



Paysafe & ABTOT

PSD2, 'Your Acquirer', the Data they hold and CyberCrime

4th December 2017

117 Houndsditch, London, EC3A 7BT

Today's agenda



**Don't worry not a discussion
about me; but the picture of
me and where it was taken**



**MasterCard & Paysafe
Better data for our
merchants**



Cyber Security?!

PSD2 & *my photo*

Aim:

- To reduce fraud

Key Facts:

- Introduction of two-factor authentication requirement
- Knowledge (something only the customer knows, i.e. password/PIN)
- Possession (something only the customer has, i.e. mobile/card)
- Inherence (something unique to the customer, i.e. fingerprint/behavioural data)

PSD2

Exemptions:

- **F2F contactless payments - under €50 with cumulative up to €150 or five transactions**
- **Online payments – under €30 up to five transactions or €100**
- **Transaction RiskAnalysis**
- **Secure corporate payments (e.g. virtual cards/lodge products)**
- **Whitelisting**
- **Recurring Payments**

Outcome:

- **Changes to 3D secure**
- **Amended consumer journey**
- **Reduction in fraud losses**

PSD2 & Recent Conferences

“The problem is that the travel industry is going to be one of the industries hit hardest, because credit card fees are widespread and very commonly used. Unfortunately it will be the smaller companies in particular who are hardest hit by the credit card surcharge ban. I think there will probably be quite a few companies out there who properly don’t comply, especially initially. Time will tell how much the industry is actually affected.”

FarinaAzam, Partner at [Travlaw](#)

The Travel Network Group creates petition to spark parliamentary surcharging debate

The Travel Network Group has created an online petition seeking to make Westminster consider the “extremely unfair” impact upon the travel sector of the upcoming card surcharging ban.

Commission sets deadline for banks to meet new payment standards

27 November 2017 | 11273 views | 0



European banks and service providers have been given an 18-month deadline to adopt new security measures and provisions for customer data exchange as mandated by the EU's revised Payments Service Directive (PSD2).

Although PSD2 comes into effect on January 2018, two of the most contentious measures in the rule-book, relating to more stringent security measures for payments transactions and the abolition of 'screen-scraping', will now be considered actionable 18-months after the relevant Regulatory Technical Standards (RTS) are published in the Official Journal of the EU, scheduled for September, 2019.

How comfortable are Travel Merchants with PSD2

- **36% not comfortable**
- **36% somewhat uncomfortable**
- **14% comfortable**
- **14% fairly comfortable**
- **0% very comfortable**

Preferred route for tackling surcharges

- **29% plan on passing the cost through to consumers by increasing prices**
- **25% will absorb additional costs**
- **21% plan on passing the costs through to consumers via a booking fee**
- **21% will seek alternative payment options**
- **4% say costs will be covered by increasing commission**

Thoughts?

- **How are the EU and Member States going to police this?**
- **Could small retailers fall under the radar for charging?**
 - **What about Brexit?**

There it is in its full glory?

25th November 2015 - over 2 years ago

DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 November 2015

on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

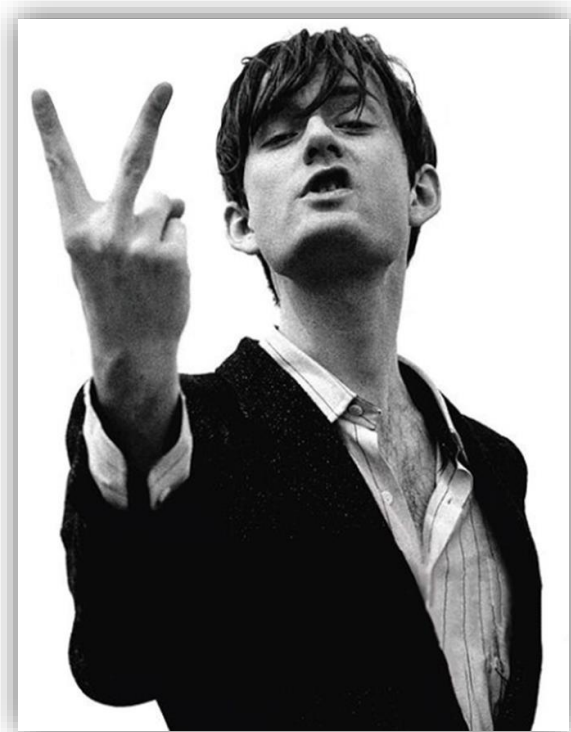
Having regard to the opinion of the European Central Bank ⁽¹⁾,

