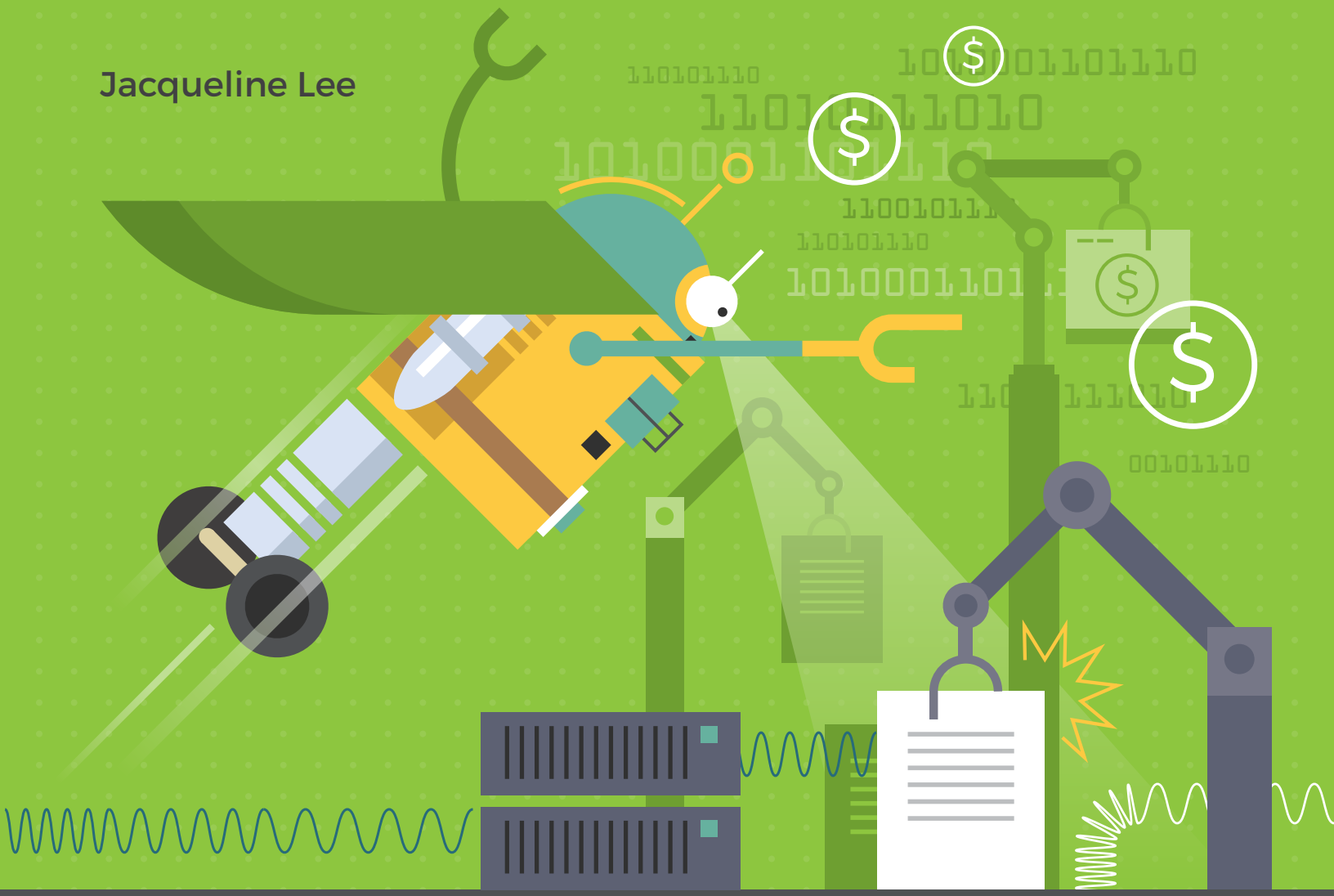
Jacqueline Lee



Preventing SLA Penalties With Managed File Transfer

A Solution that Offers Security and Compliance

ipswitch

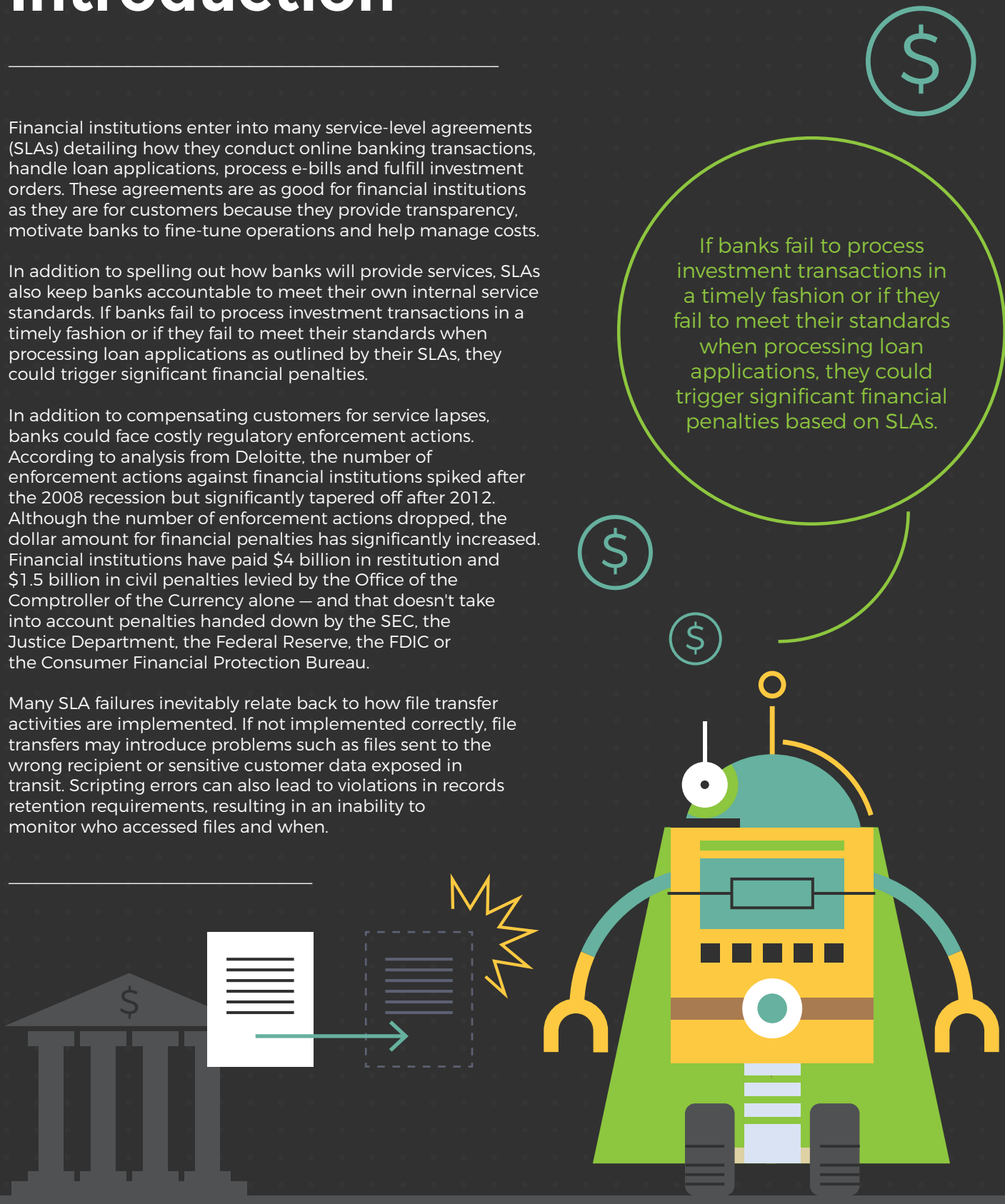
