Why doesn't eCommerce use unbreakable encryption?

A blockbuster fourth quarter contributed to the strongest year-over-year growth for U.S. e-commerce in six years, according to a report released this morning from the U.S. Commerce Department. Consumers spent $453.46 billion on the web for retail purchases in 2017, a 16.0% increase compared with $390.99 billion in 2016. That's the highest growth rate since 2011, when online sales grew 17.5% over 2010. – Digital Commerce 360

Fraud attacks on e-commerce businesses during the holiday season grew significantly on a year-over-year basis, according to antifraud technology provider ThreatMetrix. The San Jose, Calif.-based identity company, in its Q4 2017 Cybercrime Report, said nearly 193 million transactions that crossed its network were fraudulent—a 173-percent increase from Q4 2016. Attack rates on e-commerce overtook those aimed at media companies for the first time in two years, the report said, driven by account creation and login attacks. - CardNotPresent

I'm trying to imagine in what other commerce situations is escalating use tied to escalating crime? 'New Store Opens!! Crime Rate TRIPLES!!' is the headline…with a quote from the Police Commissioner 'Don't worry! I shop there all the time!'

There must be, and is, something wrong here. Account creation and login attacks will continue to escalate as the dollars available to steal escalate. And what is there to deter them, if we keep using the same tools, the same security technology, the exact same eCommerce methods? Didn't that famous Einstein guy teach us about the lunacy of expecting something different from the same thing? When will we learn – next year?

It isn't enough to *add tools* either: just because we can layer sophisticated data analysis over top of transaction data and attempt to identify the 'bad' ones isn't the same thing as actually making a 'bad' one *have to be different*. There isn't any sophistication required to see a rotten apple – the goal is simply to improve the tools used to convey them; then it's a no-brainer to pick them off the belt as they go by. eCommerce fraud exists, and will continue to escalate, as long as the way the conveyer belt is built remains the same. It's too slow, stops and starts, lets apples roll right off, has sections of it that are hidden from view, and hasn't changed the underlying motor drive since the conveyor belt was first invented! Lunacy, indeed.

The good news is that there *are* new tools, new methods available – and they include provably secure, unbreakable, transaction security. If these were used, not only would it be impossible to interfere with existing accounts, but account creation can actually be controlled. And no further worries about your stored credit cards, as you won't need to have them anyplace other than in your wallet! And logins? Unbreakable means these new methods can be configured by the commerce owners to better suit their systems, processes and sales channels. Using a combination of these new tools, along with our increased sophisticated data analysis, sales can continue to escalate *as fraud declines to a near-stop*.

We'll never be able to halt store employee theft completely – merchants have to trust somebody! – but wouldn't it be nice to shop right alongside that Police Commissioner in the safest neighborhood in town…The Internet?!