Having regard to the opinion of the European Economic and Social Committee ⁽²⁾,

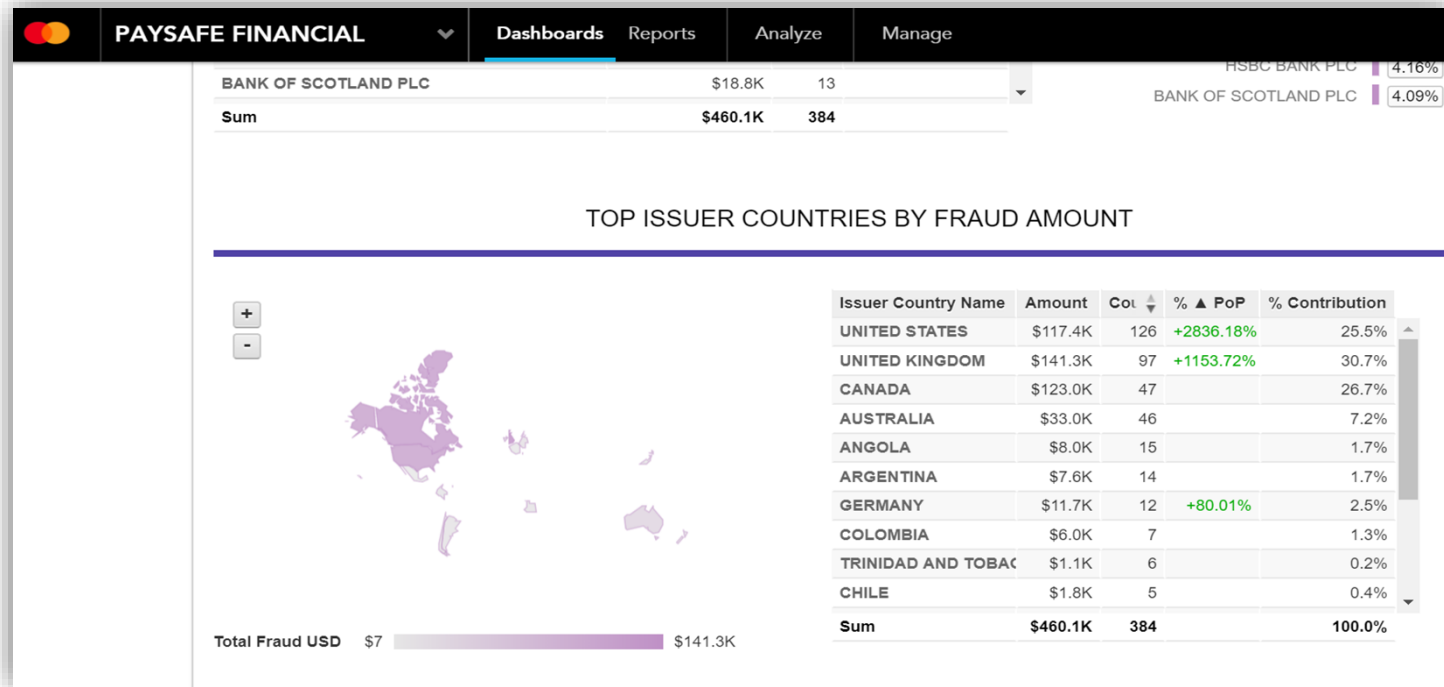
Acting in accordance with the ordinary legislative procedure ⁽³⁾,

