to mitigate endpoint security risks in support of our collective interest proceeds across multiple fronts, including efforts to enhance end-to-end understanding of the security relationships within a network; initiatives to enhance assurance that external endpoints are operating in adherence with an operator's security requirements; and the development of application tools to enhance a participant's management of fraud risk. I want to elaborate upon three recent actions we have taken to enhance endpoint security, and to provide a preview of additional measures in train. Each of these actions, I will suggest, has particular relevance for community banks:

- Last Fall the Reserve Banks implemented functionality that enhances the tools available to Fedwire participants to manage the messages they send to the Fedwire services. These enhanced control features allow customers accessing Fedwire services through the FedLine Advantage channel to restrict the creation of transfers outside of specified hours, or to banks outside of the United States, or in dollar amounts that exceed designated thresholds, among other parameters. The additional features also trigger out-of-band notification when changes occur to a participant's processing options. For example, a customer might assign a senior manager without operational responsibilities to be notified at an out-of-band email address when designated processing options are changed or thresholds exceeded. We believe that these enhancements have resulted in meaningful risk reduction for individual customers and the payments system at large, and have generated renewed awareness of the critical importance of strong endpoint security controls.

- Also last Fall, the Reserve Banks offered additional protection to depository institutions with assets under a designated size against uncapped losses due to fraudulent payment activity through an expansion of our real time monitoring capabilities. The program, which depository institutions were strongly encouraged to adopt, helps to limit losses from unauthorized Fedwire Funds transfers by rejecting those that would exceed a depository institution's net debit cap. The rejection of a Fedwire Funds transaction provides another opportunity for the institution to verify authorization for, and fund, the transaction, thereby reducing the financial risk to the institution and its account holding Reserve Bank.

- In June 2016 the Reserve Banks amended Operating Circular 5, which governs electronic access of depository institutions to Federal Reserve Financial Services, by adding an information security appendix. Of particular note, the appendix sets out requirements for customer information security programs designed to protect the environment and systems used to access Reserve Bank services and applications. Adherence to the terms set forth in the operating circular represents an indispensable element of a depository institution's endpoint security program, designed to protect both the individual institution and the network at large. Attention to these security responsibilities regrettably is no longer the exclusive

purview of technologists and auditors, but compels awareness and direct engagement of executive management and directors.

Collectively, these measures represent material enhancements in endpoint security controls supporting the payment system. At the same time, given an escalating threat environment that is not static, we cannot stand still. Therefore, looking forward, we are presently considering another wave of application level enhancements to give depository institutions greater control of their payment activity, such as an exploration of tools that will identify anomalous payments relative to historical patterns; contemplating a further expansion of real-time monitoring to include all depository institutions; and considering adoption of an assurance program to enhance confidence that external endpoints are operating in adherence with security requirements. We recognize, especially in the resiliency and security domains, that either intentionally we are progressing or inevitably we are regressing; given the technological sophistication and guile of our adversaries, there is no idleness.

Conclusion

Let's pivot in conclusion from the age of electronic payments to the payment form of antiquity. Many of you will shortly tour the gold vault, the largest such repository in the world, representing approximately one third of the world's known supply. You will immediately discern upon descending to the bedrock of Manhattan, marveling at the massive vault door, appreciating the multi-faceted control environment, that payments security is a timeless preoccupation.

Hardly any of the gold in the vaults of the Federal Reserve Bank of New York is the property of the United States, whose reserves you know from 007 lore reside in Ft. Knox. Instead, it is gold held on behalf of foreign and international monetary authorities. Indulge me, if you will, in a fascinating historical anecdote in the annals of official reserve custody, which I will endeavor, perhaps feebly, to tie to today's theme.

The Spanish Civil War was a brutal conflict that pitted Nationalist rebel forces, allied with Fascist Italy and Nazi Germany, against the Republican government supported by the Soviet Union. In 1938, with their government on the cusp of implosion and before fleeing into exile, the Republicans hastily sent their gold stock to their trusted ally, the Soviet Union, for safekeeping. This episode is recounted in a history of the Spanish Civil War by Hugh Thomas, who writes the following:

> According to Orlov (now I confess to not reading the whole book, so I do not actually know who Orlov is; nevertheless, according to no less an authority than Orlov!), Stalin celebrated the arrival of the [Spanish] gold with a banquet at which he [toasted], "The Spaniards will never see their gold again, just as one cannot see one's own ears."

Sometimes there is illustrative power in a negative example, even from one whose transgressions went exceedingly beyond being an untrustworthy custodian. The antithesis of what this Bank stands for could not be expressed with more force or greater clarity.

The ultimate foundation of this institution, you see, far beyond its technical capacities in monetary policy execution, or its supervision of financial institutions, or its provision of financial services, is trust.

This trust must be earned, every day, across every mandate, especially in an era in which confidence in public institutions has waned. The nature of this trust is fickle: it accrues slowly, and can evaporate instantly. It is a charge we take very seriously, especially when it comes to the resiliency and security of the foundational elements of our nation's payment system.

Thank you for your generous attention today. I'd be pleased to respond to a few questions.