Docket No. OP-1670
Response from Nice Actimize

At Nice Actimize we've been involved in Real Time payments for over 10 years, especially in the UK.

With multiple real time services available in other jurisdictions it is clear such services are good for innovation and providing equality in the financial system.

Where such systems are ubiquitous, real benefits to consumers and small businesses include:

- Increased credit interest or decreased funding costs
- Easier management of funds and creditor positions and ability to manage money on the move
- Innovation in payments, leading to reduced costs for small business and consumers

However, with along with these benefits comes increase fraud.

Key thoughts:

Our experience from the UK suggests the following:

Demand by consumers and fraudsters/Money Launderers alike, will be higher than anticipated and will manifest sooner, due to a number of reasons:

- New payment innovations
- Time and effort savings
- Irrevocability

Fraudsters like new networks and expect less sophisticated controls at implementation and will ruthlessly exploit these.

Fraud losses will increase and quickly, so early investments in fraud controls will be quickly returned. Failure to do so will be costly in the medium term.

As controls increase, fraudsters target humans (customers) more, via social engineering, leading to increased authorized fraud. However, authorized frauds still have costs (operational and reputational) for the firms, so they do have reason to help prevent these frauds as it is cheaper to prevent than deal with the consequences.

Authorized frauds are often life-changing events for the consumer or business since they're less likely to be refunded and are for larger amounts than say, card fraud.

Reputational issues

Firms who do not offer a real time payments service will suffer as their clients move to those that do, so providing the ability to access such a service is key to fostering a competitive environment.

Firms that do not invest in the appropriate fraud systems to manage real time payments will see higher relative fraud losses. This could be magnified for smaller firms as they could be targeted heavily if they slip behind.

This may cause customers to move institutions as well as regularity scrutiny.

Operational issues

Firms need to have systems and processes to allow flexibility to cover any fraud attacks. This is important to stop fraud attacks quickly as otherwise a small attack can escalate into a major attack with large operational issues and costs, along with losses and high negative customer impacts.

Nation State attacks may not be covered by insurance as they could be seen as an act of war and this needs to be factored.

Recommendations

Let banks compete and be responsible for authentication and making decisions on how and when to stop payments, while ensuring there are minimum standards and good fraud typology definitions.

Where there are new overlay services such as request to pay, these should be carefully designed to avoid exacerbating social engineering MO's. Trust is key to these services, so if these are provided through banks, the controls allowing parties to request payments must be robust as consumers will assume it is trustworthy if provided through a financial institution. If not, a large increase in authorized fraud could follow.

There is a need for network level fraud reporting and automation of repatriation of fraudulent funds in order to reduce the impact on consumers and improve prevention and recovery rates.

Ensuring the beneficiary bank knows which transactions have been confirmed as fraud accurately and quickly is key to reducing losses. Having this intelligence within the network rather than outside it can help enormously.

Velocity (volume and value) checks for entities at the network level with a score(s) that can be passed through to the bank counterparties (synchronous or asynchronous) will help with this too.

Some agreement to perform counterparty checking for name matches to the account details provided, an extension of the directory services mentioned within this FedNow notice, is also desirable.

Mandating real time fraud profiling capabilities on banks for both outbound and inbound payments is key to reducing fraud and money laundering across the ecosystem.

Facilitating intelligence and data sharing mechanisms will help reduce overall fraud in the system and if this can be linked directly at the network level, so much the better.

Industry education campaigns to help consumers understand key fraud MO's are also important.

Relevant NICE Actimize Publications

Real Time Payments White Paper

https://www.niceactimize.com/white-papers/Real-Time-Payments--Learnings-from-a-Decade-in-the-UK-45

Real Time Inbound Payments White Paper

https://www.niceactimize.com/white-papers/The-Moment-for-Implementing-RealTime-Inbound-Payment-Profiling-is-Now-Are-you-ready-to-manage-the-AML-issues-49

Blogs:

FedNow Fraud Threats

https://www.niceactimize.com/blog/fednow-fraud-threats-and-how-fis-can-counter-them--618

Fraud Definitions

https://www.niceactimize.com/blog/fed-fraud-definitions-wg-an-important-first-step-towards-collaborative-fraud-fighting-626

Canadian Payment Modernisation 1 & 2

https://www.niceactimize.com/blog/canadian-payments-modernisation-taking-on-new-fraud-threats-612

https://www.niceactimize.com/blog/canadian-payments-modernisation-what-fis-can-do-to-counter-fraud-threats-613