Whereas:

I am sure it is more like this for you though



Mastercard & Paysafe



Mastercard & Paysafe

The screenshot displays the 'Acquirer Dashboard' interface. At the top, a navigation bar includes 'PAYSAFE FINANCIAL', 'Dashboards', 'Reports', 'Analyze', 'Manage', and 'Help'. Below this, the dashboard title 'Acquirer Dashboard' is shown with utility icons for lock, clock, print, and settings. A series of tabs allows navigation between 'Getting Started Videos', 'Portfolio', 'Fraud Overview' (selected), 'Fraud Detail', 'Chargeback Overview', 'Chargeback Detail', 'Decline Overview', 'Decline Detail', and 'Analysis by'. The main area contains a grid of filter dropdown menus: 'MERCHANT REGION' (All), 'MERCHANT COUNTRY' (All), 'ACQUIRER ICA' (All), 'MERCHANT CATEGORY CODE' (4722), 'ENTRY MODE DESCRIPTION' (All), 'LOCATION TYPE' (All), 'MERCHANT ID' (All), 'MERCHANT NAME' (All), 'FRAUD TYPE' (All), 'CARD PRESENT OR NOT' (All), and 'SECURE CODE' (All). The Mastercard logo is positioned on the right side. At the bottom, two chart titles are visible: 'FRAUD BY QUARTER' and 'FRAUD BY CP vs. CNP'.

Mastercard & Paysafe

PAYSAFE Brand Agnostic ▾ Dashboards Reports Analyze Manage

Acquirer Dashboard

Getting Started Videos Portfolio **Fraud Overview** Fraud Detail Chargeback Overview Chargeback Detail Decline Overview Decline Detail Analyze

MERCHANT REGION: All ▾ MERCHANT COUNTRY: All ▾ ACQUIRER ICA: All ▾ MERCHANT CATEGORY CODE: All ▾

ENTRY MODE DESCRIPTION: All ▾ LOCATION TYPE: All ▾ MERCHANT ID: All ▾ MERCHANT NAME: All ▾

FRAUD TYPE: All ▾ CARD PRESENT OR NOT: All ▾ SECURE CODE: All ▾ BRAND NAME: All ▾

FRAUD BY QUARTER FRAUD BY CP vs. CMP

Mastercard & Paysafe

FRAUD BY TYPE

Quarter	Q4/2016		Q1/2017		Q2/2017
Fraud Type	Amount	% Contribution	Amount	% Contribution	Amount
ACCT TAKEOVER	\$1.3K	0.46%	\$432	0.25%	
COUNTERFEIT	\$19.7K	6.89%	\$1.6K	0.92%	
FRAUD APP	\$562	0.20%	\$5.1K	2.94%	
LOST	\$2.7K	0.94%	\$850	0.49%	
MO/TO	\$256.4K	89.48%	\$164.6K	94.04%	\$
MULT IMP	\$2.2K	0.77%			
NEVER RECEIVED	\$35	0.01%			
STOLEN	\$3.6K	1.25%	\$2.4K	1.37%	
Sum	\$286.5K	100.00%	\$175.1K	100.00%	\$

% Change from last quarter		
Fraud Type	% ▲ Prev. Qtr	▲ ▼
MO/TO	219.04%	\$566
COUNTERF	685.74%	\$17.
NEVER REC	21885.46%	\$12.
LOST	388.49%	\$10.
STOLEN	1.65%	\$4.7
ACCT TAKE	15.02%	\$1.6
FRAUD APP	133.32%	\$677