Introduction

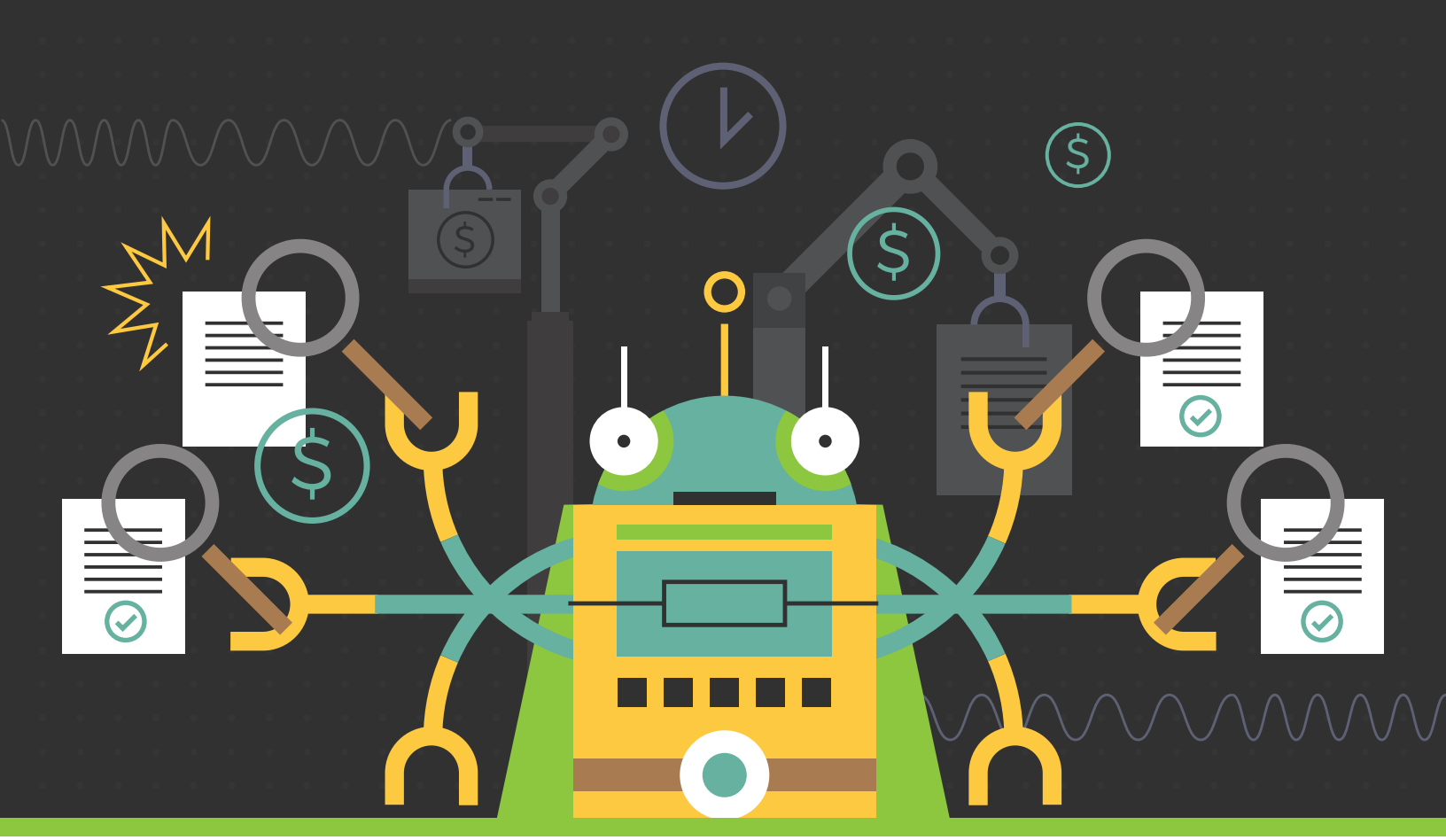
Financial institutions enter into many service-level agreements (SLAs) detailing how they conduct online banking transactions, handle loan applications, process e-bills and fulfill investment orders. These agreements are as good for financial institutions as they are for customers because they provide transparency, motivate banks to fine-tune operations and help manage costs.

