A Case Of Mistaken Identity

by Steve Brown

You might recall Double Trouble, a short-lived TV series that aired in the mid-1980s, which highlighted the antics of identical twin sisters Kate and Allison. Though the series only lasted two seasons, there were several episodes in which the teenage troublemakers switched places or borrowed each other's identities. There were sometimes damaging consequences, but always with lessons learned.

Today, it's all too easy for thieves to usurp innocent people's identities or credentials and gain access to sensitive employee or customer data. One area where banks may be particularly vulnerable is with employees who work remotely. The need for additional security has increased significantly over the past several years as many banks have been growing their work-from-home programs.

Just like lightning seeks out the shortest route to something with a positive charge, cyber-thieves also seek the easiest point of entry. In many cases this could be the home computer of a bank employee who works remotely. Consider last year's massive data breach at JP Morgan in which names, addresses, phone numbers and email addresses of some 83mm households and small business accounts were exposed. The breach reportedly originated with hackers who broke into the computer of an employee working from home.

To be certain, there are old school organizations that still resist the idea of employees working remotely, but times are changing and they probably won't be able to hold out forever. Consider that as part of its annual analysis of the top companies with remote jobs, FlexJobs (a website for telecommuters) reported a 26% increase in the number of remote jobs posted compared with 2014. These stats aren't specific to banks, but they paint an interesting picture of what's happening in the broader job market. Banks that don't eventually offer some type of work-at-home-option are likely to find themselves fighting to keep good employees. Hence it makes sense for all banks to explore the latest technology developments that allow employees to work at home without compromising the security of the bank or its customers.

In this vein, a number of small and large banks are trying to make it safer for employees to work at home using the latest authentication technology. So for instance, instead of logging in from home with just their name and password, some banks require staffers to take the additional step of entering a code sent to them on their cell phones via text message, others require fobs and still others are experimenting with biometrics.

Out-of-band authentication is commonly used when initiating mobile banking apps, but it can also be used to authenticate remote computers. Fingerprint sensors are also coming into broader use, as well as other physical authentication methods.

Of course even with out-of-band authentication, the possibility of fraud still exists, so banks need to pile on as many protections as reasonably required. Limiting the timeframe of the passcode that's been generated is one precaution to take. Another is to limit each passcode to a specific session and machine. Banks should also control who within in the company can enter or alter an employee's cell

phone number, so thieves can't wreak havoc by creating their own numbers to receive text messages.

In the fast-moving world we live in today, it's not always clear that people are who they appear to be. As banks increasingly allow employees to work remotely, the dangers of a security breach will continue to mount. Bankers know that what's funny on TV may not be in reality. Our advice is for bankers to protect your franchise and your customers, as you slowly and carefully expand your remote working staff given changes in the industry. In this way, you can avoid double trouble.

BANK NEWS

Collapse Averted

After teetering on bankruptcy as a country, Greek politicians have agreed to very strict conditions to get $86B in Euros over 3Ys from EU leaders. Under terms of the agreement: Greece will have to ask permission to gain access to $50B of the funding (in a controlled account), reform their pension system, enact spending cuts, recapitalize the banking system, raise taxes, have parliamentary agreement to all reforms, pay down debt.

M&A Activity

1) First State Community Bank ($1.8B, MO) will acquire Central Bank ($264mm, MO) for an undisclosed sum. 2) BankFirst Financial Services ($741mm, MS) will acquire Newton County Bank ($162mm, MS) for an undisclosed sum.

Closure #6

Premier Bank ($32mm, CO) was closed by regulators on Friday and sold to United Fidelity Bank, fsb ($300mm, IN) under a purchase and assumption agreement. United gets 2 branches, all deposits and essentially all of the assets.

Facial Recognition

The Silicon Valley Business Journal reports Facebook's artificial intelligence lab is developing software that can recognize individuals in a picture with 83% accuracy - even if their face is obscured.

Check Risk

Security experts say 90% of bad checks are written on accounts less than 1Y old.

Higher Reserves

Reuters reports US banks may need to boost loan loss provisions amid ongoing weakness in oil and gas.

Rate Hikes

Boston Fed President Rosengren said Sep may be the appropriate time for rate hikes. Meanwhile, Fed Cleveland President Mester said she would support two rate hikes this year despite turmoil in Greece and China.

Branch Closures

There are still more than 90,000 bank branches in the US, but experts say trends point to another 15% (about 13,500) being closed in the coming years as consumer behavioral changes continue to impact the industry.