Mastercard & Paysafe

FRAUD BY PRODUCT

Quarter	Q4/2016		Q1/2017		Q2/2017	
Product	Amount	% Contribution	Amount	% Contribution	Amount	% Contribution
COMMERCIAL CREDIT	\$19.7K	6.88%	\$29.5K	16.86%	\$11.1K	5.88%
COMMERCIAL DEBIT	\$514	0.18%	\$687	0.39%	\$1.0K	0.55%
COMMERCIAL PREPAID	\$220	0.08%				
COMMERCIAL WORLD			\$40	0.02%	\$737	0.39%
COMMERCIAL WORLD ELITE						
CONSUMER CREDIT	\$181.5K	63.36%	\$101.4K	57.91%	\$109.1K	57.98%
CONSUMER CREDIT WORLD	\$23.9K	8.34%	\$21.5K	12.27%	\$26.4K	14.03%
CONSUMER CREDIT WORLD ELITE	\$11.3K	3.93%	\$2.6K	1.49%	\$2.9K	1.56%
CONSUMER DEBIT	\$40.6K	14.15%	\$15.9K	9.10%	\$35.6K	18.93%
CONSUMER DEBIT WORLD			\$1.8K	1.05%		
CONSUMER PREPAID	\$8.8K	3.08%	\$1.6K	0.90%	\$1.3K	0.68%
Sum	\$286.5K	100.00%	\$175.1K	100.00%	\$188.2K	100.00%

Mastercard & Paysafe

TOP ISSUERS BY FRAUD AMOUNT

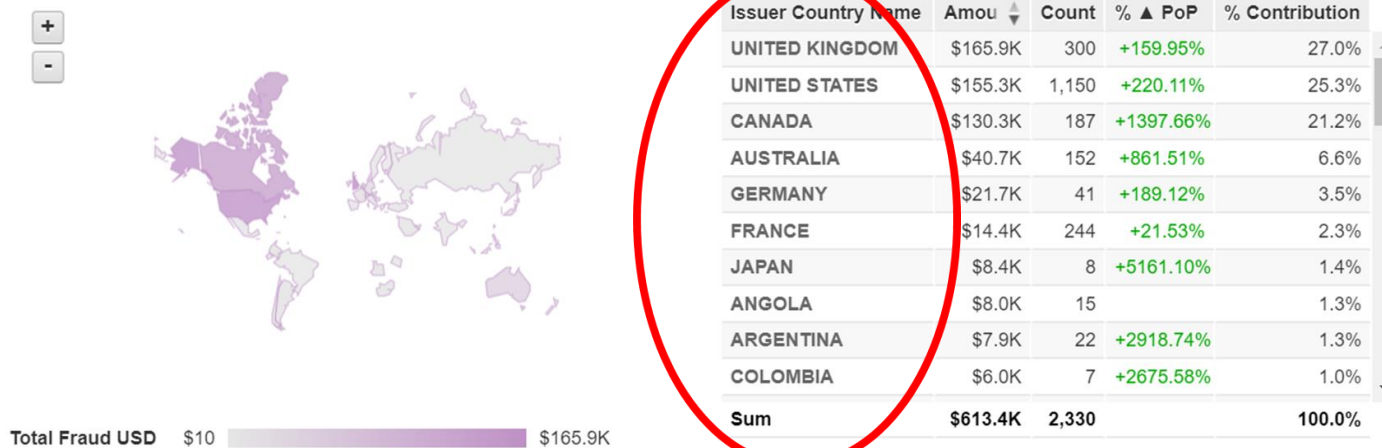
Issuer ICA Name	Amount	Count	% ▲ PoP
BANK OF MONTREAL	\$139.4K	92	+8254.27%
BANK OF AMERICA NATIONAL ASSOCIATION	\$31.4K	103	+348.16%
JPMORGAN CHASE BANK N.A.	\$30.5K	48	+6019.34%
SANTANDER UK PLC	\$26.0K	28	
TESCO PERSONAL FINANCE LIMITED	\$25.2K	24	+606.90%
CITIGROUP PTY LIMITED	\$24.8K	34	
LLOYDS BANK PLC	\$23.7K	33	-4.67%
HSBC BANK PLC	\$20.1K	21	+649.01%
BANK OF SCOTLAND PLC	\$20.0K	22	+47054.83%
BMO HARRIS BANK N.A.	\$19.8K	18	+6716.77%
Sum	\$613.4K	2,330	