In addition to spelling out how banks will provide services, SLAs also keep banks accountable to meet their own internal service standards. If banks fail to process investment transactions in a timely fashion or if they fail to meet their standards when processing loan applications as outlined by their SLAs, they could trigger significant financial penalties.

In addition to compensating customers for service lapses, banks could face costly regulatory enforcement actions. According to analysis from Deloitte, the number of enforcement actions against financial institutions spiked after the 2008 recession but significantly tapered off after 2012. Although the number of enforcement actions dropped, the dollar amount for financial penalties has significantly increased. Financial institutions have paid $4 billion in restitution and $1.5 billion in civil penalties levied by the Office of the Comptroller of the Currency alone — and that doesn't take into account penalties handed down by the SEC, the Justice Department, the Federal Reserve, the FDIC or the Consumer Financial Protection Bureau.

Many SLA failures inevitably relate back to how file transfer activities are implemented. If not implemented correctly, file transfers may introduce problems such as files sent to the wrong recipient or sensitive customer data exposed in transit. Scripting errors can also lead to violations in records retention requirements, resulting in an inability to monitor who accessed files and when.





Protecting Customers' Data

A wide range of regulations, including the Sarbanes-Oxley (SOX) Act, Dodd-Frank and Gramm-Leach-Bliley, all require clear procedures for monitoring the security and integrity of private data. Facing increasing numbers of file transfers and growing file sizes, many bank IT departments struggle to match the pace.

Timing

Bank SLAs contain promises to process information within specified time frames. When file transfers fail, the consequences range from inconvenience for customers to significant financial loss for the banks. An e-bill paid late could lead to finance charges and late fees, and a mishandled deposit could trigger overdrafts and other headaches.

Bank SLAs contain promises to process information within specified time frames.

Best Execution and SLAs Related to Trading

When it comes to placing trading orders for customers, timing is everything. Delays of even nanoseconds in the time that a brokerage order reaches an exchange can lead to disadvantageous pricing for investors. The Securities and Exchange Commission states that if a firm advertises speed in execution of trades — or includes language about trade execution speed in its SLAs — they can neither exaggerate the speed nor fail to inform investors if a delay takes place. Such actions could not only violate SLAs but also the principle of best execution.

To get the best possible pricing for clients, brokers can use multiple options for executing trades. They may transmit the order directly to the exchange, route it through a market maker, use an electronic communications network or send it to another division within the firm. When financial institutions or custodians fail to achieve best execution, particularly for large pension funds and other institutional investors, costly litigation and regulatory fines can ensue.

In 2014, for example, FINRA brought action against broker-dealers who failed to live up to the principles of best execution for their clients. One broker-dealer paid $1.85 million in fines and $638,000 in restitution for processing orders in a way that failed to get the best prices for its clients. Another broker-dealer paid a $210,000 fine and $70,548 for failing to deliver best execution in 51 corporate bond transactions.

Tracking

Banks need clear processes for monitoring the security and integrity of their customers' private data. They need to know who accesses data, who transfers it to a third party and who actually receives it, and they need to know when and how each transfer happens.

