

# MESSAGE FROM THE INTERIM PRESIDENT

## The Federal Reserve and Cybersecurity

What can we do about cybersecurity? That's the central question of this issue's cover story, "Cyberattacks and the Digital Dilemma," which explores the incentives businesses, governments, and consumers have to invest in and monitor the security of their systems, applications, data, and online activities.

It's a question of vital importance. In 2016, the FBI received nearly 300,000 complaints from consumers about cybercrime, at a cost to the victims of more than \$1.3 billion. That only includes people who reported the crime; the security-software company Symantec puts the total financial cost to U.S. consumers at more than \$20 billion. For U.S. businesses, a data breach currently costs about \$7.4 million on average, according to a research study sponsored by IBM. And these numbers pale in comparison to the potential harm if hackers were able to infiltrate systems within our country's critical infrastructure sectors, including the financial services sector.

At the Fed, we are highly aware of cybersecurity risks and the importance of maintaining trust and confidence in the banking system. That's why protecting the integrity of our data, systems, and applications underpins everything we do, from sending an email to transferring trillions of dollars each day between financial institutions. Led by National IT's Office of the Chief Information Security Officer, and based here in the Fifth District, the Federal Reserve Banks execute a comprehensive cybersecurity strategy anchored on three goals: defending Federal Reserve System networks, applications, and data; developing the cybersecurity workforce skills necessary for tackling tomorrow's threats; and deploying threat-driven, risk-based processes. Simply put, our goal is to reduce cybercriminals' financial motivation by making it too costly to attack us.

The Fed's physical and virtual footprints are quite large, comprising 12 regional Reserve Banks, an additional 24 branch offices, and more than 22,000 employees — not to mention the thousands of financial institutions we supervise and provide payment services for. Among other protections, we've deployed layers of sophisticated security technologies at our internal and external network entry and exit points, as well as protections at System endpoints. These are coupled with multiple layers of protection at the application level, including the most up-to-date encryption technologies, for the core data themselves.

Even the best programs and technologies aren't enough if our employees don't play an active and informed role. That's why we're also committed to building our "human firewall" as a core component of our defense strategy. Every Fed employee undergoes extensive annual training to stay up to date on our cybersecurity and data privacy

requirements. We also make sure our employees have the knowledge they need to spot potential scams or "phishing" attempts — emails that try to trick the recipient into revealing personal data.

We're confident that our technologies, our processes, and our people help to form a strong layered defense against hackers and other cybercriminals. As strong as that defense is, however, we are well aware of the dangers of complacency. We're always on the lookout for the next emerging threat and adjusting our defenses accordingly.

This issue of the magazine also addresses a topic of great interest to policymakers recently: the persistence of inflation below the Fed's long-run target of 2 percent. Historically, lower unemployment rates have been correlated with higher inflation; given October's unemployment rate of 4.1 percent, one might conclude the current stance of monetary policy is too accommodative. But it's possible that relatively low inflation is a temporary circumstance. For example, some unusual events have lowered specific prices substantially, which has an effect on the overall price level. Since those unusual events are only transitory, inflation is likely to increase in coming months. Overall, the Federal Open Market Committee expects inflation will rise and then stabilize at around 2 percent over the next few years, and that additional increases in the federal funds rate will be forthcoming.

That said, we don't have a perfect understanding of the current behavior of inflation. Some economists have proposed that the relationship between unemployment and inflation has weakened over time, meaning it takes bigger swings in unemployment to trigger changes in inflation. Demographic changes could also be a headwind for wage growth and inflation.

In addition to the articles on cyberattacks and inflation, I hope you will enjoy discussions of a universal basic income, the subprime auto lending market, and an interview with trade economist Douglas Irwin. Thank you for reading. EF



A handwritten signature in black ink that reads "Mark L. Mullinix". The signature is fluid and cursive, with a small flourish at the end.

MARK L. MULLINIX  
INTERIM PRESIDENT AND CHIEF OPERATING OFFICER  
FEDERAL RESERVE BANK OF RICHMOND