Top 10 Issuers Contribution

BANK OF MONTREAL	22.72%
BANK OF AMER... ASSOCIATION	5.12%
JPMORGAN CHASE BANK N.A.	4.97%
SANTANDER UK PLC	4.24%
TESCO PERSON...ANCE LIMITED	4.10%
CITIGROUP PTY LIMITED	4.04%
LLOYDS BANK PLC	3.86%
HSBC BANK PLC	3.28%
BANK OF SCOTLAND PLC	3.26%
BMO HARRIS BANK N.A.	3.24%

Mastercard & Paysafe

TOP ISSUER COUNTRIES BY FRAUD AMOUNT

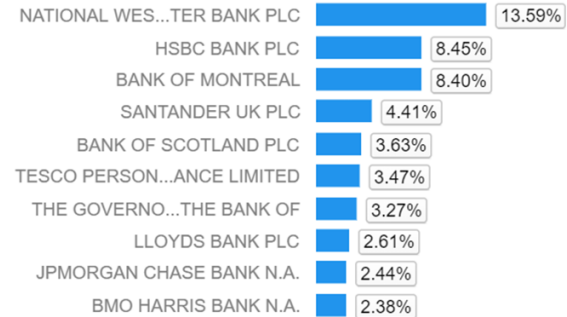


Mastercard & Paysafe

TOP ISSUERS BY DECLINE AMOUNT

Issuer ICA Name	Amount	Count	% ▲ PoP
NATIONAL WESTMINSTER B...	\$755.6K	690	+327.04%
HSBC BANK PLC	\$469.9K	289	+115.75%
BANK OF MONTREAL	\$467.2K	197	+27606.47%
SANTANDER UK PLC	\$245.5K	176	+58.82%
BANK OF SCOTLAND PLC	\$202.1K	208	+130.22%
TESCO PERSONAL FINANCE	\$193.2K	229	+77.34%
THE GOVERNOR AND COMP.	\$182.0K	343	-19.20%
LLOYDS BANK PLC	\$145.2K	168	+46.77%
JPMORGAN CHASE BANK N.	\$135.4K	191	
BMO HARRIS BANK N.A.	\$132.3K	79	
HSBC BANK MIDDLE EAST	\$122.2K	8	+10124.56%
BARCLAYS BANK PLC.	\$113.6K	91	+3330.44%
CLYDESDALE BANK PLC.	\$105.0K	174	+7.72%
BANK OF AMERICA NATION	\$101.8K	144	+2001.13%
NEWDAY LTD	\$95.4K	119	+140.87%
COMMONWEALTH BANK OF	\$95.0K	138	+2535.47%