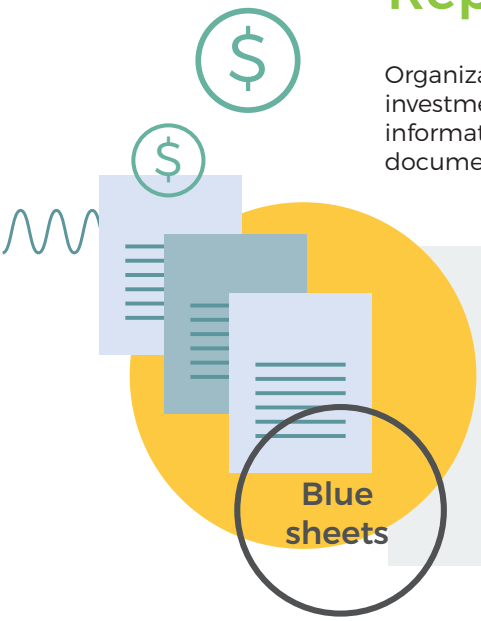
Too often, documents disappear, and a lack of tracking data makes it impossible to recover them or find out if there was a data breach. In addition to causing problems for customers, banks become exposed to liability.

In one incident in 2013, a customer service agent informed customers at a major bank that their loan documents were missing. The bank in question had purchased the loan from another bank, which had provided incomplete documentation. Instead of seeking to restore the missing documents, the bank allegedly fired the agent and forbade others to tell customers when documents were missing. The agent ended up suing the bank.

In addition to tracking the placement of documents, banks have an obligation under the Safeguards Rule of Gramm-Leach-Bliley to design, maintain and implement plans that protect customer information. A major bank was fined $1 million by the SEC in 2016 because it failed to implement its own data security plans. An employee transferred customer files onto a personal computer, which was then compromised by outside attackers. In addition, the employee who placed customer data on a personal computer was ordered to pay $600,000 restitution, was sentenced to 36 months probation and was banned from the securities industry for five years. The employee had discovered a workaround for authenticating file transfers because the bank did not implement role-based access to files, which compromised confidential customer information.

Reporting

Organizations like FINRA and the SEC expect investment banks to provide complete information about every trade. These documents, called blue sheets, include data like security name, purchaser name, transaction date, share quantity, share price and whether the transaction was a buy, sell or short sale order.



In 2016, FINRA fined a major bank $6 million for submitting blue sheets that either misrepresented or omitted trade data. In addition to submitting incorrect or incomplete blue sheets, the bank often submitted them well after the due dates established by FINRA. This bank wasn't the only one that faced penalties for late and bungled blue sheet submission. The previous year, two other banks paid $4.25 million and $2.95 million respectively to FINRA.

Staying Away From Avoidable Penalties

A managed file transfer (MFT) solution that covers file transfers between users, customers, partners and systems helps financial institutions meet SLAs regarding transaction timing and document review.

A managed file transfer (MFT) solution that administers file transfers between users, customers, partners and systems helps financial institutions meet SLAs pertaining to transaction timing and document review. It also provides clear visibility over all transfers, leading to an easily accessible audit trail and helping banks fulfill regulatory compliance obligations. Picture a file transfer solution that automatically collects blue sheet data, making submitting blue sheets to the SEC a snap. Imagine a system that automatically alerts managers to unusual access or file transfer patterns, helping banks respond to unauthorized access or cyberattacks more quickly and effectively.

A good MFT solution

- Encrypts data at rest and in transit
- Keeps sensitive data, access logs and authentication processes from being altered
- Is operable with minimal scripting knowledge within IT
- Helps banks meet their data protection and compliance requirements