Top 10 Issuers

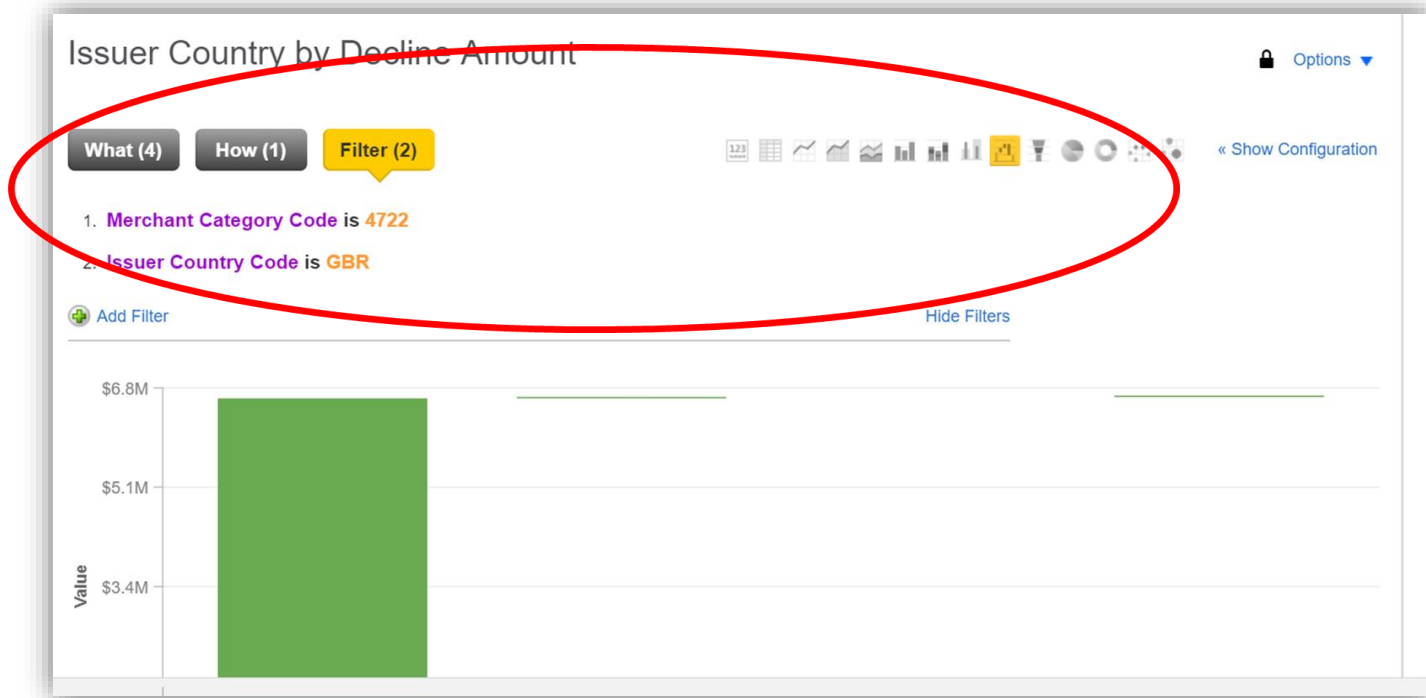


Mastercard & Paysafe

DECLINE BY RESPONSE CODES

Quarter	Q1/2017			Q2/2017			Q3/2017			Q4/2017		
	Response Code	Amount	% Contribution	Amount	% Contribution	Amount	% Contribution	Amount	% Contribution	Amount	% Contribution	
Do not honor	\$1.4M	1.39%	6.88%	\$3.9M	16.28%	\$3.6M	19.97%					
Insufficient funds/over	\$435.3K	0.45%	2.18%	\$772.2K	3.23%	\$630.0K	3.50%					
Lost card	\$874	0.00%	0.00%	\$175.5K	0.73%	\$241.5K	1.34%					
Transaction not perm	\$1.6K	0.00%	0.01%	\$122.0K	0.51%	\$119.4K	0.66%					
Invalid transaction	\$23.2K	0.00%	0.12%	\$18.8K	0.08%	\$88.1K	0.49%					
Exceeds withdrawal l	\$258.2K	0.08%	1.29%	\$188.1K	0.79%	\$80.4K	0.45%					
Capture card	\$16.7K	0.00%	0.08%	\$126.5K	0.53%	\$79.9K	0.44%					
Invalid card number	\$13.5K	0.00%	0.07%	\$51.8K	0.22%	\$42.3K	0.23%					
Stolen card	\$168	0.00%	0.00%	\$26.2K	0.11%	\$26.5K	0.15%					
Restricted card	\$13.8K	0.00%	0.07%	\$28.5K	0.12%	\$21.6K	0.12%					
Refer to card issuer	\$1	0.00%	0.00%	\$22.7K	0.09%	\$17.0K	0.09%					
Security violation				\$18.9K	0.08%	\$14.9K	0.08%					
Exceeds withdrawal c	\$2.8K	0.00%	0.01%	\$65.8K	0.28%	\$12.6K	0.07%					
Expired card	\$9.9K	0.00%	0.05%	\$22.3K	0.09%	\$8.9K	0.05%					
Invalid/nonexistent a				\$9.0K	0.04%	\$6.2K	0.03%					