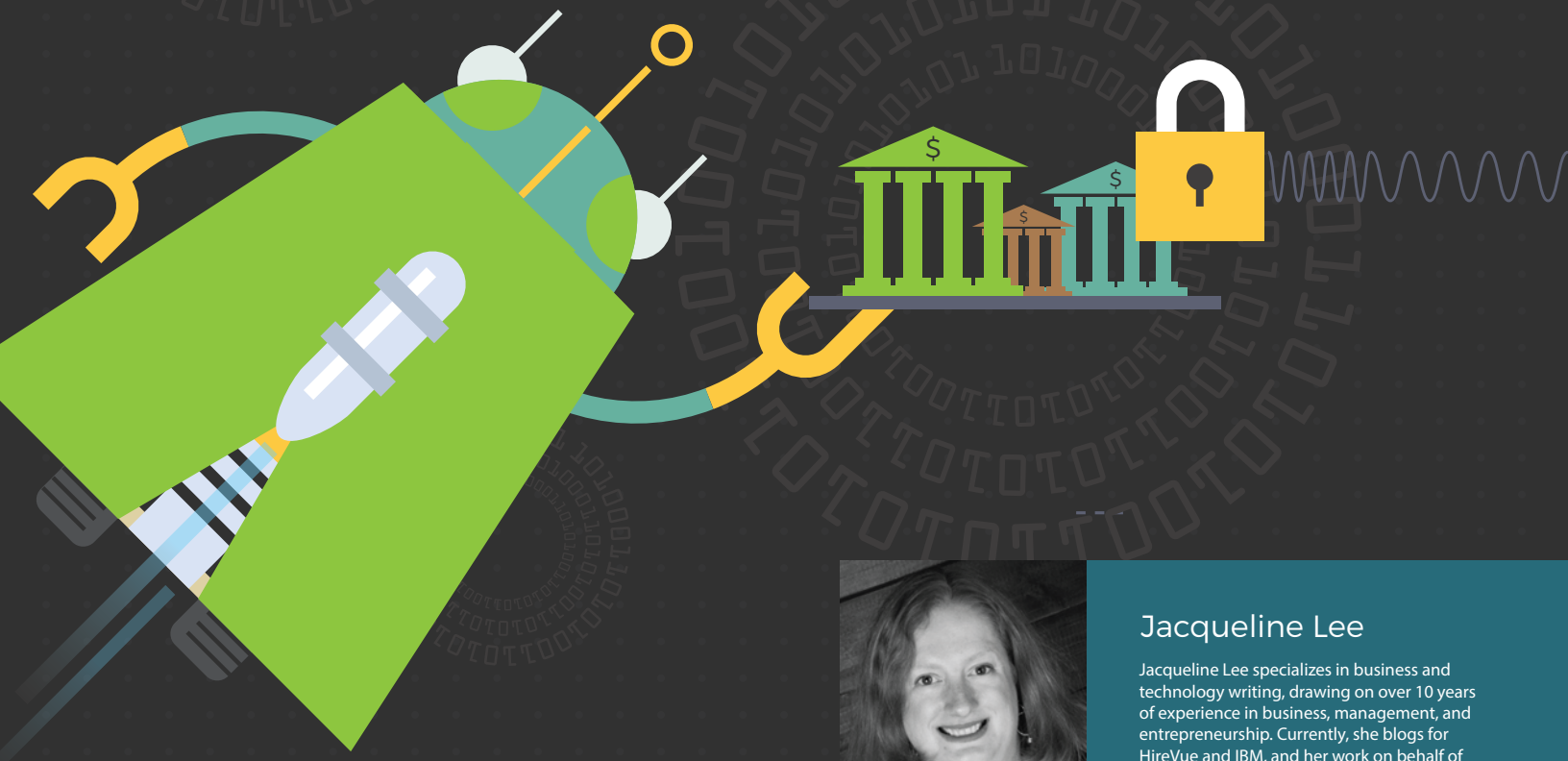
Conclusion

Protect Customers and Profits

Choose a solution that offers security, easy operation and out-of-the-box regulatory compliance, and something that helps your bank meets its SLA obligations.

Instead of developing a file transfer system from scratch and manually upgrading it — and to avoid employees using insecure file transfer methods that put information at risk — it makes sense for banks of all sizes to use MFT.

Choose a solution that offers security, easy operation and something that helps your bank meets its SLA obligations. Find out how MFT can protect both your customers and your profits.



Jacqueline Lee

Jacqueline Lee specializes in business and technology writing, drawing on over 10 years of experience in business, management, and entrepreneurship. Currently, she blogs for HireVue and IBM, and her work on behalf of client brands has appeared in Huffington Post, Forbes, Entrepreneur, and Inc. Magazine.