Mastercard & Paysafe



How safe is your child? Best-selling smart toys have 'worrying security failures' that let strangers talk to your little ones without your knowledge



- Consumer group Which? paid hackers to break into a range of the gadgets
- They include the I-Que robot, Furby Connect, Toy-fi Teddy, and CloudPets
- Hackers say a lack of Bluetooth security protection measures made this easy

Cybercrime



Cybercrime

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.



Financial losses through spear phishing

One of Europe's Biggest Companies Loses €40 Million in Online Scam

German electrical cable maker Leoni falls victim to BEC scam

Investigators say the email was crafted in such a way to take into account Leoni's internal procedures for approving and transferring funds. This detail shows that attackers scouted the firm in advance.

Austrian Aeronautics Company Loses Over €42 Million to BEC Scam

May 26, 2016



Fischer Advanced Composite Components AG (FACC), an aeronautics company in Austria, is the latest victim to a **business email compromise** (BEC) scheme after being **swindled** to a record 42 million euros (around \$47 million) through a **spear-phishing** attack.

FACC is a major designer and manufacturer of aircraft components and systems, with a client base that includes Boeing, Airbus, Rolls-Royce, Siemens SAS and Mitsubishi Heavy Industries.

According to reports, the incident occurred last January and involved a fake email that impersonated its then CEO Walter Stephan, conning one of FACC's financial department employee into wiring 50 million euros that was supposedly for one of the company's acquisition projects. FACC, realizing that they were tricked, adopted countermeasures and was able to stop the transfer of 10.9 million euros on the recipient accounts. The rest of the money, however, has already **disappeared** in Slovakia and Asia.



<http://news.softpedia.com/news/one-of-europe-s-biggest-companies-loses-40-million-in-online-scam-507818.shtml>

- impersonate emails from German executives/CEO
- unauthorized money transfer
- victim: CFO/accountant
- ~ 40 Mio EUR losses

If we can't rely on our Credit Agencies to protect our data – then who?



Constant examples in the news



Three Uber security managers resign after CEO criticizes practices

Joseph Menn, Dustin Volz

4 MIN READ



SAN FRANCISCO/WASHINGTON (Reuters) - Three senior managers in Uber Technologies Inc's security unit resigned on Friday, an Uber spokesperson said, days after the company's new chief executive officer disclosed a massive data breach and criticized past security practices.

vtech

VTech

This data breach is the first to directly target children. An unauthorized party accessed customer data through the Learning Lodge app store and Kid Connect servers on Nov. 14.

CONSEQUENCES:

- 6.4 million children and 4.9 million parents' accounts worldwide were compromised.
- Exposed information: names, passwords, IP addresses, download history, and children's genders and birth dates.

Cybercrime....the way we pay



Come and speak with the Paysafe team after the seminar

- **Simon Chandramani** – simon.chandramani@paysafe.com
- **Nick Ryan** – nick.ryan@paysafe.com
- **Tom Pilling** – tom.pilling@paysafe.com
- **Debbie Morgan** - debbie.Morgan@Paysafe.com
- **Veronica Smith** - veronica.Smith@paysafe.com
- **Elysia Field** - elysia.field@paysafe.com

Thank you!

Tom Pilling
Head of Risk at Paysafe
Acquiring Division Europe

tom.pilling@paysafe.com

